T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

ELEKTRONİK BANKACILIKTA BANKALARIN ÖZEN YÜKÜMLÜLÜĞÜ

DOKTORA TEZİ

Sevinc NOVRUZOVA

Danışman
Prof. Dr. Şahin AKINCI

Konya-2021

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin	Adı Soyadı	Sevinc NOVRUZOVA
	Numarası	124133001008
	Anabilim / Bilim Dalı	Hukuk / Özel Hukuk
	Programı	Tezli Yüksek Lisans ( ) Doktora (X)
	Tez Danışmanı	Prof. Dr. Şahin AKINCI
	Tezin Adı	Elektronik Bankacilikta Bankalarin Özen Yükümlülüğü

ÖZET

Teknolojinin gelişimi ile birlikte bankacılık işlemlerinde de değişimler yaşanmaktadır. İletişim imkânları, bankacılık işlemlerini kolaylaştırmakla kalmamış bazen de bankacılık sektörünün yapısının değişmesini birlikte getirmiştir. Telefon bankacılığı, internet bankacılığı, mobil bankacılık işlemleri günümüzde daha yaygın bir şekilde kullanılmaktadır. Karşılaştırmalı olarak baktığımızda bir çok ülkelerde faaliyet gösteren bankaların faaliyetlerini internet ortamına taşıdığı ve müşterilerine bankacılık hizmetlerini verdikleri, müşterilerine cep telefonu üzerinden bankacılık işlemlerini yapabilme imkânlarını verdikleri bilinmektedir. Çalışmamızda banka ve müşterilerin aynı anda ve/veya aynı yerde fiziki olarak karşı karşıya gelmeksizin elektronik vasıtalarla ile yaptıkları bankacılık işlemleri olarak ifade edebileceğimiz elektronik bankacılıkta tarafların yükümlülükleri ve sorumlulukları çerçevesinde ağırlıklı olarak bankanın özen yükümlülüğünün incelenmektedir. İnteraktif bankacılıktan elektron paraya doğru ilerlemelerin yaşandığı günümüzde elektronik bankacılıktan kaynaklanan risklerin ve sorumlulukların da ağırlıklı olarak bankalar açısından incelenmesiyle çalışmamız mevcut olan eksikliklerin giderilmesine bir aday olacaktır.

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Sevinc NOVRUZOVA
	Numarası	124133001008
	Anabilim / Bilim Dalı	Hukuk / Özel Hukuk
	Programı	Tezli Yüksek Lisans ( ) Doktora (X)
	Tez Danışmanı	Prof. Dr. Şahin AKINCI
	Tezin İngilizce Adı	---

ABSTRACT

With the development of technology, changes are experienced in banking transactions. Communication facilities not only facilitated banking transactions, but also brought about a change in the structure of the banking sector. Telephone banking, internet banking, mobile banking are more widely used today. When we look at it comparatively, it is known that banks operating in many countries carry their activities to the internet environment, provide banking services to their customers, and give their customers the opportunity to perform banking transactions via mobile phones. In our study, in electronic banking, which can be defined as banking transactions performed by banks and customers at the same time and / or in the same place without physically confronting them, in electronic banking, the responsibility of the bank is mainly examined within the framework of the obligations and responsibilities of the parties. Our study will be devoted to overcome the existing deficiencies by examining the risks and responsibilities arising from electronic banking mainly from the perspective of banks in today's world of advances from interactive banking to electron money.

İÇİNDEKİLER

İKİNCİ BÖLÜM
ELEKTRONİK BANKACILIK HİZMETLERİ VE ELEKTRONİK BANKACILIKTA BANKANIN ÖZEN YÜKÜMLÜLÜĞÜNÜN HUKUKİ NİTELİĞİ, KONUSU, ÖLÇÜSÜ VE UYGULAMA HÂLLERİ

ÜÇÜNCÜ BÖLÜM
ELEKTRONİK BANKACILIKTA BANKANIN ÖZEN YÜKÜMLÜLÜĞÜNÜN İHLÂLİNİN HUKUKÎ SONUÇLARI

KISALTMALAR

ABD : Ankara Barosu Dergisi

AİBÜ SBED : Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi

AÜEHFD : Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi

AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi

AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi

B. : Baskı

BanK : 5411 sayılı Bankacılık Kanunu

BBSEBHY : Bankalarda Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

BHEY : Bankacılık Hizmetlerinin Erişilebilirliğine Dair Yönetmelik

BKartK : 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu

bkz. : Bakınız

C. : Cilt

CBLJ : Canadian Business Law Journal

CLSR : Computer Law and Security Review

Çev. : Çeviren

DAUM : Doğu Anadolu Araştırma ve Uygulama Merkezi Dergisi

Digital Evidence & Elec. Signature Law Rev. : Digital Evidence and Electronic Signature Law Review

E. : Esas

Ed. : Editör

ETDK **:** 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında

eTebliğ **:** Eski Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ

GÜHFD : Gazi Üniversitesi Hukuk Fakültesi Dergisi

HD. : Hukuk Dairesi

K. : Karar

m. : Madde

MHAD : İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi

MÜHF-HAD : Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmları Dergisi

N.C. BANKING

INST. : North Carolina Banking Institute

Nw. J. Tech. **:** Northwestern Journal of Technology and Intellectual Property

& Intell. Prop

Okla. City

U. L. Rev. : Oklahoma City University Law Review

s. : Sayfa

S. : Sayı

SÜHFD : Selçuk Üniversitesi Hukuk Fakültesi Dergisi

T. : Tarih

TBB : Türkiye Bankalar Birliği

TBBD : Türkiye Barolar Birliği Dergisi

TBK : 6098 sayılı Türk Borçlar Kanunu

TKHK : 6502 sayılı Tüketicinin Korunması Hakkında Kanun

TTK : 6102 sayılı Türk Ticaret Kanunu

vd. : ve devamı

Y. : Yıl/Year

Yarg. : Yargıtay

GİRİŞ

Çalışmamızın konusu banka ve müşterilerin aynı anda ve/veya aynı yerde fiziki olarak karşı karşıya gelmeksizin elektronik vasıtalarla ile yaptıkları bankacılık işlemleri olarak ifade edebileceğimiz elektronik bankacılıkta tarafların yükümlülükleri ve sorumlulukları çerçevesinde ağırlıklı olarak bankanın özen yükümlülüğünün incelenmesidir. Çalışmada önce elektronik bankacılığın tanımı, türleri, hukuki niteliği üzerinde durulmakla tarafların yükümlülükleri ve bankanın özen yükümlülüğünün sınırlandırılması şartları ve güvenlik sorunu üzerinde durulmuştur. Elektronik Bankacılıkta Bankanın Özen Yükümlülüğü başlığı taşıyan bu çalışmamızda, "Giriş" ile "Sonuç" bölümleri dışında üç bölüm bulunmaktadır.

Çalışmamızın ilk bölümünde elektronik bankacılığını teknik anlamda altyapısını oluşturan ve ona bağlı temel kavramlara ayrılmaktadır. Bu bölümde ilk olarak, teknik altyapını oluşturan bilgisayar, internet, elektronik posta, dünya çapında ağ, websitesi, alan adı ve sunucu, host, server gibi kavramlar üzerinde durulmaktadır. Daha sonra elektronik ticaret ve elektronik ticaretin türleri hakkında bilgi verilmektedir. Ayrıca söz konusu bölümde sonra elektronik bankacılığın tanımı ver türleri ile ilgili bilgi verilmektedir. Bu bölüm elektronik bankacılığın teknik altyapısını oluşturan temel kavramlar hakkında bilgiler içermekte olup, diğer taraftan bu alanda temel hukuki düzenlemeler hakkında da bilginin verilmesini amaçlamaktadır. Temel teknik altyapını oluşturan kavramlarla birlikte saldırı türleri ve koruma yöntemleri/güvenlik önlemleri hakkında da geniş bilgi verilmektedir. Bu bölümde sistem güvenliğini tehdit eden unsurlar olarak, trojan (truva atı), casus yazılımları (spyware), klavye dinleme sistemleri (keylogger), olta (phising) yöntemi, yanlış alan adına yönlendirme (Pharming/DNS-Spoofing) ve digerleri irdelenmiş, sistem güvenliğini sağlayan yöntemler olarak güvenli yuvalar katmanı, güvenli elektron işlem ele alınmaktadır.

Çalışmamızın ikinci bölümünde elektronik bankacılık hizmetinde bankanın özen yükümlülüğünün hukuki niteliği, konusu, ölçüsü ve uygulama hâlleri hakkında bilgi verilmektedir.

Doktrinde özen yükümlülüğünün bir edim veya yan yükümlülük olarak tanımlaması ilgili görüşlere rastlanmaktadır. Nitekim özen yükümlülüğünün, edim yükümlülüğü olarak nitelendirmek doğru deyildir. Şöyle ki, özen yükümlülüğü sözleşmeye hukuki özelliğini veren yükümlülük değildir. Aynı zamanda, alacaklı özen yükümlülüğünün ihlâli hâlinde ayrıca ifa davası da açabilmek imkânını haiz değildir. Özen yükümlülüğünün edimin ifasının yerine getirilmesinde yardımcı olan yan yükümlülük olarak tanımlamak isabetli olmaz. Zira banka yan yükümlülüklerin ifasını da özenle yerine getirmek durumundadır. Mesela, bankanın bilgilendirme yükümlülüğü bir yan yükümlülük olarak karşımıza çıkar. Ancak banka bilgilendirmeni de özenle yapmak zorundadır. Çalışmamızda özen yükümlülüğünün, diğer yapma yükümlülüklerine eklenerek onların tamamlayıcı bir parçasına çevrilmesi ve bu yükümlülüklerin doğru ifası için gerekli olduğu ölçüde var olmasına ilişkin görüş savunulmaktadır. Şöyle ki, elektronik bankacılık hizmetlerinin sağlanmasına ilişkin banka ve müşteri arasında sözleşme görüşmelerinin başlanmasından itibaren bankanın müşteri karşısında farklı nitelikte yükümlülükleri doğmaktadır. Bu yükümlülükler, edim yükümlülüğü (bankanın şube dışındaki/alternatif dağıtım kanalları aracılığıyla müşteriye elektronik bankacılık hizmetlerini sunmak). Bankanın özen yükümlülüğü, söz konusu borç ilişkisi çerçevesinde bankanın yapma edimi veya yan yükümlülük şeklinde ifa etmesi gereken tüm yükümlülüklerinin sözleşmeye uygun yerine getirilmesi için bir kriter olarak karşımıza çıkmaktadır. Başka bir ifadeyle, bankanın diğer yükümlülüklerini doğru ifa etmesi özen yükümlülüğünü yerine getirilmesiyle sağlanır.

Bankanın özen yükümlülüğünün konusu, müşterilere alternatif dağıtım kanallarını kullanmakla banka hizmetlerine kural olarak, sanal şekilde herhangi bir zaman veya mekân kısıtlaması olmaksızın erişebilme imkânı tanımak için gerekli davranışlarda bulunma ve bu hizmetlerin sağlanmasına ilişkin başarılı sonucu engelleyecek davranışlardan kaçınma olarak ifade edilmiştir. Söz konusu yükümlülüğün ölçüsü değerlendirileren basiretli tacir gibi davranması gerektiği, özel denetime tabi olması, elektronik bankacılık hizmetlerinin teknoloji açısından bünyesinde taşıdığı risklere vakıf olması ve bunlara karşı gereken önlemleri alması gibi hususlar dikkate alınmalıdır.

Bankanın güven kurumu olarak özen yükümlülüğünün ağırlaştırılması değerlendirilirken bankanın elektronik bankacılıkta gerekli güvenlik tedbirlerinin alınmasında basiretli tacir gibi davranması gerektiği Yargıtay uygulamasında ortaya çıkmaktadır.

Bu özen yükümlülüğünün uygulama halleri sözleşme öncesi, sözleşme sırasında ve sonrası aşamalar açısında ele alınarak incelenmiştir. Sözleşme öncesi aşamada bankanın elektornik bankacılıkta bilgilendirmede göstereceği özen ele alınmış, sözleşme sırasında bilgilenirme/uyarma ile beraber gerekli tedbir alma/önlem alma ve sistem aksaklıklarının/hataıarının ve eksikliklerin giderilmesi ile ilgili incelemeler yapılmıştır. Sözleşme sonrası aşamada bankanın özen yükümlülüğü bir koruma yükümlülüğü olan sır saklama yükümlülüğünün yerine getirilmesinde uygulama alanı bulmaktadır. Bankacılık mevzuatı açısından bankaların sır saklama yükümlülüğü hem müşteri sırrını hem dü banka işletmesi sırlarını kapsayacak şekilde kullanılmaktadır. Çalışmamız açısından müşteri sırrı önem arz etmektedir.

Elektronik bankacılıkta özen yükümlülüğüne aykırı davranan bankanın müşteri ile arasında olan sözleşme hükümleri gereğince sorumlu olacağı açıktır. Bu sebepten üçüncü bölümde bankanın sözleşmeden doğan sorumluluğunun şartları, özen yükümlülüğünün ihlâliının sonuçları ve nihayet tarafların ispat külfetine ve kusur kıstasına ilişkin konulara değinilmiştir. Genel olarak elektronik bankacılık sözleşmesinden kaynaklanan sorumluluk müşterinin (alacaklının) ifa etmeme veya özensiz ifa nedeniyle bankaya (borçluya) yönelttiği aynen ifa ve (veya) tazminat talebi şeklinde ortaya çıkar. Çalışmamızda bankanın gereği gibi ifa etmemesi sözleşme ile kararlaştırılmış asli edim borcunun ifasında özensiz davranması şeklinde ele alınmıştır. Gereği gibi ifa etmeme ise, sözleşme ile kararlaştırılmış asli edim borcunun ifasında özensiz davranılması biçiminde görünebilir. Zira "özen" kavramsal olarak daima bir aslî veya yan edimi, davranışı şart koşar. Ancak sözleşme ihlâli sadece aslî edim borcu bakımından değil, yan yükümlülüklerin, özellikle de koruma yükümlülüklerinin ihlâlinden de kaynaklanabilir. Mesela, bilgilendirme veya sır saklama yükümlülüklerinin ihlâlinde olduğu gibi.

Çalışmamızın son bölümünde bankanın yerine getirilmesi gereken edimlere ilişkin gerekli açıklama yapılmakla birlikte elekronik bankacılık hizmetlerinin sağlanmasına ilişkin birçok yükümlülüklerin incelenmesi ele alınmıştır. Şöyle ki, banka güvenli teknik ortamı sağlamalı, teknik ve güvenlikle ilgili güncel gelişmeleri takip etmeli, müşterisini bilgilendirmeli ve uyarmalı, elektronik bankacılık sisteminin kötüye kullanılmasını önleyecek tedbirler almalıdır. Bu edimlerin ifasında gereken özenin gösterilmemiş olması durumunda bankanın sözleşmeye aykırı davranışı çalışmamızda ele alınmıştır. Görüldüğü üzere işteki nitelik eksikliği, borçlanılan edimden sapma özen eksikliği olarak ortaya çıkar. Başka bir deyişle, özenin temelinde yatan şey, bankanın taahhüt ettiği işin gereği gibi sonuçlanması için belirli bir çaba sarf etmesi gereğidir.

BİRİNCİ BÖLÜM

ELEKTRONİK BANKACILIĞA İLİŞKİN TEMEL KAVRAMLAR

§ 1. Teknik Altyapıyı Oluşturan Temel Kavramlar

I. Internet

A. Tanımı ve İşleyişi

Dünya çapında Internetin[1] resmi bir tanımı mevcut değildir. ABD'de 1997 tarihli *Reno v. American Civil Liberties Union* davasında, ABD Yüksek Mahkemesi'nin vermiş olduğu kararda yapmış olduğu tanımlama uyarınca, "*internet, milyonlarca insanın birbirileri ile iletişim kurmasını ve dünyanın her köşesinden gelen akılalmaz hacimdeki bilgilere ulaşmasını sağlar. Diğer bir deyişle internet, tüm dünya sathına yayılmış, eşi benzeri bulunmayan ve tamamen yepyeni olan insani bir iletişim ortamıdır*"[2].

İnternet, dünya üzerindeki bilgisayar ve yerel bilgisayar ağlarını birbirine bağlayan global bir bilgisayar ağları sistemi gibi de tanımlanmaktadır.[3] Dolayısıyla bu sistem birbirinden bağımsız binlerce ağlardan oluşmaktadır ve bu ağlara milyonlarca bilgisayar bağlı bulunmaktadır.

Her bir bilgisayar belleğine yerleştirilen bilgilerden üçüncü kişilerin yararlanmasını sağlamak için bilgisayar ağlarının olması gerekmektedir. Bu tür ağlar

---

[1] Tez çalışmamızda İnternet kelimesi özel isim olduğu için ilk harfi büyük yazılmışdır. Bu kelime ilk kez 1973 yılında Amerika Birleşik Devletler Savunma Konulu İleri Araştırma Projeleri Dairesi (*Defense Advanced Research Projects Agency - DARPA*) tarafından gerçekleştirilmiş *"İnternetting Project"* adı verilen bir araştırmadan esenlenerek ortaya çıkmıştır. Bkz. **Leiner, M. B.,** v.d., "*A Brief History Of The Internet*", Computer Communication Review, Vol. 39, No 5, October 2009, s. 22.

[2] **Sağlam**, **İ.,** Elektronik Sözleşmeler, Legal Kitabevi, İstanbul 2007, s. 31; **Özdilek**, **A. O.,** Internet ve Hukuk, Papatya Yayıncılık, İstanbul, 2002, s. 13; Internet, 7/24 olarak dünyanın her yerinden anında ve rahat erişim sağlanılabilen açık bir pazar olarak tanımlanmaktadır. Bkz. **Pekşirin, H.,** *Modern İletişim Araçları ve Özel Hukuk (İnternette Sözleşme Akdi)*, **Ankara Barosu Hukuk Kurultayı 2000**, C. 3, s. 324.

[3] **Craig**, **B.,** Cyberlaw: The Law of the Internet and Information Technology, Pearson Education, 2012, s. 2; **Alptürk**, **E.,** Elektronik Ticaretin Hukuku Ve Vergilendirilmesi, Kazancı Matbaacılık Sanayi, İstanbul, 2005, s. 109; **Bozbel**, **S.,** "*İnternet Üzerinden Yapılan Hukuki İşlemler ve Bu Konuda 97/7 Sayılı Tüketicinin Korunmasına Dair AT Yönergesi*", **Yargıtay Dergisi,** C. 27, 2001, s. 1-2; **Aksoy**, **R.,** İnternet Ortamında Pazarlama, 2. bs., Seçkin Yayıncılık, Ankara, 2009, s. 31; **Küçükyılmazlar**, **A.,** Elektronik Ticaret Rehberi, İstanbul Ticaret Odası, Yayın No: 2006-3, Şubat 2006, s. 23.

bizlere her hangi bir bilgisayat sistemine girebilmek veya istenilen web sitesini sunabilmeniz için imkân tanımaktadır. Dünyada bu imkânı sunan kuruluşlara İnternet Servis Sağlayıcıları/İSS (*Internet Service Providers*) denilmektedir. İSS'lere ulaşım ise modem aracılığı ile yapılır. Modem telefon sinyallerini bilgiye çeviren bir alet olarak tanımlanmaktadır. Nitekim bundan başka bilgisayarlar arasında bağlantının kurulması için TCP/İP[4] sistemi kullanılmaktadır. İş bununla bitmiyor. İnternet sitelerinin izlenmesi ise önemli bir konudur. Bunun için *"Browser"* (Internet Explorer, Nestcape gibi) denilen internet tarayıcılarına başvurulmaktadır. Bu *"browserler"* aracılığı ile *"HTML"* dili ile yazılan internet sayfaları tercüme edilmektedir. Anlaşılan odur ki, internete girebilmek için onun fiziki altyapısını oluşturan pc, modem, telefon bağlantısı[5] ve internet servis sağlayıcıların[6] bir araya gelmesi gerekmektedir.

B. İnternetin Unsurları

1. Server (Sunucu)

Server dijital bilgileri kapasitesi oranında depo ederek diğer bilgisayarlara hizmet sağlayan programlardır. Serverin esas görevi bilgisayara ait bilgileri manyetik bir ortamda[7] depolamak olduğu için bunlar genellikle kendileri doğrudan internete

---

[4] TCP/İP ile ilgili ayrıntılı olarak İnternetin unsurları bölümünde değinilmiştir.

[5] İnternet, kullanıcılar arasında haberleşme amacıyla bilgi iletişimi sağlayan bir sistemdir ve her ülkenin ilgili mevzuatı çerçevesinde bu sistemin çalışması için ulusal telekomünikasyon idarelerinin kontrolü gerekir ki, belirli telefon hatları ile internet insanlara sunulmuş olsun. Yerel mevzuat çerçevesinde, her bir İSS internete bağlantının sağlanması için yerel telekomünikasyon kuruluşları ile anlaşma yapmak zorundadırlar. Bkz. **Güran S.** vd., İnternet ve Hukuk, Superonline Workshop Metni, İstanbul, 2000, s. 4.

[6] Bu çalışmada "İSS'ler" Internet Servis Sağlayıcılarının kısaltması kullanılmıştır. İnternet hizmeti sunan kuruluşlar olarak kabul ediliyorlar. İSS'lerin kendine ait bir bilgisayat donanımı ve yerel telekomünikasyon şirketinden kiraladığı telefon hatları vardır. İSS'ler her kesin internete bağlanmasını, aynı zamanda üçüncü kişilerle internet üzerinden iletişim kurmalarını ve internetin sağladığı imkânları kullanmaları sağlayan aracı unsurdur. İSS olmadan insanların internete bağlanması imkânsızdır. Bu bakımdan İSS'ler insanlarla internet arasında bir köprü görevini üstleniyorlar. Bkz. **Güngör M./Evren, G.,**, İnternet Sektörü ve Türkiye İncelemeleri, T.C. Telekomünikasyon Kurumu Tarifeler Dairesi Başkanlığı, Ankara, 2002, s. 7; *"Kavramsal olarak tanımlarsak, İSS'ler, kullanıcıların internete erişimini sağlayan ve/veya elektronik hizmetlerin, kullanıcıların kullanımına sunulmasına aracılık eden gerçek veya tüzel kişilerdir."* Bkz. **Soysal**, **T., "**İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", TBBD, S. 61, Y. 2005, s. 310.

[7] *"Sunucu bilgilerin depo edildiği ve yayımlandığı bir manyetik ortamdır."*Ayrıntılı bilgi için bkz. **Tan, D. S.,** Herkes İçin İnternet, Beta Yayınları, İstanbul, 1998, s. 87; **Alptürk**, s. 113; **Sınar, H.**, İnternet ve Ceza Hukuku, Beta Yayınları, İstanbul, 2001, s. 41.

bağlı değillerdir. Bu sebeple server muhafaza ettiği bilgiye ulaşılmasını sağlamak veya bu bilgiyi internet ortamına ulaştırmak için İSS hizmetinden yararlanması gerekmektedir. Kendisinin İSS hizmeti görmesi durumunda server bir İSS olarak çalışmakta ve İSS'lere uygulanan hukukî statüye tabi tutulmaktadır. Bu şekliyle İSS bir server olarak da hizmet vermiş olur[8].

2. Host

Host kelimesi *"ağa bağlı bilgisayarlardan server hizmeti gören ana bilgisayarı ifade etmektedir."*[9] Daha açık ifade edecek olursak, host bilgilerin saklandığı ve internete bağlı bulunan bilgisayar anlamına gelmektedir. Nitekim hosting kelimesi host kelimesinden farklıdır. Şöyle ki, "*başkalarının hazırlamış olduğu içeriği kendi sunucularında depolayabilme ve buradan da doğrudan internet bağlantılarını kullanarak siberuzay ortamına aktarabilme hosting hizmetidir. Başka bir deyişle, hosting, internet ağına sunulan web sayfalarına alan adları yolu ile ulaşılması sırasında web sayfasını kendi bilgisayarında barındırarak alan adının ilgili sayfaya yönlendirilerek ilgili sayfaya ulaşılmasını sağlayan hizmete denilmektedir.*"[10] "*Bir servis sağlayıcının müşterisine ait bir web sayfasını bünyesinde barındırması ve bu sayfaya internet kullanılarak dışarıdan erişilmesini sağlaması da hosting olarak anılmaktadır."*[11]

3. Dünya Çapında Ağ (World Wide Web)

Web denilen World Wide Web (Dünya Capında Ağ) şimdiye kadar oluşturulan en geniş kapsamlı ortam ve çok çeşitli bilgiler toplamından ibarettir. Bu sistem kendisi için özel olarak hazırlanmış olan ve hipertext transfer protokol (http) olarak isimlendirilen protokolü kullanarak bilgilerin transferini sağlar[12]. Hiper ortamın özelliği bir döküman üzerinden başka bir dokümana ulaşılabilmesidir. Bu

---

[8] **Güran v.d.**, s. 11-13.
[9] Daha açık ifade edecek olursak, host bilgilerin saklandığı ve internete bağlı bulunan bilgisayar anlamına gelmektedir. Ayrıntılı bilgi için bkz. **Özel, S.,**, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, Seçkin Yayıncılık, Ankara, 2004, s. 157-158.
[10] **Alptürk**, s. 114; **Soysal**, Servis Sağlayıcıları**,** s. 318.
[11] **Özel**, s. 157-158.
[12] **Alptürk**, s. 35.

sayede internet ortamında hipermetin bağlantısı kullanılmak suretiyle milyonlarca doküman arasında bağlantı kurulması sağlanabilmektedir.

4. Alan Adı (Domain Name)

Alan adı (*domain name*) web sitesinin Internet'teki adı ve adresidir. Alan adı olmadan müşteri bankanın web sitesine ulaşamaz. *"Alan adları IP (Internet Protocol) denilen, bilgisayarların birbirini tanımasını sağlayan numara sisteminin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş kısaltmalardır."*[13] Bu kısaltmalar genellikle, com, net, org gibi kelimelerle bitmektedir. Domain adına örnek olarak www.yapikredi.com.tr, www.amazon.com'u verebiliriz. Görüldüğü üzere, bankaların İnternet bankacılığı hizmeti verebilmeleri için mutlaka bir alan adına ihtiyaç vardır.

5. Web Sitesi

Web Sitesi elektronik bankacılık hizmeti sunan bankalar için internetin en önemli unsurlarından sayılır. Bankaların İnternet bankacılığı hizmeti verebilmeleri için bir web sitesine ihtiyaçları vardır. Web sitesi, bir bilgisayarda depolanan ve diğer bilgisayarlar aracılığıyla okunabilen, dijital forma dönüştürülen veya dijital olarak üretilen metin, hareketli veya hareketsiz görüntü ve seslerden, bunların ikisi veya daha fazlasının birleşmesinden meydana gelen birden çok sayfalardan oluşan içerik sunma aracı olarak tanımlanabilir[14]. Diğer taraftan, web sitesi birbirine bağlı bilgisayarların oluşturduğu bilgi içeren alanlar olarak tanımlanmaktadır. Böylelikle, bir alan adının tahsis edilmesi internet ortamında web sitesine sahibi olmak için temel şarttır[15].

---

[13] **Altan, M.,**, Fonksiyonlar ve İşlemler Açısından Bankacılık, Beta Basım Yayın, İstanbul, 2001, s. 180-181; **Soysal**, Servis Sağlayıcıları, s. 318.
[14] **Oğuz, S.**, "Telif Hakkı İhlallerinden İnternet Servis Sağlayıcıların Sorumlulukları", GÜHFD, C. XII, S. 1-2, Y. 2008, s. 152.
[15] **Oğuz,** s. 152.

6. Elektronik Posta

Elektronik posta, iki bilgisayar arasında elektronik veri değişimini ifade etmekle birlikte, bir bilgisayardan diğerine bu verinin gönderilmesine aracılık eden bir internet servisidir. Elektronik posta "Basit Posta Aktarım Protokolu (Simple Mail Transfer Protocol-SMTP)" kullanılarak, gönderilen iletinin hedeflenen adrese ulaşmasını sağlar[16]. Önceleri sadece haberleşme amacıyla kullanılan elektronik posta ile 1995 yılından itibaren resim, müzik ve dosya gibi elektronik verilerin de eklenerek yollanması mümkün olmuştur[17].

7. TCP/IP

İnternet ortamında bilgi alış verişi ve yahut paylaşımının yapılması için TCP/IP'ye ihtiyaç vardır. TCP/IP aracılığı ile milyonlarca bilgisayarlarda deponlanmış bilgi alışverişlerini etkin bir iletişim şeklinde gerçekleştirmek mümkündür. TCP/IP iletişim protokolüne verilen genel addır[18]. İnternet üzeri aranan istenilen bilgiye erişmek için bu bilgilerin depolandığı bilgisayarlara ve bu bilgisayarlar içindeki alanlara birer internet adrese verilmelidir. Her bir İSS'de yer alan bir sunucu bilgisayara bağlanılmaktadır. Bu sunucu aracılığı ile bilgisayara bağlantı sırasında kullanıcı ismi ve şifreye göre boş olan adreslerden biri (IP numarası) atanır. Bu IP adresi istenilen zaman web sitesine veya e-posta kutusuna bağlanırken kullanılır. Her bağlantıda IP adresinin son numarası değişikliği olur. Nitekim bu değişiklik internet sunucusundaki log kayıtlarında depolanan tarih, IP adresinin bağlı olduğu telefon numarası ile ilgili bilgileri etkilemir. Söz konusu bilgiler değişmeden log kayıtlarında yer almağa devam edir[19].

---

[16] **Soysal**, **T., "**Elektronik Posta Yoluyla Kişilik Haklarına Müdaheleden Doğan Hukuki Sorumluluk", ABD, Y. 65, S. 1, Kış 2007, s. 146.

[17] **Sınar**, s. 22-23; Kendisine mektup gönderilen kişi, bu mektubu elektronik posta kutusundan alıp okuyabilir, yazıcıdan metnini alabilir, diskete kaydedebilir ya da diğer kimselere gönderebilir. Elektronik delil niteliği hakkında bkz. **Keser Berber, L.,** Adli Bilişim, Yetkin Yayınları, Ankara, 2004, s. 126 vd.; E-posta göndericinin bilgisayarı tarafından bir mail server (posta hizmeti sağlayıcı) aracılığıyla alıcının mail serverine iletilir. Alıcının genellikle bir e-posta alma protokolü vardır. Bu yolla ulaşan e-posta, alıcının mail serveri tarafından yine alıcının mailboxuna (posta kutusuna) konur. Bkz. **Bozbel**, s. 760-761.

[18] **Sınar**, s. 21; **Özgür E.,** İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Ankara, 2012, s. 71.

[19] **Ahmet G.**, Doğrudan/Dolayı Bilişim Suçları, Seçkin Yayınları, Ankara, 2016, s. 27.

II. Elektronik Ticaret

A. Tanımı

Elektronik ticaret internetin yaygınlaşmasıyla birlikte yeni bir yöntem değildir[20]. Zira elektronik ticaret sadece internet vasıtasıyla yapılmaz. Eski zamanlardan günümüze insanlar telefon, teleks, telgraf, faks gibi araçlar ile haberleşmekte ve bu araçları ticari gayeler için kullanmaktadırlar. İşte elektornik ticaret kavramının bu araçları kapsayacak şekilde kullanıldığı görülmektedir. Elektronik ticaret genel olarak, *"birey ya da kurumların telekomünikasyon bağlantıları vasıtasıyla, açık ya da kapalı ağlar üzerinden gerçekleştirdiği; metin, ses ve görüntü biçimindeki sayısallaştırılmış verilerin, elektronik ortamda işlenmesi, saklanması, iletilmesi esasına dayanan işlemler bütünü olarak tanımlanmaktadır[21]. Bu durumda "geniş anlamda elektronik ticaret"ten bahsedilmektedir."* [22] 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında[23] Kanun'un (ETDK) 2. maddesinin (a) bendinde gereğince, "*Elektronik ticaret: Fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti*" ifade eder. Diğer taraftan elektronik ticaret kavramı, yalnızca bilgisayar ağları üzerinden gerçekleştirilen ticari faaliyetleri ifade etmek üzere de kullanılmakta ve bu durum ise "dar anlamda elektronik ticaret" olarak nitelendirilmektedir[24].

"*Elektronik ticaret, yazı, ses ve/ve ya görüntü şeklindeki verilerin, elektronik ortamda işlenmesi ve iletilmesi suretiyle gerçekleştirilen ticari işlemlerin bütünü olarak tanımlanabilir."*[25]

---

[20] **Tian, Y./Stewart**, **C.,** "History of E-Commerce", Electronic Commerce: Concepts, Methodologies, Tools, and Applications, Ed. S. Ann Becker, Vol. 1, Information Science Reference, New York, 2008, s. 1 vd.

[21] **Altınışık**, **Ü.,** Elektronik Sözleşmeler, Seçkin Yayıncılık, Ankara, 2003, s. 30.

[22] **İnal, E.,** E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması, Vedat Kitapçılık, İstanbul, 2005, s. 14; **Demir, M.,** Mesafeli Sözleşmelerin İnternet Üzerinden Kurulması, Turhan Kitabevi, Ankara, 2004, s. 119.

[23] 5.11.2014 tarihli 29166 sayılı RG.'de yayımlanmıştır.

[24] **Demir**, s. 119.

[25] Birleşmiş Milletler Uluslararası Ticaret Merkezi (International Trade Center-ITC) tarafından yayınlanan bir rehberde de, elektronik ticaret kavramı,*"mal ve hizmetlerin dağıtım, pazarlama, satış veya tesliminin elektronik araçlarla yapılması"* şeklinde geniş olarak tanımlanmıştır. Bu rehberde, ticari işlemi oluşturan aşamalardan birinin veya hepsinin (pazarlama veya araştırma aşaması, sipariş veya ödeme aşaması, teslim aşaması) internet ortamında gerçekleşmesi halinde elektronik ticaretin söz

Görüldüğü gibi elektronik ticaret kavramı farklı şekillerde dar veya geniş anlamlarda tanımlanabilmektedir. Üzerinde uzlaşılmış tek bir tanımı bulunmamakla birlikte, yapılan tanımlarda ortak noktaya baktığımızda elektronik ticareti telekomünikasyon ağları üzerinden gerçekleştirilen iletişime dayanan ticarî faaliyetler olarak ifade edebiliriz.

B. Türleri

1. Elektronik Ticaretin Konusu Bakımından

Günümüzde her türlü mal ve hizmetin elektronik ticarete konu olması mümkündür: elektronik eşya, bilgisayar programları, belirli konularda (finansal, hukukî, yönetimle ilgili konular vs.) danışmanlık hizmetleri gibi. Mal alımı ve hizmet sunulmasının internet ortamında gerçekleşip gerçekleşmemesine göre doğrudan-dolayı ticaret ayırımı yapılmaktadır.

a. Doğrudan (Dolaysız) Elektronik Ticaret

Doğrudan ticaretin konusu, internet ortamında fiziki mekanla herhangi bir temas olmaksızın ifa edilmeye elverişli olan, gayri-fiziki mal veya hizmetlerdir. Bu bağlamda, bilgisayar programları (software) gibi dijital hâle getirilerek dünya çapında sunulabilen, dağıtılabilen, yüklenebilen, denetlenebilen, kullanılabilen veya kopya edilebilen ürünler (dijital ürün, görüntü, ses, metin) gibi, hukukî veya malî konularda danışmanlık yapılması veya belirli bir konuda bilgi sunulması gibi hizmetler de doğrudan ticarete konu olabilirler.

---

konusu olacağı belirtilmektedir. Dünya Ticaret Örgütü (WTO) de, "*elektronik ticareti, mal ve hizmetlerin satış öncesi, satış ve teslim aşamalarının telekomünikasyon ağları üzerinden yapılması olarak tanımlamaktadır*." Bkz. **Özdemir Kocasakal**, **H.,** Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, Vedat Kitapçılık, İstanbul, 2003, s. 8.

b. Dolaylı Elektronik Ticaret

Elektronik ticaretin konusunun fiziksel bir ürün (bilgisayar, kitap, CD gibi) olması hâlinde dolaylı ticaret söz konusudur. Zira, bu tür ürünlerle ilgili ticarî işlemlerin, ürünün alıcıya teslimine kadar olan aşamalarının tamamının (reklam, pazarlık, sipariş, sözleşmenin kurulması) internet ortamında gerçekleştirilmesi mümkün iken, teslim işleminin internet ortamında gerçekleştirilmesi mümkün değildir. O hâlde dolaylı ticareti, sözleşmenin kuruluşunun (borçlandırıcı işlemin) internet ortamında gerçekleştiği, sözleşmeden kaynaklanan mal ve hizmet teminine ilişkin edimin ise geleneksel yöntemlerle (fiziksel ortamda veya off-line) ifa edildiği ticarî ilişkiler olarak tanımlamak mümkündür.

2. Elektronik Ticaretin Tarafları Bakımından

Aynı zamanda ticari ilişkiye taraf olanların sıfatına göre elektron ticaret aşağıdaki farklı ayrımlara tabi tutulmaktadır:

a. Tacirler Arası (B2B) Elektronik Ticaret

B2B işlemlerin temelinde, genellikle EDI[26] sistemi yer almaktadır. Bunun yanında, elektronik pazar yerleri[27] de tacirler arası işlemlerin gerçekleştirilmesi için bir altyapı sağlamaktadır.

b. Tacirler ile Tüketiciler (B2C) Arası Elektronik Ticaret

Tüketici işlemleri, kişilerin mesleki veya ticari bir amaç gütmeksizin, kişisel veya ailevi ihtiyaçlarını karşılamak amacıyla yaptıkları mal veya hizmet teminine ilişkin işlemlerdir. Tüketiciler, ihtiyaç duydukları mal veya hizmetlerin teminine ilişkin bu işlemleri internet ortamında gerçekleştirebilir, bu bağlamda sipariş verme, satın alma ve ödeme gibi işlemleri gerçekleştirmek üzere internetten

[26] EDI, bilgi ve belgelerin, insan faktörü olmaksızın, bilgisayar ağları yardımıyla, bilgisayarlar arasında otomatik olarak değişimini sağlayan bir sistemdir. Bkz. **Turan, G.,** Elektronik sözleşmeler ve elektronik sözleşmelere uygulanacak Hukukun Tespiti, TBB, S. 77, Y. 2008, s. 91.

[27] Elektronik pazar yerleri, çeşitli işlemlerin, mal veya hizmetlerin tanıtmalarına ve bunları satmalarına veya ihtiyaç duydukları ürünleri satın almalarına imkân veren, ilgili tarafların bağlanabileceği bir web sitesi şeklinde oluşturulan sanal ticaret merkezleridir. **Bkz.** Turan, s. 91.

yararlanabilirler. Meselâ, bir süpermarketin, mağazalarında sunduğu malları, web sitesı aracılığıyla da tanıtması ve ürünlerin satışına imkân tanımasında olduğu gibi. Özellikle, eğlence, seyahat, habercilik, finansal hizmetler ve e-posta gibi nesnel olmayan hizmetlerde tüketici-tacir arası elektronik ticaret daha büyük artış göstermektedir[28].

c. Tüketiciler Arası (C2C) Elektronik Ticaret

Tüketiciler arası elektronik ticarette hem satıcı hem de alıcı bir son kullanıcıdır[29]. Tüketiciler arası ticarî işlemlerin en yaygın görülen örneği, bazen ticaret şirketlerinin de katıldığı, internet ortamında (*on-line*) gerçekleştirilen artırma ile satışlardır. *On-line* açık artırmalar sayesinde, bireyler, ihtiyaç duymadıkları ürünleri satabilme ve kullanılmış (ikinci el) ürünleri satın alabilme imkânına kavuşmaktadırlar.

d. Tacirler İle İdare Arası (B2A) Elektronik Ticaret

Günümüzde resmî birtakım işlemlerin de internet aracılığıyla gerçekleştirilmesi mümkün olabilmektedir. Mesela, kamu kuruluşları tarafından ihale şartnameleri internet ortamında ilan edilmekte ve böylece ihale işlemi başından sonuna kadar internet ortamında gerçekleşebilmektedir[30].

III. Elektronik Bankacılık

A. Genel olarak

Elektronik bankacılık elektronik ticaret kavramının bir alt öğesidir[31]. Elektronik bankacılık, bankacılık ve finans sektöründe etkinliği ve verimliliği önemli

---

[28] **Alptürk**, s. 101.
[29] **Alptürk**, s. 102.
[30] Kamu ihalelerinin internette yayımlanması ile birlikte, firmaların elektronik ortamda teklif vermeleri ve vergi odemelerinin takibi, e-beyan, e-tebligat bu ticaret modeline örnek gösterilmektedir. Bkz. **Alptürk**, s. 101.
[31] **Akkılıç M. E., "**Teknolojik Gelişmelerin Bankaların Dağıtım Kanallarının Yapısı Üzerine Etkileri", DAUM Dergisi, S. 2, Y. 2005, s. 110.

ölçüde artırırken rekabet avantajı yaratacak şekilde müşteri memnuniyetine yeni bir boyut kazandırmıştır. *Basel Komitesi "elektronik bankacılığı hem bireysel, hem de kurumsal bankacılık işlemlerinin elektronik kanallar aracılığıyla yapılması olarak tanımlamıştır."*[32] Elektronik bankacılık bir dağıtım kanalı anlamına gelmektedir. "*Bilgi toplumunun taleplerinin karşılanması, maliyetlerin düşürülmesi, teknolojik rekabet üstünlüğünün sağlanması amacıyla alınan stratejik ve taktiksel kararlar doğrultusunda günümüzdeki tüm teknolojik imkânların bankacılıkta ve bankacılık faaliytlerinde uygulanması sonucu elde edilen ürün ve hizmetler bütünüdür."*[33] Fikrimizce, daha kısa ve net tanımlayacak olursak , elektronik bankacılık, bankacılık hizmetlerinin her türlü elektronik vasıtalar aracılığıyla verilmesi şeklinde tanımlanabilir. Mevzuat açısından baktığımızda elektron bankacılık ilk kez Bankacılık Düzenleme ve Denetleme Kurulu tarafından çıkarılan, 15.03.2020 tarihli, 31069 sayılı RG.'de yayımlanmış Bankalarda Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğinin (BBSEBHY) 3. maddesinin 1. fıkrasının (l) bendinde tanımlanmıştır. Söz konusu madde uyarınca, *"elektronik bankacılık hizmetleri: İnternet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını"* ifade ediyor. Daha kapsamlı tanımlamaya çalışırsak o zaman, elektronik bankacılık BBSEBHY hükümlerini de dikkate alarak bilgi toplumunun taleplerinin karşılanması, maliyetlerin düşürülmesi, teknolojiye dayalı rekabet üstünlüğü kazanılması, stratejik seviyede etkin karar verilebilmesi gibi maddi amaçlar göz önünde bulundurularak, günümüzün teknolojik imkânlarının bankacılık faaliyetleri için uygulanması, geliştirilmesi ve bu çalışmalar sonucunda elde edilen ürün ve hizmetler bütünüdür.

Konunun daha iyi anlaşılabilmesi için elektronik bankacılık türlerinin kısaca incelenmesi gerekmektedir.

---

[32] Ayrıntılı bilgi için bkz. Risk Management Principles for Electronic Banking issued by Basel Commitee on Banking Supervision, (2003), http://www.bis.org/publ/bcbs98.pdf (son erişim tarihi: 30.01.2021).

[33] **Erol İ./Çınar S./Duramaz S.**, "Bankaların Yeni Gelir Kaynağı: Elektronik Bankacılık İşlem Ücretleri, Türk Bankacılık Sektöründe Banka Karlılığı Üzerindeki Etkisi", AİBÜ Sosyal Bilimler Enstitüsü Dergisi, C. 15, S. 2, Y. 2015, s. 3.

B. Türleri

Elektron bankacılık kapalı ve açık olmak üzere ikiye ayrılıyorlar. ATM ve POS bankacılığında kullanılan kanal kapalı olarak nitelendiriliyor ve buraya erişim üyelik koşulları anlaşması ile bağlı olan katılımcılarla (tüketici, banka, tacir ve üçüncü şahıs hizmet sağlayıcı) sınır tutulur. Açık ağlarda ise durum farklıdır.Müşterilere elektron bankacılık hizmetleri yaygın olarak kullanılan erişim aygıtları, telefon, bilgisayar, akıllı kartlar aracılığı ile sunulur.[34] Bilgi teknolojilerinin desteklediği elektronik bankacılık; "*EFT (Electronic Funds Transfer)*[35]*, ATM (Automated Teller Machine) ve POS (Point of Sale) makineleri, çağrı merkezleri, kredi kartları, telefon bankacılığı, kiosk bankacılığı, WAP bankacılığı (Wireless Application Protocol), Palm bankacılığı ve internet bankacılılığı gibi yeni dağıtım kanallarını ve ürünleri içermektedir"*[36]. Türkiye Bankalar Birliği'nin, *"elektronik bankacılığı aşağıdaki gibi sıraladığı görülmektedir*[37]*: ATM; Telefon Bankacılığı; İnternet Bankacılığı; WAP Bankacılığı; Palm Bankacılığı; SWIFT."*

Diğer taraftan, elektronik bankacılık (*Electronic Banking*) Ev ve Ofis Bankacılığı (*Home and Office Banking*)[38], Telefon Bankacılığı (*Telephone Banking*),

---

[34] **Yüksel-Mermod**, **A.,** Finansal Küreselleşme Işığında Elektronik Bankacılık ve Riskler, Beta Yayınevi, İstanbul, 2011, s. 63.

[35] Borcun ifasının fon transferi olarak kullanılması halinde direkt bir ödeme aracı hizmeti olarak kabul olunmamakta, sadece paranın alacaklıya naklinde bir vasıta olarak kullanılmaktadır. Bkz. **Muzaffer Şeker,** Elektronik Ödeme Sistemleri, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl:10, Sayı 20, Güz 2011, s. 64

[36] **Kolodinsky, M. J./Hogarth, M. J./Hilgert, M.A.**, "The adoption of electronic banking technologies by US consumers", International Journal of Bank Marketing, Vol. 22, Issue 4, 2004, s.238-241.

[37] **Yurttadur, M./Süzen, E.,** "Türkiye'de Banka Müşterilerinin İnternet Bankacılığına Yaklaşımlarının İncelenmesi Üzerine Bir Uygulama", Tüketici ve Tüketim Araştırmaları Dergisi, C. 8, S. 1, Y. Haziran 2016, s. 99 vd.

[38] "*Ev ve ofis bankacılığı, ilk defa 1980'li yılların başında Amerika'nın en büyük bankaları (Citibank, Chase Manhattan, Chemical and Manifactured Hanover) tarafından hayata geçirilmiştir. 1980'lerde Avrupa ve A.B.D.'de bankacılık ve finans kuruluşları ev ve ofis bankacılığı kavramı üzerine programlar yapmaya başlamış, başlangıçta bilgisayar ağının çok fazla gelişmiş olmamasından dolayı müşterilere yardımcı olmak üzere faks makineleri ve telefonlar kullanılmıştır. Ev ve ofis bankacılığı, müşterilerin evlerine veya işyerlerine bankadaki hesapları ile doğrudan işlem yapmalarına imkân veren banka bilgisayarı ile bağlantılı elektronik bir hattın bağlanmasıdır. Burada müşterinin kendi bilgisayarına kurulu olan bir banka programı ile de elektronik hattın kendi bilgisayarı ile bağlantılı elektronik bir hizmettir.Görüldüğü üzere bilgisayar kullanımının henüz yaygınlaşmadığı ve internet bağlantılarının olmadığı dönemlerde oluşturulan ve kişisel bilgisayarların (PC) kablolu olarak bankanın otomasyon sistemine bağlanması esasına dayanan öncü bir dağıtım kanalıdır. Nitekim teknolojinin gelişimiyle yerini internet bankacılığına terk etmiş bulunmaktadır."* Bkz. **Yüksel-Mermod**, s. 74.

Televizyon Bankacılığı[39] (*Television Banking*), Kablosuz Uygulama Protokolü (*Wireless Application Protocol -WAP*) Bankacılığı, Avuç içi (*Palmtop*) Bilgisayar Bankacılığı, Kabin (*Kiosk*) Bankacılığı, Kısa Mesaj Servisi (*SMS - Short Message Service*) Bankacılığı ve Internet Bankacılığı (*Internet Banking*) şeklinde sekiz ana gruba ayrılmaktadır[40]. Söz konusu elektronik bankacılık türlerine aşağıdaki sırasıyla kısa olarak değinmekte fayda vardır.

1. ATM Bankacılığı

Eskiden uygulamada elektronik bankacılık denilince ilk önce akla ATM[41] bankacılığı gelmekteydi. Ancak şu anki dönemimizde elektronik bankacılık bununla sınırlı değildir. Türkiye'de ilk kez İş Bankası tarafından 1982 yılında ATM bankacılık hizmeti verilmiştir.[42] BBSEBHY'nin Altıncı bölümü ATM Bankacılığı ile bağlı hükümleri düzenlemektedir.

2. Telefon Bankacılığı

Telefon bankacılığı, elektron bankacılık türlerinden biri olup, banka ile müşterisi arasındaki işlemlerin iletişim aracı olarak telefon üzerinden gerçekleştirilmesidir. Bu tür işlemlerin gerçekleştirilmesinde üç teknolojik yöntem[43] kullanılmaktadır.

---

[39] "*1994'te ABD ve 1997'de Avrupada başlayan dijital yayınla beraber tüm dünyada bankalar kendi bankacılık ürünlerini ve hizmetlerini televizyon aracılığıyla sunabilme yönünde çalışmalara başlamışlar. Dijital TV'nin ana ünitesi sayılan set topbox'ların bir işlemci hafızaya sahip küçük çaplı birer birer bilgisayar olmaları esasına dayanan sistemden yola çıkılarak, işlemler internet bankacılığında olduğu gibi gerçekleştirilmektedir."* Bkz. **Yüksel-Mermod**, s. 74.

[40] **Yılmaz**, **D.** s. 57; Elektron Bankacılığın türleri sırasında Satış Noktası Terminali (POS), Kredi Kartları, Akıllı Kartlar, Akıllı Telefonlar da dahildir. Bkz. **Mikhaylichenko**, **K.,** "Finansal Hizmetlerin Küreselleşmesine Katkı Açısından Elektronik Bankacılık", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, İstanbul, 2015, s. 16.

[41] ATM'ler 7/24 müşterilerine hizmet veren otomatik vezne makineleri olarak kabul olunmaktadır. Doktrince kabul gören tanım gereğince, "*ATM'ler üzerlerindeki bilgisayar ve bu bilgisayarları çalıştıran işletim sistemi aracılığı ile bankanın ana bilgisayarı ile iletişim kurarak müşterilerin bankacılık sistemindeki hesaplarına ulaşmalarını ve bu hesapları üzerinden standart bankacılık işlemlerini kendi kendilerin yapmalarını sağlamaktadır*."**Yüksel-Mermod**, s. 57; **Distançionnoe Bankovskoe Obslujivanie**, Çentr İssledovaniy Platejnıx Sistem ve Rasçetov, KNORUS Yayınevi, Moskva, 2010, s. 15; **Erol/Çınar/Durmaz**, s. 4.

[42] **Yüksel-Mermod**, s. 73.

[43] **Distançionnoe Bankovskoe Obslujivanie**, s. 13-14.

Bunlardan ilki, müşterilerin banka çalışanı ile canlı irtibat kurmadan telefonun tuşlarıyla[44] irtibata geçmesidir. Bu tür yöntem tamamen mekullanmak suretiyle bankacılık işlemlerini gerçekleştirmektedir. Telefon bankacılığını diğer geleneksel kanallardan ayıran en önemli özellik, tamamen mekanik bir sisteme dayalı olması ve müşterilerin karşı taraftan canlı bir müşteri temsilcisiyle irtibat kurmadan telefonun tuşlarıyla işlem gerçekleştirebilmesidir[45].

İkinci yöntemde telefon tuşları yerine müşterinin sesi ve verdiği cevapları tanıyabilen bilgisayarlar kullanılmaktadır. Başka sözle, bilgisayardaki ses kayıtlarına göre müşterinin sesinin ayırt edilmesi ve yahut tanınması yapılmaktadır. Üçüncü yöntemde ise her bir telefon tuşuna uygun bir bankanın hizmeti ile ilgili menyu yer almaktadır. Müşteri kendi telefonunun tuşlarını kullanarak istediği bankacılık hizmetinden yararlanmak seceneğine sahiptir[46].

Buna göre telefon bankaçılığı[47] müşteri banka şubesine gitmeden telefon kullanarak, bankacılık işlemlerini[48] 7 gün 24 saat yapabilmelerini sağlayan elektronik bankacılık türüdür. BBSEBHY'nin 3. maddesinin 1. fıkrasının (l) bendinde yer alan elektron bankacılık hizmetlerinin tanımı çerçevesinde ele alırsak, "*telefon bankacılığı müşterilerin uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektron dağıtım kanalı olarak*"

---

[44] "*Bu aramanın tuşlu telefon kullanılmak suretiyle yapılması gerekmektedir. Daha doğru bir ifade ile göndermeli olarak bu işlemin yapılması gerekmektedir. Bilindiği gibi telefon tuşlarına her basılmada farklı bir ton sesi duyulmaktadır. Bu farklı tonlar, farklı elektronik komutlara ayarlanmakta ve bankanın bilgisayarına bu surette talimat verilmektedir. Eski teknolojide çevirmeli telefon olarak bilinen ve tuşlu telefonlarla da gerçekleştirilebilen "pulse" olarak ifade edilen gönderme şekli ise vuruşlu olarak çalışır. Bu sistem ile bilgisayarı kontrol etmek mümkün değildir."* Bkz.: **Savaş**, **A.,** "İnternet Bankacılığı ve Tarafların Yükümlülükleri", SÜHFD, C. 19, S. 2, Y. 2011, s. 141.

[45] Banka, müşteriye bu hizmetden yararlanmak için bir müşteri numarası tahsis etmektedir. Numara ile beraber şifre bilgisi de banka işlemlerinin yapılması için müşteriye iletilmelidir. Mevduat sahibi, müşteri numarası ve şifresini güvenli bri şekilde sakladığı müddetçe hesabından başkalarının işlem yapabilmesi mümkün değildir. Bkz. **Çeker, M.,** "İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden Bankaların Sorumluluğu (Yargıtay 11. Hukuk Dairesi'nin Bir Kararı Münasebetiyle)", Prof. Dr. Hüseyn Ülgen'e Armağan, C. 2, Vedat Kitapçılık, İstanbul, 2007, s. 1337.

[46] **Tamer, S.,** Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi, TBB Yayınları, İstanbul, 2001.

[47] Kişisel bankacılık 1990'ların ortalarında telefon bankacılığı ile tanışmıştır. Türk bankacılık sektörü ise telefon bankacılık uygulamalarını 1996 yılından itibaren uygulamaya başlamıştır. Bkz. **Aksoy, E. E.,** "İşadamlarının Elektronik Bankacılık Kullanma Durumları ve Karşılaşılan Problemler", Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, 2007, s. 48.

[48] Müşteri tarafından hesap işlemleri, para transferleri, yatırımlar, döviz işlemleri, kredi kartı işlemleri, hisse senedi, hizmetler hakkında bilgi almak ve bilgi güncellemesi işlemleri yapılabilmektedir.

ifade ediliyor. BBSEBHY'nin Dördüncü Bölümü telefon bankacılığında kimlik tanıma ve doğrulama, işlem güvenliği ve hizmet kalitesi gibi konuları düzenlemektedir.

3. Mobil Bankacılık

Mobil bankacılık elektron bankacılık türlerinden biri olup, kartlı ödeme sisteminden mobil ödeme sistemine geçişin göstergesidir.

Mobil Bankacılık üç değişik şekilde karşımıza çıkmaktadır: kısa mesaj servisi (SMS) yoluyla müşterinin bilgilendirilmesi; Kablosuz Uygulama Protokolü (Wireless Application Protocol - WAP) destekleyen cep telefonları yoluyla internet üzerinden işlemlerin yapılması; palmtop (avuç içi) bilgisayar ile internet üzerinden işemlerin yapılması[49].

SMS bankacılığı hizmetler genel olarak banka hesabı üzre bakiye bildirimi, kur bildirimi, hesap hareketlerinde uyarı, kredi kartı son ödeme tarihi, hesap kesim tarihi, borç tutarı, kredi kartı limit azalması durumunda uyarı, kredi kartı borç ödeme günü geciktiğinde uyarı, vadeye bağlı tüm ürünlerin hesaba dönüşünde uyarı, verilmiş emirlerin gerçekleşmemesi durumunda uyarı, banka kartı ile para çekildiğinde uyarı, kredi kartı ile nakit avans çekildiğinde uyarı şeklinde ifade edilebilir[50].

Diğer bir tür olan wap bankacılığı ise wap teknolojisi temeline (veya kablosuz uygulama protokolüne) dayalı olarak internet üzerinden bankacılık işlemlerinin yapılmasıdır[51]. Kablosuz Uygulama Protokolü (*Wireless Application Protocol/WAP*) ile günlük döviz kuru, repo oranları, yatırım fonu fiyatları, altın fiyatları, mevduat faiz oranları, hazine bonosu faiz oranları, hesap bakiyeleri ve kredi kartı borcu görüntüleme şeklinde bankacılık hizmetleri yapılabilmektedir. WAP bankacılığı ile

---

[49] Bkz. **Mobil Ödeme Hizmetleri**, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 2015, s. 24 vd.

[50] **Yıldırım**, s. 96; **Distançionnoe Bankovskoe Obslujivanie,** s. 30.

[51] **Distançionnoe Bankovskoe Obslujivanie,** s. 31; "*Kablosuz uygulama protokolü (WAP) mobil cihazlar üzerinden Internet'e erişim sağlayan kablosuz iletişim standardıdır. Bir başka açıdan WAP, GSM destekli cep telefonu kullanıcılarına Internet erişimi hizmeti sağlayan kablosuz iletişim uygulama protokolüdür. WAP ile sunulan hizmetler arasında tüketiciye ve kurumlara yönelik; bankacılık, elektronik ticaret, elektronik posta, kurumsal bilgi, spor ve bilgilendirme servisleri, eğlence, televizyon/sinema, seyahat, kültür ve sağlık hizmetleri sayılabilmektedir."* Bkz. **Altan**, s. 59.

genellikle bilgilendirme amaçlanmakla birlikte, kredi kartı borcu ödeme, EFT ve fatura ödemeleri de yapılabilmektedir[52].

Palmtop (avuç içi) bilgisayar, üzerinde Palm OS işletim sistemi olan bilgisayar cihazlarına verilen isimdir. Avuç içi bilgisayarlarda bilgi girişi kaleme benzeyen ancak yumuşak bir ucu olan plastik bir çubukla yapılır. Çubuk, cihazın dokunmaya duyarlı ekranına tıklamakta veya bir şeyler çizmekte kullanılır. Avuç içi bilgisayarlar Windows, Macintosh, Linux gibi programlara bağlanabilir ve üzerindeki tüm bilgi desktop bilgisayarınıza kısa bir sürede aktarılabilir (backup)[53].
BBSEBHY'nin 3. maddesinin 1. fıkrasının (çç) bendi uyarınca, *"mobil bankacılık: Akıllı telefon veya tablet gibi mobil bir cihaz üzerinde yüklü, bankaya ait mobil uygulama üzerinden müşterilerin bankacılık işlemlerini gerçekleştirebildikleri özelleşmiş internet bankacılığı dağıtım kanalı"* olarak tanımlanıyor. BBSEBHY'nin Üçüncü Bölümü mobil bankacılıkta kimlik doğrulama ve işlem güvenliği gibi konuları düzenlemektedir.

4. Kabin (Kiosk) Bankacılığı ve Görüntülü Ödeme Makineleri

Kabin (Kiosk), bankalar tarafında kurulan bir merkez olup, müşterilere interaktif bankacılık hizmetlerin sunulmasina yönelmiştir. Bu tür kabinler ATM tasarımında kurulmaktadır. Normalde ATM'ler gibi açık havada, AVM'de ve genel ortamlarda kuruluyorlar. Bu kabinler aracılığı ile müşteriler hem aktif (*para yatırma, para çekme, döviz işlemi vd)*, hem de pasif bankacılık (*hesab bakiyesi inceleme talebi, hesap bakiyesi sorma, kişisel bilgi değişikliği talebi vd*) işlemlerini yapa biliyorlar.[54]

BBSEBHY'nin 3. maddesinin 1. fıkrasının (l) bendinde yer alan elektron bankacılık hizmetlerinin tanımı çerçevesinde ele alırsak, "*kabin (kiosk) bankacılığı kiosk cihazları ile müşterilerin uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektron dağıtım kanalı olarak*" ifade ediliyor. Kabin (Kiosk) Bankacılığı ile ilgili konular BBSEBHY'de özel hükümlerle değil, elektronik bankacılık hizmetlerine ilişkin ortak hükümlerle

[52] **Altan,** s. 59.
[53] **Altan**, s. 430.
[54] **Distançionnoe Bankovskoe Obslujivanie,** s. 47.

düzenlenmektedir. Ortak hükümler kimlik doğrulama, işlem güvenliği, müşterilerin bilgilendirilmesi, işlem güvenliği ile ilgili olup, BBSEBHY'de elektronik bankacılık türü olarak belirlenen kabin (kiosk) bankacılığına da uygulanmaktadır.

5. Satış ve Hizmet Noktası (POS) Bankacılığı

Satış ve Hizmet Noktası (Point of Sale - Service/POS) bankacılık türünde alınan mal ya da hizmetin karşılığının para yerine banka kartıyla ödenmesi ve üye işyerinde bulunan bir cihaz tarafından sağlanmakta; kart bilgileri değerlendirilerek, satış noktasına elektronik olarak para aktarılmaktadır. Bu cihazlar üye iş yerlerine bankalar tarafından verilmektedirler.[55]

6. Kredi Kartları

Banka tarafından müşteriye nakit para yerine almış olduğu mal ve yahut hizmetin ödemesini gerçekleştirmesi için verilen bir finansal araçtır[56].

7. Internet Bankacılığı

"Internet bankacılığı, banka müşterilerinin nakit çekme dışında her türlü bankacılık işlemlerini internet üzerinden yapabilmesini sağlayan elektronik bankacılık türlerinden biridir."[57] İnternet bankacılığının kullanılması için banka ve müşteri arasında yapılacak sözleşme ile banka müşterisine, internet şubesinde

---

[55] **Mikhaylichenko**, s. 27; Elektronik bankacılıkta kullanılan EFTPOS sistemleri, genel alanlarda yerleştirilen terminaller aracılığıyla banka ile bağlantı kurulmasına ve alınmış malın bedelinin ödenmesine imkân sağlamaktadır. EFTPOS ile ATM'ler arasındaki fark da kendisini bu noktada göstermektedir. Zira ATM'ler, nakit para ihtiyacını gidermenin yanı sıra, esas itibariyle, daha önceki tarihte gerçekleşmiş işlemlerle ilgili ödemelerin yapılmasını sağlamaktadır. Bkz. **Arkan**, **S.,** Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukuki Sorunlar, TBB Yayınları, Ankara, 1991, s. 25.

[56]**Mikhaylichenko**, s. 17.

[57] İnternet bankacılığı ilk kez ABD'de ortaya çıkmış ve 1995 yılından itibaren gelişmeye başlamıştır. Bankaların ülkenin farklı eyaletlerinde kendi şubelerini açma konusunda karşılaştıkları sorunlar internet bankacılığının ABD'de ortaya çıkmasının temel sebebini oluşturmuştur. İlk kez "*Security First Network Bank"* ağ aracılığıyla müşterilerine hizmet sağlamaya başlamıştır (**Distançionnoe Bankovskoe Obslujivanie,** s. 20).

oturum[58] açabilmesi için müşteri numarası ve şifre verilir. İnternet bankacılığı bankanın websitesi aracılığı ile müşterilere sunulur. Müşteri, kendisine banka tarafından verilmiş müşteri numarası ve şifreyi bankanın web sitesindeki ilgili alanlara girmelidir[59]. Bu veriler web sunucusunda tutulan verilerle karşılaştırılır. Bu veriler web sunucusunda tutulan verilerle aynı değilse, hatalı işlem raporu web sitesi üzerinden müşteriye bildirilir.[60] *"İnternet bankacılığı kapsamında müşteri, kendi hesapları arasında para aktarma (virman), aynı bankadaki başka kişilere ait hesaplara havale çıkarma, hesab bulunmayan kişilerin adına havale gönderme ya da başka bankalardaki hesaplara EFT çıkarma, otomatik ödeme talimatı verme, düzenli havale talimatı, trafik cezası veya vergi borcu ödeme, kredi kartı başvurusunda bulunma, kredi kartı borcunu öğrenme ve ödeme, vadeli, vadesiz, yerel veya yabancı döviz tevdiat hesabı açma, döviz alıp satma, hisse senedi ve yatırım fonu işlemi yapma, şifre ve adres, telefon gibi kişisel bilgilerinde değişiklik yapmak gibi dilediği işlemi yapma imkânına kavuşur."*[61] Bir başka deyişle, müşteri banka tarafından ona tahsis edilen parolayı internet bankacılık sayfasına girerek dâhil edir ve işlemini kendi iradesiyle yapmak istediğini beyan etmiş olur ve aynı zamanda yapmış olduğu işlemin sonuçlarından şahsen sorumludur[62]. Internet bankacılığında kullanıcı olan müşteri banka çalışanı gibi düşünülebilir, fakat banka çalışanı tüm müşteri bilgilerine ulaşabilirken kullanıcı sadece sisteme tanımlı kendine özgü bilgilere ulaşa bilir ve işlem yapabilir[63].

---

[58] BBSEBHY'ın 3. maddesinin 1. fıkrasının (dd) bendi uyarınca, *"Oturum: veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı"* ifade eder.

[59] Bankalar sisteme giriş için kimlik doğrulamada, yetkisiz kimselerin işlem yapmasını engellemek için kullanıcı adı ve parolanın tek kullanımlık parolaya da ek bir unsur olarak yer vermektedirler. BBSEBHY'ın 3. maddesinin 1. fıkrasının "jj" bendi gereğince, *"Tek kullanımlık parola: kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele yaratılan alfabetik ve/ve ya rakamsal karakterler dizisini"* ifade eder.

[60] "*Genellikle bankalar güvenlik gerekçesiyle, müşterinin kullanıcı adı ve parolalarını üç kez yalnış girmeleri halinde, internet şubesi girişini bloke ederler ve onları yeni kullanıcı adı ve parolalarını almak üzere, bankaların fiziki şubelerine yönlendirirler.Web sunucusunda tutulan verilerle müşterinin girdiği veriler aynı ise müşterinin bir sonraki aşamaya geçerek internet bankacılığı hizmetlerinden yararlanmasına izin verilir."* Bkz. **Yılmaz**, s. 33-34.

[61] **Mustafa Çeker**, "İnternet Ortamında Yapılan Usulsüzlüklerden Bankaların Hukuki Sorumluluğu (Yargıtay 11. Hukuk Dairesi'nin Bir Kararı Münasebetiyle)", Prof. Dr. Bilge Öztan'a Armağan, Ankara, Seçkin Yayıncılık, 2008, s. 249.

[62] **Çeker**, Sorumluluk, s. 251.

[63] **Taner Kaya**, "İnternet Bankacılığı", Bilişim ve Hukuk Dergisi (Ankara Barosu), S. 9, Y. 2008, s. 32.

"*Banka sözleşmelerinde internet bankacılığı, şahsın (tüketicinin) kablolu, kablosuz iletişim sistemleri ile teknik şartları haiz bilgisayar (avuç içi dizüstü) GSM, telefon gibi araçlar üzerinden ve Internet-Wap aracılığı ile otomatik, sesli cevap sistemi ile şifreyi ve parolayı kullanarak, bankanın belirleyeceği kurallar ve limitler dahilinde şahsın banka hesapları üzerinde her türlü işlem yapma yöntemi olarak tanımlanmaktadır."*[64] BBSEBHY'nin 3. maddesinin (r) bendinde[65], " *İnternet bankacılığı: Bankaların kendi ticaret ünvanı, işletme adı ya da herhangi başka bir ad altındaki bir web sayfası üzerinden sundukları hizmetlere müşterilerin, kullandıkları cihaz ya da platformdan bağımsız olarak internet yoluyla ulaşabildiği ve kendilerine ait finansal veya kişisel verileri görüntüleyebildiği, değiştirebildiği ya da finansal sorumluluk yaratacak işlemler gerçekleştirebildiği elektronik dağıtım kanalları*" olarak tanımlanıyor ve elektronik bankacılık hizmetlerinden biri olarak kabul ediliyor.

8. Açık Bankacılık Servisleri

"Açık bankacılık" yapısı son yıllarda müşterilere kendilerine ait finansal verileri aynı anda tek ekrandan görebilmesini ve buna uygun işlem yapmasını sağlamaktadır.[66] Açık bankacılık, en basit anlatımı ile üçüncü kişi hizmet sağlayıcılara, kullanıcıların izinleri dahilinde finansal bilgilerine erişmelerini ve işlem gerçekleştirebilmelerini sağlayan güvenli bir yöntem olarak tanımlanabilir. Söz konusu sistem müşteri bilgilerine erişen üçüncü kişi hizmet sağlayıcılar tarafından müşteriler için yeni finansal ürün ve hizmetlerin geliştirilebilmesi, finansal ürün ve

---

[64] **Naci Özdamar**, "İnternet Bankacılığı ve Banka Kartları", Bilişim ve Hukuk, Ankara Barosu Uluslararası Hukuk Kurultayı, C. 2, Y. 2008, s. 67; **Muktedir Lale,** "İnternet Bankacılığında Hukuki Sorumluluk", Terazi Hukuk Dergisi, S. 42, Şubat 2010, s. 22.

[65] Söz konusu Yönetmeliğin kabulü ile Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ yürürlükten kalkmıştır. eTebliğ hükümlerinde internet bankacılık daha dar anlamda tanımlanmışdır. eTebliğ'in 3.maddesinin 1. fıkrasının (ö) bendi uyarınca, "*İnternet bankacılığı: müşterilerin banka tarafından sunulan hizmetlere internet yoluyla ulaşmalarını ve yapmak istedikleri işlemleri gerçekleştirmelerini sağlayan bankacılık hizmeti dağıtım kanalı*" olarak tanımlanıyordu.

[66] Ama artık COVID-19 bunun "gündemdeki bir konu" olmaktan çok daha fazlasını hak ettiğini göstermiş oldu. Özellikle bugün dünya genelinde yaşanan COVID-19 salgını, finansal ürün ve hizmetlerin evden çıkmadan ve hatta fiziki olarak parayla temas dahi etmeden erişilebilecek bir yapıya büründürülmesi gerekliliğini insanlığa tecrübe ile ispat ederek, bunun kuramsal değil hayati bir ihtiyaç haline geldiğini açıkça ortaya koymuş oldu. Bkz. PWC: Açık Bankacılık - Dünya ve Türkiye, Raporu, 2020, s. 2.

hizmetlere ilişkin şeffalık ve rekabetin artırılması ve böylece müşteriler için finansal hayatın kolaylaştırılması ve müşteri deneyiminin artırılması hedefler.

Açık bankacılığın nasıl çalıştığını iyi anlamak için ilk önce açık bankacılığın uygulanabilmesini sağlayan güvenli aracılardan yani **Uygulama Programlama Arayüzü**'ne (*Application Programming Interface*, "**API**") değinmekte fayda vardır. API, en kısa şekilde "*iki uygulamanın birbiriyle iletişim kurmasını sağlayan aracı bir yazılım*" olarak tanımlanabilir. Finansal hizmetler sektörü açısından ise API, "*belirli bir finansal kuruluşun internet sitesinde geliştirilen bir uygulamanın, kodlar ve kullanıcı bilgileri gizli kalacak şekilde, üçüncü kişi hizmet sağlayıcılara ait farklı programlar tarafından kullanılabilmesini sağlayan bir teknoloji*" olarak karşımıza çıkar. Ancak gerekli kullanıcı bilgileri ve şifrelerinin üçüncü kişiler ile paylaşması gereksinimi dikkate alarak veri güvenliğinin ihlâli ve bankaların sahte işlemleri ayırt etmesinin güçleşmesi gibi önemli güvenlik sorunları da ortaya çıkabiliyor[67]. Gerçi buna rağmen pek çok ülkede bu yöntem finansal hizmetler için dahi kullanılmaya devam ediyor[68]. Bununla birlikte BBSEBHY'nin 3. maddesinin 1. fıkrasının (a) bendinde **açık bankacılık servisleri** "*Müşterilerin ya da müşteriler adına hareket eden taraların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalı*" olarak tanımlanıyor ve elektronik bankacılık hizmetlerinden biri olarak kabul ediliyor. Bunun doğal bir sonucu olarak da elektronik bankacılık hizmetlerine ilişkin PSD2[69]'ye bağlı RTS kapsamındaki

---

[67] Bkz. PWC: Açık Bankacılık – Dünya ve Türkiye, Raporu, 2020, s. 4.

[68] Açık bankacılık ilk kez Birleşik Krallığ'ta kullanılmaya başlamıştır. Açık bankacılık alanında İngiltere'de rekabetin ve tüketicinin korunması konusundaki otorite olan *Competition and Markets Authority* (CMA) tarafından kurulan *Open Banking Implementation Entity* (OBIE) aracılığıyla 2018 yılı itibariyle mevzuatsal yenilikler getirildi. Açık bankacılık hizmetinin yaygınlaşabilmesi için, bankalar tarafından veri paylaşılması, Avrupa Birliği'nde olduğu gibi açık bankacılık alt yapısının düzenlendiği Japonya ve Meksika gibi bazı ülkelerde de zorunlu tutuluyor. Bununla birlikte ABD, Çin, Arjantin, Singapur, Hong Kong ve Güney Kore gibi ülkelerde teşvik edilmeye rağmen açık bankacılık alanında standartlara uyma gibi bir zorunluluk öngörülmüyor. Paylaşım için kullanılacak olan API ve benzer kanallara ilişkin standardizasyon konusunda ise Fransa, Almanya, Polonya gibi bazı Avrupa Birliği üyesi ülkelerin kendi standartlarını oluşturarak Birleşik Krallığı takip ettiğini görüyoruz. **Bkz.** PWC: Açık Bankacılık – Dünya ve Türkiye, Raporu, 2020, s. 8.

[69] "*Ödeme hizmetlerine ilişkin 2009 senesinde Avrupa Birliği ile İzlanda, Norveç ve Lihtenştaynda uygulanmaya başlayan 2007/64 sayılı Avrupa Birliği Ödeme Hizmetleri Direktifi ("PSD1") ile ödemeler alanında bankalara rakip olacak ödeme hizmeti sağlayıcılarının mevzuatsal dayanağı oluşturulmuştu. PSD1'in kapsamını geliştiren PSD2 ise 12 Ocak 2016 tarihinde yürürlüğe girerek*

kurallara benzer kimlik doğrulama, işlem güvenliği, dolandırıcılık riskine karşı işlemlerin takibi ve müşterilerin bilgilendirilmesi gibi kuralların tamamı açık bankacılık servisleri açısından da geçerli hâle gelmiş oldu. Ancak PSD2'den farklı olarak bu düzenleme ile yalnızca bankalara yükümlülükler getirildiği için, açık bankacılık hizmet sağlayıcılarının uyması gereken yükümlülükler bakımından henüz mevzuatta bir belirleme yapılmıyor[70].

---

açık bankacılık kapsamındaki iki yeni ödeme hizmetine yasal zemin kazandırmış oldu: ***(1) Ödeme Başlatma Hizmetleri (Payment Initiation Services-"PISP"):*** *Kullanıcının talebi ile bir başka ödeme kuruluşunda bulunan hesabına ilişkin olarak ödeme emri başlatılması; ve* ***(2) Hesap Bilgisi Hizmetleri (Account Information Services- "AISP"):*** *Kullanıcının diğer ödeme kuruluşlarında bulunan bir veya birden fazla hesabına ilişkin olarak konsolide bilgilerin çevrim içi olarak sağlanması. Üye devletlere ayrıca 13 Ocak 2018 tarihine kadar bu düzenlemeyi kendi iç mevzuatlarına aktarmaları için süre verildi. PSD2 kapsamında ödeme başlatma veya hesap bilgisi hizmeti sunacak olan tüm hizmet sağlayıcıların direktifte öngörülen şartlarla kendi ülkelerindeki yetkili kuruluşlar tarafından yetkilendirilmesi ve Avrupa Birliği'ndeki finansal kuruluşlara ilişkin düzenlemelerin uygulanmasını sağlamakla görevli Avrupa Bankacılık Otoritesi ("European Banking Auhority", "EBA") nezdinde tescil edilmesi gerekli. Yeni düzenleme ile getirilen en önemli hususlardan birisi ise, açık bankacılık kapsamında veri paylaşımının bankaların inisiyatilerine bağlı olmaktan çıkarılarak bankaların veri paylaşımı konusunda zorunlu tutulması. Bunun yanında, PSD2 kapsamında PISP'ler ve AISP'ler için bir dizi yükümlülük öngörülüyor. PISP ve AISP'lerin yalnızca bu iki hizmetin sağlanması için hareket ettikleri durumlarda, müşteriye ait fonları tutmadıklarından, sermaye yeterliliği gerekliliklerine uyma yükümlülükleri bulunmasa da, faaliyetlerini aksatmadan yerine getirmelerini teminen, asgari tutarı gerçekleştirilen faaliyetin büyüklüğüne göre EBA tarafından belirlenen, bir sorumluluk sigortası yaptırmaları veya benzer bir güvence sağlamaları bekleniyor. Ayrıca her iki hizmet sağlayıcısının da kullanıcı adı ve şifre gibi ilgili bankanın sistemine giriş yapmasını sağlayacak kullanıcı bilgilerine hiçbir şekilde erişiminin olmaması ve tüm taralarla iletişimi güvenli yollardan sağlama zorunluluğu mevcut. Buna ek olarak hem AISP'lerin hem de PISP'lerin hizmeti sağlamadan önce müşteriden açık rıza alma zorunlulukları var ve müşteri tıpkı Türk hukukunda olduğu gibi bu açık rızayı dilediği zaman geri çekme veya kapsamını sınırlama hakkına sahip. PISP'lerin ayrıca her bir işleme ilişkin olarak müşteriyi bilgilendirmeleri ve AISP'lerin ise yalnızca banka tarafından kendilerine sağlanan bilgilere erişim sağlamaları gerekli. Sorumluluk açısından, PISP'lerin ödemenin tam ve zamanında yapılmasından müşterinin hesabının bulunduğu banka ile birlikte sorumlulukları bulunuyor*." **Bkz.** PWC: Açık Bankacılık- Dünya ve Türkiye, Raporu, 2020, s. 10.

[70] Türkiye Merkez Bankası tarafından daha tüm ödeme hizmet sağlayıcılarının açık bankacılık alanında uyması gereken zorunlu kurallar ikincil mevzuat kapsamında değerlendirilmiş ve ilgili alandaki kabul edilecek Kanun müzakeresinde görüşülmüş, lakin daha bir sonuca varılmamıştır. Bkz. PWC: Açık Bankacılık- Dünya ve Türkiye, Raporu, 2020, s. 10.

§2. Elektronik Bankacılıkta Saldırı Türleri ve Koruma Yöntemleri

I. Sistem Güvenliğini Tehdit Eden Unsurlar

A. Genel Olarak

Elektron bankacılık işlemlerinin gerçekleşmesi zamanı karşılaşabilecek risklerden en önemlisi müşterilerin kişisel bilgilerinin ele geçirilmesinin önüne geçmek ve banka olarak müşterinin kişisel bilgilerinin korumasına gereken özenin gösterilmesidir. Saldırganlar tarafından çeşitli yöntemler kullanılarak bilgilere erişim yapılması görülmektedir ve bu tür saldırılar banka tarafından uygulanan güvenlik önlemlerine göre değişiyor. Burada konuya tektaraflı bakmamak gerekir. Şöyle ki, bu müdahale hesap sahibinin özensiz davranışından (*kişisel bilgilerini yakınlarına veya yanında çalışanlara vermesi vs*) ve ya banka çalışanlarından (çalışanın bir şekilde elde ettiği bilgileri kötü amaçla kullanması) kaynaklana biliyor.

B. Tehdit Unsurlarının Türleri

1. Olta (*Phising*) Yöntemi

Phising[71] *"on line dolandırıcılığı-şifre avcılığı"* anlamında kullanılan bir yöntemdir[72]. İngilizce'de *"Phising"* olarak bilinen olta saldırıları da son yıllarda artış gösteren saldırılar arasındadır. Olta saldırılarında, saldırgan binlerce, hatta milyonlarca kişiye yönelik bir tuzak kurar (*olta atar*) ve yakaladıklarının bilgisini ele geçirmeye çalışır. Bu saldırılar hedefindeki kişileri ödülle kandırarak, onların güvenini kazanarak veya kızdırarak, korkutarak yani çeşitli yollardan manipüle ederek, kişisel bilgilerini saldırganın kontrolündeki sistemlere göndermeye ikna

[71] Phising, "password" (şifre) ve "fishing" (balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan, Türkçe'ye yemleme (oltalama) olarak çevrilen bir saldırı yöntemidir. Bkz. **Dülger**, **V. M.,** Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2015, s. 132.

[72] **Açıkgöz, O.,** "Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratılan Bankaya Karşı Mevduat Sahibinin Hukuki Sorumluluğu", **MÜHF-HAD**, C. 22, S. 1, s. 396; **Bilgen**, **M.,** İnternet Bankacılığından Kaynaklanan Zararlarda Bankaların Sorumlulukları, Bankacılar Dergisi, Sayı 71, 2009, s. 78.

etmeyi hedefler. Olta saldırılarında kullanılan yöntemlerin içerisinde e-posta[73], sms, telefon ve sahte siteler yoluyla olanlar en yaygınlarıdır.

Nitekim olta yöntemi e-posta ile gönderilen sahte mesajların içinde gelmektedir. Bu tür emailler sanki bir ticari kurumdan (bankalar, alış-veriş siteleri vb.) geliyormuş gibi bir izlenim yaratır. Bazı hâllerde gönderilmiş olan emailin içerisinde yerleştirilen bir linkin tıklanmasıyla bilgisayara virüsün bulaşımı gerçekleşir.[74]. E-posta içeriği normalde kişisel bilgilerin güncellenmesi gibi talepte bulunuyor ve yahut sistemdeki yeniliklerin hesabınızda aktif olması için şifrenizi girin gibi mesajlardan oluşuyor[75]. Meselâ, e-posta alıcısına, acilen bir işlem yapmasını aksi takdirde banka hesabının kullanılmaz olacağını, veya bir ceza ödemesi gerekeceğini belirterek, aynı e-posta içinde verdiği linke[76] tıklayarak kimlik bilgilerini[77] girmesini ister. Bu tip mesajlar bankaadi@yahoo.com gibi, bankadan geldiği hissi yaratan ama detaylı bir şekilde incelendiğinde, aslında başkasına ait olduğu anlaşılan adreslerden gönderilir.

Sms yoluyla gönderilen mesajlar da e-posta yöntemindeki gibi çalışır. Yalnız burada farklı olan, insanların cep telefonuna gelen mesajlara e-posta'dan daha fazla güvenmesi ve telefonun kısıtlı olanaklarında gönderen veya tıklanacak linkler

---

[73] E-posta yolu ile gönderilen *phising* mektublarının coğunda müşteriye *"hesabınıza şüpheli işlemler sebebiyle bloke konulmuştur ve bu blokenin kaldırılması için size sunulan linki açmanız ve kişisel bilgilerinizi yenilemeniz gerekir"* talepleri iletilmektedir. Bu yöntem 600 tane (300 tanesi phising, diğer 300 tanesi ise malware virüsü saldırısı ile ilgilidir) elektronik bankacılık dolandırıcılık olaylarının araştırılması zamanı ortaya çıkmıştır. Diğer bir saldırı yöntemi de müşteriye gönderilen e-postada "bankanın programının Avrupa direktifleri gereğince güncellenmesi projesi çerçevesinde hesabınızla ilgili kişisel bilgilerde yalnışlıklara rastlandı, lütfen size sunulan linkden bilgi güncellenmesini yapınız". Bu bilgiler güncellendikden sonra müşteriler telefonla aranarak kod sözü de alınır ve bununla da hesabları kolaylıkla boşaltılır. Bkz. Jurgen Jansen, Rutger Leukfeldt, "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases", Proceedings of the 5th Workshop on SocioTechnical Aspects in Security and Trust, 2015, https://www.researchgate.net/publication/280013974_How_people_help_fraudsters_steal_their_money_An_analysis_of_600_online_banking_fraud_cases, s. 5.

[74] Meselâ,"*Tarafınıza X adlı kişiden Y tutarında para transferi yapılmıştır. Lütfen aşağıdaki linke tıklayarak, internet bankacılığınıza giriş yapın ve bilgilerinizi kontrol edin gibi ifadeler içeren e-postalar gönderilir. Eğer internet bankacılığına girerek işlemi onaylamazsanız para transferi gerçekleştirilmeyecektir"* gibi tuzağa düşürücü anlatımlar da bulunabilir.

[75]**Dolandırıcılık Eylemleri ve Korunma Yöntemleri**, TBB Yayınları, Aralık 2015, s. 15.

[76] "*Link, ekran üzerinde görüntüsü olan bir web sitesinden diğer bir web sitesine bir bağlantıdır. Bu bağlantı bir metin veya resim aracılığıyla gerçekleşir. Bu metin veya resmin mouse (fare) ile tıklanmasıyla diğer siteye geçiş gerçekleşir."* Bkz. **Güran vd.**, s. 11-13.

[77] "*Phising yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen işlemleri çalmaktadırlar: kredi, debit/ATM kart numaraları/CVV2, şifreler ve parolalar, hesap numaraları, internet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri."* Bkz. **Eralp**, s. 71; **Dolandırıcılık Eylemleri ve Korunma Yöntemleri**, s. 15.

hakkında detaylı bilginin kolayca elde edilememesidir. Bu gibi SMS'lerde gönderen kısmında banka adı, emniyet gibi ibareler bulunabilir[78]. Diğer taraftan, internet üzerinde çalışan neredeyse tüm phising saldırıları gerçek bir sitenin sürümünü kullanır. Bununla da kullanıcı doğru bir adresi yazdığı hâlde sahte bir sayfaya yönlendirilir ve kişisel bilgilerinin ele geçirilmesi böylece sağlanmış olur. Bu sitelere phising e-postalarından veya arama motorlarından erişebileceği gibi, Facebook, MSN Messenger gibi güvenilir platformaların içine gizlenmiş kötü niyetli linkler üzerinden de erişebilir. Bazen kullanıcının arkadaşlarına onun tarafından gönderilmiş gibi suç teşkil eden iletiler gönderilebilmektedir.

Belirtmek gerekir ki, arama motorlarında bazı bankaların dolandırıcılar tarafından hazırlanan sahte web adreslerinin yer aldığı göz önüne alındığında, bu saldırıların yaygın olduğu görülmektedir. Bu hâlde tedbir olarak banka adreslerinin, adres çubuğuna elle (manuel) olarak yazılması önerilebilir[79]. Telefon edilerek kendini banka yetkilisi gibi tanıtmak ve hesap sahiplerinden kişisel bilgilerin güncellenmesi amacıyla sorulara cevabın istenilmesi de sıklıkla rastlanan saldırı yöntemlerindendir. Dolayısıyla, saldırganlar, olta saldırıları ile oltaya düşürdükleri kişilerin bankacılık şifrelerini, e-posta kullanıcı adı ve şifrelerini, sosyal ortamlardaki kullanıcı hesaplarını, kimlik bilgilerini, paralarını ve akla gelebilecek her türlü varlığını ele geçirmeyi hedefleyebilirler[80]. Doladırıcılığı gerçekleştirecek kişi(ler) olta saldırısı yöntemi ile edindikleri bilgileri kullanarak müşterilerin banka hesaplarına erişmekte ve varlıklarını ele geçirmektedir. Ele geçirilen hesaptan paranın çekilmesi aşamasında, daha az şüphe çekebilecek üçüncü kişiler kullanılır. Bu kişilere menfaatler karşılığı görevler verilir. İş ilanlarında çaba harcamadan kolay para kazanılacağı şeklinde bilgi verilir, başvuruda bulunan kişilerin hesap bilgileri alınır ve bu kişilere ait hesaplar kullanılarak olta saldırısı yöntemi ile ele geçirilen hesaplardan para transferi yapılır. Bu yöntemle, müşteri ve hesap bilgilerini ele

[78] **Özmen**, **Ş.,** Ağ Ekonomisinde Yeni Ticaret Yolu E-Ticaret, 4. bs., İstanbul Bilgi Üniversitesi Yayınları, 2012, s. 501; **İnal**, **E.,** "İnternet Dolandırıcılığı Eylemlerine Karşı Bankanın Yükümlülükleri ve Sorumluluğu", Banka ve Tüketici Hukuku Sorunları Sempozyumu, XII Levha Yayıncılık, 2010, s.367.
[79] **Dülger**, s. 132.
[80] **Özmen,** s. 501; **Bilgen**, Sorumluluk, s. 79.

geçiren ve dolandırıcılık olayının asıl faili olan kişiler kimliklerini gizler ve aracı olarak kullandıkları üçüncü kişilere suçu yükleyerek zaman kazanmış olurlar[81].

Sonuç itibariyle, banka dolandırıcılıklarının çok büyük bir kısmı *phising* ismiyle anılan bir online dolandırıcılık yöntemiyle gerçekleştiriliyor. Bu yöntemde dolandırıcılar bankanın web sitesini taklit ederek kullanıcıları kendilerinin yarattığı sahte siteye çekiyor, kişisel bilgileri elde etmiş oluyor ve aracı üçüncü kişileri kullanmakla banka müşterilerinin hesaplarındaki parayı çalabiliyorlar.

2. Trojan (Truva Atı)

"*Bilgisayarlara e-posta ya da internet aracılığıyla sızarak internete bağlı olunduğu sırada kullanıcı farkına varmadan dışarıya veri gönderen programlara "truva atı" (trojan horse) denilmektedir.*"[82] Truva atı, yasal bir program içindeki yasal olmayan tarzda talimatlar ya da bir işi yapıyormuş gibi görünüp kullanıcısından habersiz işlemler yapan zararlı bir program olarak da tanımlanmaktadır[83].

Truva atı zararlı yazılım olarak programların içine sızıp, amacı kişisel bilgilere erişmek ve yasal olmayan işler için kullanmaktır.[84]. Görüldüğü gibi, truva atları da diğer birçok zararlı yazılımda olduğu gibi kullanıcılar tarafından internette veya e-posta yolu ile ücretsiz kullanabilecekleri basit programlar[85] ya da uygulamalar aracılığı ile bilgisayarlara bulaşmaktadırlar.

Bununla da söz konusu programlar kullanıcı tarafından yapılan işlemleri ve tabii olarak, onun kullanıcı adı, şifre gibi diğer kişisel bilgilerini kaydeder ve bu bilgilerin üçüncü kişi dolandırıcıların eline geçmesine imkân tanır[86].

---

[81] **Dolandırıcılık Eylemleri ve Korunma Yöntemleri**, s. 15.
[82] **Avşar, Z./Güngören, G.,** Bilişim Hukuku, Türkiye Bankalar Birliği Yayını No: 270, İstanbul, 2010, s. 49.
[83] **Yılmaz**, **D.,** Hacking/Bilişim Korsanlığı ve Korunma Yöntemleri, Hayat Yayınları, İstanbul, 2004, s. 380; **Dülger**, s. 104.
[84]**Savaş**, s. 156.
[85] Truva atları gizlenmek için oyunlar veya porno resimler içeren grafik programlarını tercih ederler. Virüslerden farklı olarak kendilerini kopyalayarak tüm bilgisayar sistemine yayılma özelliğine sahip değildirler. Truva atı türü programların tümü zararlı değildir. Ancak yazılım hatası veya kullanıcının bazı şeylere dikkat etmemesi durumlarında çok zararlı etkiler yapabileceklerinden uzak durulması gerekmektedir..
[86] **İnal**, Sempozyum, s.367.

3. Klavye Dinleme Sistemleri (Keylogger)

"*Keylogger bir bilgisayarda yapılan her tuş vuruşunu izleme eylemidir*." Bu yazılım kötü niyyetlidir, kullanıcı parolası ve yahut finansal bilgiler gibi hassas verilerin elde edilerek her hangi bir suçun işlenmesinde kullanmasına yöneliktir[87]. Bu yöntemin gerçekleşmesine olanak sağlayan bilgisayara başarılı olarak yerleştirilen "truva atı" dır. Bunsuz her hangi gözetlemeni yapmak mümkün olmayacaktır. Şöyle ki, yerleştirilen truva atı aracılığı ile kullanıcının klavye hareketlerini kaydedip karşı tarafa gönderilecektir. Bununla da hassas kişisel bilgilere kolaylıkla erişmek mümkün olacaktır.

4. Ekran Kayıtları (Screen Logger) Yöntemi

Bu yöntemin işleyişi de, klavye hareketleri (key logger) ile aynı mantıkla çalışmaktadır. Yalnız klavye hareketleri ile sınırlı olmayıp, kullanıcının fareyi ekranda bir noktaya tıklatmasıyla sistem devreye girer ve ekranın tamamının ya da küçük bir bölümünün o andaki resmi çekilerek karşı tarafa ulaştırılır. Bu yolla sanal klavye ile girilen bilgilerin de ele geçirilmesi mümkün bulunmaktadır[88].

5. Yanlış Alan Adına Yönlendirme (*Pharming/DNS-Spoofing*)

İnternet üzerinden iletişim kurabilmek her bir internet kullanıcısının IP adresi (İnternet Protokolü) alması gerekmektedir. IP adresini oluşturan numaraları akılda tutmak zor olduğu için internet üzerinden iletişime geçilecek bu numaralara bir isim (*domain-name*) verilmektedir[89]. Bu saldırı türünde kötü niyetli kişiler, alan adı sunucusundaki (DNS -Domain Name Service) dosyada ilgili ismin (domain name) temsil ettiği numarayi değiştirmektedir. Kullanıcı alan adını (*domain name*) girdiği zaman başka bir numaraya yönlendirilmektedir. Bu tür müdahale normalde dolandırıcılar tarafından daha önce müşterinin bilgisayarına bir virüs ve ya truva atı

---

[87] **Memiş**, **T.,** "Elektronik Bankacılıkta Bankanın Yükümlülük ve Sorumlulukları", Prof. Dr. Ergon A. Çetingil ve Prof. Dr. Rayegan Kender'e 50. Birlikte Çalışma Yılı Armağanı, Çizgi Basım Yayın, İstanbul, 2007, s. 882.

[88] **Bilgen**, Sorumluluk**,** s. 79; **Bilgen**, **M.,** Banka Hukukunda Sözleşmeler, Uyuşmazlıklar ve Hukuki Sorumluluk, Adalet Yayınevi, Ankara, 2011, s. 754.

[89] **Bilgen**, Sözleşmeler**,** s. 761.

(*trojan horse*) içeren bir e-posta gönderilmesi aracılığı ile gerçekleştirilmektedir. Dolayısıyla burada müşterinin herhangi bir aktif davranışı söz konusu olmamaktadır. Meselâ, müşteri mevduat hesabının bulunduğu bankanın web sitesininin ismini doğru yazdığı hâlde otomatik olarak sahte bir web sitesine yönlendirilmektedir. Yönlendirildiği zaman bu sahte sitede kişisel bilgilerini kullanmaya başlar ve bu arada kullanılan kişisel bilgiler dolandırıcıların eline geçer.[90]

6. *"Man in the Middle"* Yöntemi (Aradaki Adam Saldırısı)

Bu tür saldırıda amaç banka-müşteri iletişiminde bir takım kötü niyetli kişilerin araya girerek müşteriye ait kişisel verileri elde etmesidir. Normalde bu tür saldırılar banka tarafından SSL protokolü (*Secure Sockets Layer*) kullanılmadığı durumlarda gerçekleşmektedir. Bu saldırı yöntem ile elde edilen müşteri bilgileri daha sonra kullanılmak ve yahut diğer üçüncü tarafa ötürülmesi amacına hizmet etmektedir.[91]

7. İstenmeyen Elektronik Posta (*Spam*)

"*Spam*[92]*, alıcı tarafından istenmeyen aynı anda birçok kişiye gönderilen zarar verici çoğu reklam amaçlı istem dışı e-maillere verilen addır. Genellikle istenmeyen e-postalar sahte (fake)*[93] *veya zararlı*[94] *e-postalar olarak da adlandırılmaktadır. Özellikle kötü niyetli yazılım ya da programlar vasıtasıyla (malware) bilgi hırsızlığı ve oltalama faaliyetlerinde sıkça kullanılan bir yöntemdir*[95]. Sahte bir email kullanıcıya geliyor ve gönderilen sahte e-postayı cevaplamak için kişi yine sahte hazırlanmış bir internet adresine yönlendirilir ve

---

[90] **Yasaman, H.,** Banka Hukuku İle İlgili Makaleler, Hukuki Mütalaalar, Bilirkişi Raporları, Vedat Kitapçılık, İstanbul, 2005, s.144; **Atamer, M. Y.,** "Kredi Kartının Üçüncü Kişi Tarafından Hukuka Aykırı Şekilde Kullanılması Halinde Doğan Zararları Kim Taşıyacaktır?", Bilgi Toplumunda Hukuk/Prof. Dr. Ünal Tekinalp'a Armağan, C. 1, Beta Basım Yayın, İstanbul, 2003, s. 22-23.
[91] **Atamer**, Kredi Kartı, s. 23, **Bilgen,** Sözleşmeler, s. 753-754.
[92] Spam sözcüğü, ilk kez ABD'de Firma Hormel Foods Corporation gıda ürünlerinde kullanılmış bir kısaltma olarak ortaya çıkmıştır. Bu kısaltma *"spiced pork and harm"* kelimelerinin baş harflerinden oluşmaktadır. Bkz. **Dülger**, s. 129; **Soysal**, Elektronik Posta, s. 156.
[93] **Akarslan**, **H.,** Bilişim Suçları, Seçkin Yayıncılık, Ankara, s. 102.
[94] **Yasaman**, s. 143;
[95] **Yasaman**, s. 143;

kurban kullanıcı adı ve şifresini girdiğinde üçüncü kişilerin eline geçer[96]. Spam farkı forumlar, haber grupları, sohbet odaları gibi yerlerde daha çok rastlanmakta olup, kullanıcıların bilgilerime bu ortamlar aracılığı ile erişildikden sonra dolandırıcılar spam içerikli sahte emailler hazırlar ve kullanıcılara gönderirler.[97] Span kelimesinin tanımına gelince ise söylemek gerekir ki, Uluslararası Ticaret Örgütü'nün 1996 yılında yayınlamış olduğu *"ICC Guidelines on Interactive Marketing Communicating"*de "*spam, bir bülten veya haber grubu üzerinden ticari amaç taşımayan, bu forum konuları ile ilgisi olmayan ve gönderilmesine açıkça izin verilmeyen reklam olarak tanımlanmaktadır*"[98]. Doktrinde "*internet üzerinden aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi "istenmeyen e-posta (spam)" olarak da adlandırılmaktadır*."[99]. Bu arada spamming kelimesi de literatürde kullanılmaktadır. Spamming, genellikle ticari amaçlı elektronik postaların, çok fazla sayıda ve bazen de tekrarlanarak, bu konuda bir talepte bulunmayan ve göndericinin hiçbir ilişkisi olmayan kişilere gönderilmesi olarak tanımlanmaktadır[100]. Tüm e-posta trafiğinin %75'ini oluşturan spamlar zararlı kod içeren URL linklerin, kötü yazılımların yayılması ve dolandırıcılıklar için bir kaynak durumundadır. Günümüzde spam üreticilerinin spam filtreleme yazılımlarının performanslarını düzenli olarak kontrol etmelerinin de etkisiyle spamlara karşı etkin bir korunma sağlanamamaktadır[101].

8. Sosyal Mühendislik (*Social Engineering*)

Sosyal mühendislikte asıl amaç her türlü yolla kişilerin internetteki zaafiyetlerini kullanarak istenilen bilgilerin elde edilmesine çalışmaktır. Bunun için

---

[96] **Akarslan**, s. 103

[97] **Yaşar, H./Çakır, H.,** "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, C. 3, S. 2, Y. 2015, s. 494.

[98] **Memiş, T.,** "Hukuki Açıdan Kitlelere E-Posta Gönderilmesi", **AÜEHFD**, C.5, S. 1-4, Y. 2001, s. 432 vd.

[99] İki tür istenmeyen e-posta vardır, birincisi internet üzerinden belli tekniklerle çok sayıda e-posta adresinin toplanması ve bunlara e-posta gönderilmesidir. İkincisi ise, "*MMF (Make Money Fast - Kolay Para Kazanın) iletileri; zincir iletiler ya da piramit benzeri pazarlama yapıları ile ilgili gelen iletilerdir. Burada kişi para kazanacağını zannederek e-postayı kendi arkadaşlarına onlar da kendi e-posta listesindeki kişilere gönderir ve böylece e-posta çok sayıda kişiye ulaşmış olur.*" Bkz. **Akarslan**, s. 103

[100] **Özdemir Kocasakal**, s. 68;

[101] **Yaşar/Çakır**, s. 494.

kullanıcıların bu tür durumlarda dikkatli olması ve süreçleri değiştirmeye yönelik tekniklere gözü açık olmalıdırlar.[102] Meselâ, en çok rastlanan yöntemlerden biri - bilgi edinecekleri kişiye şirketin personeliymiş gibi kendilerini tanıtarak, bazı acil bilgilere ihtiyaç duyulduğunu ifade edip şifre gibi önemli bilgilerin sızdırılmasının sağlanmasıdır[103].

9. Denial of Service (DOS) Saldırıları

Bu yöntemde saldırgan, ilk olarak kendi geliştirdiği veya bulduğu küçük bir program yardımıyla Internet'i tarayarak savunmasız bilgisayarları tespit etmektedir. Bunun yapılmasındaki amaç herhangi bir internet sitesine çok talep göndererek, onu hizmet veremez hâle getirmektir. Bu tür saldırılarla daha çok internet sitesine bağlanmak istenen banka müşterileri yüz yüze geliyor. Güvenliğe önem vermeden Internet bağlantısı yapan ağlardaki bilgisayarlar, deneme amacıyla korumasız olarak Internet'e bağlanan bilgisayarlar vb. bu taramada yakalanmaktadırlar. Yakalanan bu sistemlere sıradan saldırı teknikleri ile erişilip ajan programı kurulmaktadır. Bu programların amacı bulundukları sisteme zarar vermek değil, sadece Internet'ten gelebilecek emir için belirli bir kanaldan bilgisayar ağını sürekli dinlemektir. Sıradan kullanıcı, hizmet almak üzere isteğini siteye (saldırganlar tarafından kurban seçilen siteye) gönderdiğinde, söz konusu site binlerce istekle karşılaşır. Bu durumda site, kapasitesinin çok üzerinde istek aldığı için hizmet veremez hâle gelir. Sunucuların, isteğin normal bir kullanıcıdan mı, yoksa bir saldırgan tarafından mı geldiğini tespit etmeleri mümkün değildir.[104]

10. Sniffing

"*Sniffing*" network ortamındaki bilgisayarlar arasında verilerin dinlenilmesini ifade eder. Ağ ortamında internete giriyorsanız sniffing kurbanı olabilirsiniz. Saldıranlar ağ altındaki bilgisayarlara yerleştirdikleri snifferler ile ağ trafiğini tespit

---

[102] Sosyal mühendislik dolandırıcılığı hakkında detaylı açıklamalar için bkz.: **Dolandırıcılık Eylemleri ve Korunma Yöntemleri**, s. 6 vd.
[103] **Özmen**, s. 508.
[104] **Yılmaz D.**, s. 134-135; **Dülger**, s. 132; **Akarslan**, s. 101.

ederek kontrol altında tutabilmektedirler. Meselâ, en tanınmışlardan biri *ethereal* sniffer programıyla izlemeye başlarlar ve önemli gördükleri bilgileri ele geçirirler. Bu tür saldırılara okul, işyeri, internet cafe gibi ağ ortamlarında maruz kalabilirsiniz. Bu saldırıların en önemli özelliklerinden biri, kullanıcılar tarafından fark edilmesinin zor olmasıdır. Bu nedenle sunucu yöneticileri tarafından sürekli kontrol edilip bu tür yazılımların temizlenmesi gerekmektedir.

11. Solucanlar

Solucanlar, kendi kendine çalışabilen ve tam çalışan kopyalarını diğer makinelere kopyalayabilen programlara denmektedir. Diğer zararlı programlardan farklı olarak, bir kez sisteme girdikden sonra kendi başına ilerleyip, coğala bilir ve en büyük tehlikesi kendilerini büyük sayıda çoğaltma yeteneğidir[105]. Meselâ, bir solucan tarafından her kese e-posta adres defterinizdeki kopyalar gönderilebilir ve sonra aynı şeyi onların bilgisayarları da yapabilir. Bu tür yöntem domino etkisi yaratır ve intenetin hızı de yavaşlıyor. Diğer bir zararvericiliği ağları kilitlemesi ve internet web sayfalarını görüntülerken uzun süre kullanıcıların beklemelerine yol açarlar. Solucan virüsü normalde e-posta, cinsel içerikli internet siteleri, kaynağı belirsiz programlar, forum siteleri, korsan oyun dvd ve cd'leri gibi farklı yollarla kullanıcıların bilgisayarlarına bulaşırlar. Solucanlara somut örnek olarak *Sasser* ve *Blaster* solucanı verilebilir. Solucan ile truva atı arasındaki farklılıklar mevcuttur. Şöyle ki, truva virüsü bilgisayarda hangi programa bulaşmışsa, o programın açılmasıyla aktif hâle gelir. Söz konusu program açılmazsa aktifleşmez. Truvadan farklı olarak solucan bilgisayarın iletişim sistemine zarar vermez, sadece kullanıcının girmiş olduğu siteler, giriş zamanı kullandığınız kullanıcı adı, şifreleri, indirilen programlar ve diger iletiler hakkında bilgi toplar ve her addımınızı rapor olarak bildirir. Solucanın sahibi istediği gibi kullanıcının bilgisayarının ekranında hareket ede bilir, klavyedeki tüm ışıkların yanıp sönmesini sağlayabilir, istediği programları açabilir[106].

---

[105] **Akarslan**, s. 93; **Özmestik**, **F. Ü.,** "Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2015, s. 14.
[106] **Eralp**, s. 73-74.

12. Sim Kart Yenileme ve Operatör Deşiğikliği

Sim kart yenilenmesi ve operatör değişikliği zamanı sahtekârlar müşteri adına düzenlenen sahte kimlikle onlara ait telefonun çalındığını veya kaybolduğunu beyan etmekle GSM bayilerinden yeni bir SIM[107] kart çıkarılması talebinde bulunuyorlar. Bu yöntem ile kullanıcıya ait internet şifresi dolandırıcılar tarafından banka tarafından gönderilen SMS sifresi kolaylıkla ele geçirmiş oluyorlar ve müşteri adından işlemleri gerçekleştirebiliyorlar. Aynı şekilde sahte kimlikle dolandırıcılık yöntemi telefon operatörü değişikliğinde de yapılabilmektedir.

Bu tür dolandırıcılık yönteminin internet bankacılığa yapılan saldırılarda engellenmesi amacıyla, bankalar GSM Operatörleri ile ortak bir mutabakata varmış ve bu mutabakat çerçevesinde, internet bankacılığı girişi sırasında gönderilen SMS bilgilerini almaya yetkili hatlarla ilgili olarak 90 gün içinde taşıma/yenileme olup olmadığı sorgulanmaktadır.

BBSEBHY'nin 34. maddesinin 8. fıkrası uyarınca, "*Banka, SIM kart değişikliği gerçekleşmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterilerini Türkiye'de yerleşik mobil haberleşme işletmeleriyle gerekli entegrasyonu sağlayarak SMS OTP göndermeden önce belirler ve ilgili müşterilere, değişiklikler teyit edilmediği müddetçe, değişikliğin yapıldığını tarihten itibaren 90 gün boyunca elektronik bankacılık hizmetleri sunulurken SIM karta dayalı unsur kimlik doğrulama unsuru olarak kullanılamaz. Değişiklikler teyit edilirken iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü bankaya aittir.*"

Söz konusu tedbir SIM kart kopyalama dolandırıcılıklarını internet bankacılığı için engellenmiştir. Nitekim banka şubesi tarafında sahte kimlik ile noterden çıkartılan vekâletnamelerle müşteri hesaplarına yapılan dolandırıcılıklarda, SIM kart kopyalama vakaları ile karşılaşılmıştır. Müşteri banka şubesi tarafından arandığında ona ait hattı kopyalayan dolandırıcı telefona cevap vererek, sahte Banka şubesi müşteriyi aradığında müşteriye ait hattı kopyalayan dolandırıcı telefona cevap vererek, sahte vekâletnameyi müşteri gibi onaylamaktadır. Bu eylem tipi sahte evrak

[107] *Subscriber Identification Module*

dolandırıcılık türü olduğundan tez çalışmasında sadece internet bankacılığa ait olan tarafı incelenmiştir. [108]

13. Vishing

Vishing bir dolandırıcılık metodu olup, müşterilerin banka hesap, kredi kartı ve bunun gibi kişisel bilgileri elde edilmesine yönelmektedir. *Vishing* ses ile aldatma yöntemidir. Dolandırıcılar bu amaçlarını gerçekleştirmek için banka sesli yanıt sistemini veya Çağrı Merkezi'ni taklit eden bir sistem kuruyorlar ve bu yöntem aracılığı ile müşterilerden onlara ait kişisel bilgileri ele geçirebiliyorlar. Meselâ, "*Ailesinin gayrimenkul imparatorluğunun başına geçen Poyraz Bey, işlerinin çok yoğun olduğu bir gün sürekli çalıştığı ve güvendiği Tatlıbank'tan, bir e-posta alır. Aldığı e-posta, ona hesaplarının 2 gün içinde pasif hâle geleceğini çok acil 0(850) *** ** ** numaralı çağrı merkezini arayıp, hesaplarını aktif hâle getirmesini tembihler. Tamamen Tatlıbank'tan gelmiş gibi görünen bu e-postaya güvenen Poyraz Bey, belirtilen çağrı merkezini arar. Düzmece çağrı merkezi sesli yanıt sisteminden de hiç şüphelenmeyen Poyraz Bey, hesaplarını aktif ettirmek için kredi kartı bilgilerini sisteme tuşlar ve işlemlerini sonlandırır. Hesaplarını aktif hâle getirilmesinin gururuyla rahatlamış bir şekilde öğle yemeğine çıkar. Oysa biraz sonra kart bilgilerini çaldırdığını öğrenecek ve yemeği kendisine zehir olacaktır*."[109]

14. Omuz Sörfü (Shoulder surfing)

Bu yöntemi dolandırıcılar tarafından ATM ve POS makinalarında işlem yapan müşterilerin kart bilgilerine ulaşmak için müşterilerin omuzu üstünden gizlice gözetleme olarak tanımlayabiliriz. Bu yöntem sadece ATM ve POS makinalarında değil, bireyin telefonunun PIN numarasını ve ya bilgisayarının parolasının üsulsuz

---

[108] Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önlemleri Yöntemleri, TBB, Ekim-2015, s. 24; Uygulamada kötü niyetli üçüncü kişiler, mevduat sahibinin kişisel bilgilerini hukuka aykırı çeşitli yöntemlerle ele geçirdikden sonra düzenledikleri sahte kimlikle GSM şirketinin bayisine giderek, GSM hattının gerçek sahibi olarak kendisini tanıtıp sim kartın bozulduğu ya da kaydedildiği gerekçesiyle yeni bir sim kart çıkartmaktadır. Bununla, müşterinin banka hesabına erişimi için zorunlu olan güvenlik şifresini ele geçirdikden sonra kısa bir süre içerisinde bankadaki mevduatı önceden anlaştıkları kişilerin hesabına aktararak haksız çıkar (menfaat) elde etmektedirler. Bkz. **Açıkgöz, O.,** "İnternet Bankacılık Hizmetlerinin Sağlanmasına Yönelik Borcun İfasında Mobil Haberleşme (GSM) Şirketinin Hukuki Konumu ve Banka ile Mevduat Sahibine Karşı Sorumluluğu", Kadir Has Üniversitesi Hükuk Fakültesi Dergisi, C. 3, S. 2, Y. Aralık 2015, s. 60.

[109] Bu örnek TBB'nin Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önlemleri Yöntemleri isimli yayınından alınmıştır. Ekim -2015, s. 24

ulaşılması hâlinde de uygulanmaktadır. Omuz üstünden müşterinin kişisel bilgilerine erişmek pasif omuz sörfüdür. Nitekim ATM üstüne mini kameraların düzenlenmesi[110] ve ya o konumda evin kiralanması ve dürbün, teleobjektif gibi uzun menzilli araçlar[111] aracılığı ile gözetilmesi aktif omuz sörfü olarak nitelendirilmektedir.

15. Kimlik Hırsızlığı *(Identity Theft)*

Tez çalışmamızda kimlik hırsızlığının elektron bankacılık tarafında dolandırıcılık yöntemlerinin gerçekleşmesi zamanı ortaya çıkan boyutları incelenmişdir. Genel olarak kimlik hırsızlığı ister tüzel, isterse de gerçek kişilere ait kimlik bilgilerinin ve ya belgelerinin dolandırıcılar tarafından ele geçirilmesi ile kullanılması şeklinde bir dolandırıcılık yöntemi olarak biliniyor. Elektron bankacılıkta müşterinin kişisel bilgilerinin ve yahut belgelerinin ele geçirilmesi genel olarak phising internet siteleri veya emailleri, virüslü e-postalar, truva atları, sosyal mühendislik (sosyal medya, telefon aramaları vb.) gibi elektron bankacılıktaki saldırı yöntemleri aracılığı ile yapılır. Söz konusu saldırı türlerine tez çalışmasında ayrıca başlık altında değinilecektir.

16. Kart Kopyalama

Kart kopyalama dolandırıcılar tarafından en sık başvurulan yöntemlerden biridir. İki tür kart kopyalamasına aşağıdaki başlıklar altında değinilecektir: (*i)* ATM kaynaklı kart kopyalaması; *(ii)* POS kaynaklı kart kopyalaması

---

[110] Lochter, Manfred/Schindler, Werner: "Missbrauch von PIN-gestützten Transaktionen mit ec- unad Kreditkarten aus Gutachtersicht", MMR 2006, s. 295, Özboyacı A., Kartlı Ödeme Sistemlerinde Kartın Kötüye Kullanılmasından Kaynaklanan Hukuki Sorumluluk, Seçkin, 2019, s. 125'den naklen

[111] Haybâck, Gerwin: Risikohaftung bei missbrâuchlichen Bankomatbehebungen, Ein österreichisch-deutscher Rechtsvergleich, Neuer wissenschaftlicher Verlag, Wien-Graz 2008, s. 96-97, Özboyacı A., Kartlı Ödeme Sistemlerinde Kartın Kötüye Kullanılmasından Kaynaklanan Hukuki Sorumluluk, Seçkin, 2019, s. 125'den naklen

a. ATM Kaynaklı Kart Kopyalama

Bu tür dolandırıcılık yöntemi ATM'lere kurulan "Skimmer" cihazı ile yapılan kopyalamadır. Bu ATM kart giriş yuvasına takılan bir cihaz ile gerçekleştirilir. Düzenlenmiş cihaz sadece kart manyetiğinin bilgilerini çalmaktadır. Kopyalama düzeneği ise bununla bitmir. Şöyle ki, müşterinin ATM'e girmekte olduğu şifrenin çalınması ise sahte klavye (PINPAD) ve yahut da klavyeye odaklanmış ve gizlenmiş bir kamera kullanılarak gerçekleşmektedir.[112] Bir çok Avrupa ülkesinde, Almaniya da dâhil olmak üzere mesai saatleri dışında ATM'lere erişim otomatik kapıların bulunduğu ve yalnız kartla girişe izin verildiği kapalı alanlarda mümkündür. Giriş zamanı PIN bilgilerinin girilmesi istenilmez. Kapının açılması için yalnız kartın fiziki varlığı yeterlidir. Almaniya'da dolandırıcıların kapıların kart giriş kısmına kopyalama cihazları düzenlediği görülmüştür. Dolandırıcıların bu eylemi kart bilgilerinin çalınmasına yönelmiştir.[113] PIN bilgilerine erişmek için mini hoparlörler düzenlemekle ATM'lerin teknik sorun nedeniyle servis dışı kaldığı anons edilir. Bu sırada dolandırıcılar kızılötesi ışın teknolojisi ile çalışan tele kamera yardımıyla kişinin PIN bilgisini kayda alırlar. Bununla da kişisel bilgiler usulsüz şekilde dolandırıcılar tarafından edinilir[114].

b. POS Kaynaklı Kart Kopyalama

Adından da göründüğü gibi, bu tür kopyalama POS makinelerinin üzerinde yerleştirilen bir kopyalama düzeneği ile gerçekleşmektedir. Bu tür kopyalama yönteminde "Skimmer" cihazı kullanılmaktadır. Bu kopyalama türü genellikle üye işyerlerinde çalışan personel tarafından yapılmaktadır. Üye işyerlerinde çalışanlar arasında bir dolandırıcılık şebekesi oluşturulmakla, ödeme yapılmak amacıyla verilen kartları ikinci bir okuyucudan geçirerek kopyalamaya çalışırlar. Bununla da dolandırıcılar şifreyi kolayca bizzat almaktadır. Diğer taraftan POS makinelerine hizmet eden teknisyenler tamir ve ya bakım zamanı makinenin içerisine bir düzenek

---

[112] ATM kaynaklı kart kopyalamasının örnekleri için bkz. Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önlemleri Yöntemleri, TBB, Ekim -2015, s. 64

[113] Lochter, Manfred/Schindler, Werner: "Missbrauch von PIN-gestützten Transaktionen mit ec- unad Kreditkarten aus Gutachtersicht", MMR 2006, s. 295, **Özboyacı, A.,** Kartlı Ödeme Sistemlerinde Kartın Kötüye Kullanılmasından Kaynaklanan Hukuki Sorumluluk, Seçkin Yayıncılık, Ankara, 2019, s. 152'den naklen.

[114] Russenschuk Viola: Die Auszahlung von Bargeld an Geldautomaten nach deutschem Zivilrecht, Duncker & Humblot, Berlin, 2002, s. 35, **Özboyacı**, s. 152'den naklen.

yerleştire bilmektedirler. Bununla da yerleştirdikleri cihazla şifreleri loglayıp çalabilmektedirler. Daha bir farklı yöntem POS makinasına benzer bir cihazlar kapıdan alış-verişlerde kart kopyalamanın gerçekleşmesidir. Dolandırıcılar ellerinde bu cihazla sifariş için kapıdan ödemeni alarken kart bilgilerini de anında kopyalama yolu ile çalmış oluyorlar. Uygulamada sahte belgelerde açılmış şirketler adına alınmış üye işyeri pos makinaları ile de kart kopyalaması yapılması mevcuttur.[115]

II. Elektronik Güvenlik Önlemleri

Günümüzde internet altyapısı tehlikeden uzak ve güvenilir etmek hiç de kolay değildir. Elektronik güvenlik önlemlerinde sıkça başvurulan sırasında şifreleme, güvenlik duvarı, kimlik doğrulama, İP güvenliği gibi yöntemleri söylemek mümkündür.

A. Şifreleme (Encryption)

Şifreleme üçüncü kişilerin haksız müdahalelerine karşı koruyucu bir yöntem olarak bilinmektedir. Bu yöntem için kriptiloji kavramı da kullanılmaktadır. Verilerin sadece katılımcılar (müşteriler) tarafından görülebilmesini, haksız müdahalelere karşı korunmasını amaçlayan şifrelemede başlıca iki yöntem kullanılmaktadır: simetrik şifreleme ve asitmetrik şifreleme[116].

Simetrik şifrelemede yönteminde şifrenin oluşturulmasında ve çözülmesinde aynı anahtar kullanılır. Bu anahtarın, iletişimin taraflarınca emin bir kanaldan tespit edilmiş ve üzerinde uzlaşılmış olması gerekir. Bu yöntemde istemde bulunan her kullanıcının, diğer her biriyle iletişim için ayrı şifresi bulunmaktadır. Böyle olunca, her katılımcıyla birlikte, katlanarak büyüyen sayıda şifre ortaya çıkar[117].

Asimetrik şifreleme yöntemi daha yenidir. 1976 yılından beri uygulanmaktadır. Bu yöntemde, her katılımcı birbirini tanımlayan bir şifre çiftine sahip olur. Bunlardan ilki açık anahtar (*public key*), diğeri gizli anahtardır (*private*

---

[115] POS kaynaklı kart kopyalamasının örnekleri için bkz. Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önlemleri Yöntemleri, TBB, Ekim -2015, s. 65.

[116] **Wan A. H.,** Electronic Financial Services: Technology and Management, Chandos Publishing, 2006, s. 104

[117] **Wan A. H.**, s. 107.

key). Gizli anahtar, güvenilir sertifika hizmet sağlayıcısı tarafından bir kişiye özgülenmiştir. Kimlik tespiti şu şekilde gerçekleşir: bir belgeyi (irade beyanını) gönderen kişi bunu gizli anahtarını kullanarak alıcıya gönderir. Göndericinin açık anahtarıyla gizli anahtarının uyumlu olup olmadığı alıcının bilgisayarındaki program ile kontrol edilir. Bunun dışında sertifika kontrolünün de yapılması gerekir. Bu kontrole göre gizli anahtarın açık anahtara uyumu ve sertifikanın geçerli ve kullanılabilir olduğu belirlendiği takdirde belgenin şifre sahibi tarafından gönderildiği ortaya çıkmış olur.

B. Kimlik doğrulama (Authentication)

"*Kimlik doğrulama, kısaca bir nesnenin diğer bir nesneye iddia ettiği varlık olduğunu kanıtlama işlemidir*." Kimlik doğrulamada günümüzde sadece parola kullanılmamakta olup kişinin sahip olduğu ve ya bildiği birçok kimlik doğrulama mekanizmaları bulunmaktadır.[118] Kimlik doğrulama sistemleri artık tekli bir doğrulama sistemi deyil, ikili doğrulama sistemi ağır basmaktadır. İkili doğrulamada kişinin hem sahip olduğu, hem de bildiği iki unsur esas alınmaktadır. Kullanıcının sahip olduğu bir şey, günümüzde internet kullanımı için en başarılı kimlik doğrulama şekli olup sadece tek bir yerde olabilen fiziki bir cihazdır. Bunlar manyetik ya da akıllı kart olabilir[119]. Görüldüğü gibi, bu yönteme göre, bilgi sistemleri üzerinden gerçekleşen işlemler için uygun olan bir kimlik doğrulama mekanizması kurulması, kimlik doğrulama verilerinin tutulduğu veri tabanının güvenliğinin sağlanması zorunludur[120].

C. Güvenlik Duvarı (Firewall)

Firewall bir koruma duvarıdır. Güvenlik sisteminde *Firewall* koruma duvarının oldukça önemli yeri var. Bu koruma duvarı ister internetten, isterse de

---

[118]**Serhateri, A.,** "Elektronik Ticarette Güvenliğin Tüketicilerin İnternet Üzerinden Alışveriş Yapma Tutumlarına Etkisi: Kocaeli Örneği", Karadeniz Uluslararası Bilimsel Dergi, C. 1, S. 27, Y. 2015, s. 227-249.

[119] **Aysal**, **H.,** "Güvenlik ve İnternet Erişim Politikaları Oluşturulması: İstanbul Üniversitesi'nde Uygulama Süreci", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, 2007, s. 126.

[120] **Yüksel-Mermod**, s. 195

diğer ağlardan gelecek muhtemel kısıtlamalara karşımı erişimi kısıtlayarak önleyici bir fonksiyona sahiptir. *Firewall* internet ile ağ arasında bir köprüdür. İnternete gelen veya internetten giden istenilen paketleri kontrol etmek koruma duvarı sayesinde mümkün olur. Dolayısıyla şüpheli dosyalar ve yetkisiz girişler (*log in*) engellenerek yerel ağ veya bilgisayardaki dosyalara, programlara zarar vermeleri önlenebilir[121]. "*Güvenlik duvarı bilgileri denetleyen ve bilgisayarın güvenlik duvarı ayarlarına göre engelleyen veya geçişine izin veren bir yazılım veya donanımdır*."[122]

D. Anti-Virüs Yazılımları

Bilindiyi gibi güvenlik önlemleri sadece "firewall" ile bitmemektedir. Virus programlarının bilgisayata yüklenmesi, yerleşdirildikden sonra güncellenmenin yapılması gerekir. Güvenlik önlemi olarak sadece "*Firewall"* yöntemi yeterli olmayacaktır. Güncelleme konusu ihmal edilmemesi gereken bir işlemdir. Hatta bilgisayarda hiç virüs programı olmaması, eski bir virüs programının çalışıyor olmasından çok daha anlamlıdır. Virüs programının bilgisayara uygulanması kötü sonuçların önüne geçmiş olacaktır. Çünkü virüs koruma programı var diye güvenip korumasız davranmak daha kötü sonuçlar doğurabilir[123]. Bu yöntem virüslerin engellenmesinde ideal çözüm önlemedir. Virüsün sisteme girmesine önceden izin verilmemelidir.[124]

E. Erken Uyarı Sistemleri

Herhangi bir web sitesine karşı üsulsüz erişim ve saldırıların zarar vermesini engellemek amacıyla erken uyarı sistemlerinin kurulması şarttır. Söz konusu güvenlik teknolojilerine sistem, ağ tabanlı yetkisiz erişim ve saldırı saptama sistemlerinin kurulması, tuzak ve yanıltıcı sistemlerin siteye eklenmesi, acil durum planının hazırlanması, sistem bütünlüğü saptama dahildir.

---

[121] Bu kısıtlama, ağ güvenliğinin anlatılacağı bir sonraki başlıkta açıklanan "*paket filtreleme*" yöntemi ile yapılır. Bkz. **Özmen**, s. 509.
[122] **Şahin**, **Y. L.,** "Ağ Güvenliği", Bilgisayar Ağları ve İletişim, Ed. Abdullah Kuzu, Nobel Yayınları, Ankara, 2011, s. 337.
[123] **Özmen**, s. 509.
[124] En iyi yaklaşımlar konusunda ayrıntılı bilgiler için bkz. **Aysal**, s. 125.

Bu sistemler güvenlik yöneticisine atağın niteliği, bu atakdan etkilenen sistemler ve söz konusu sistemlerde güvenlik açıklarını kapama imkânı verir. Onu da belirtmek gerekir ki, bu bilgilere yasal başvurularda delil sağlamak açısından da çok önemlidir[125].

F. Biyometrik Güvenlik Sistemleri

Biyometrik güvenlik sistemleri elektron bankacılıkta esasen kimlik tanımlama ve bankacılık işlemlerinin gerçekleştirilmesi zamanı kullanılmaktadır. Biyometrik güvenlik sistemleri ister internet bankacılıkda ve yahut ATM bankacılıkta kullanıcı tanımlamasında, isterse de çağrı merkezlerinde kimlik tespitinde sıkca kullanılan bir sistemlerdir.

Güvenlik açısından baktığımızda biyometrik güvenlik sistemleri insanların kendine özgü olan biyolojik özelliklerini olduğu gibi aktara biliyor ve her hangi taklit edilme söz konusu olamaz. Nitekim insanların ürettiği şifre, kredi kartları, kimlik kartları ve buna benzer diğer dijital evraklar biyometrik sistemler ile kıyasladığımızda güvenlik açısından bir addım daha geride kalmış oluyor. Biyometrik sistemler parmak izi, el geometrisi, yüz tanıma, retina tanıma, ses tanıma, imza tanıma, DNA tanıma, yazma/tuş basma ritmi tanıma olarak belirleniyor. Bunların içerisinde en yaygın olarak kullanılan ise parmak izi, el geometrisi, yüz, iris, retina, ses, imza olarak sıralanabilir. Bu sıralananların dışında el ve damar tanıma, el yazısı tanıma, yürüyüş tanıma, kulak biyometriğine göre kimlik tespiti tuş vuruşu gibi daha pek çok çeşitli biyometrik sistemler arasında yer almaktadır. [126] Biyometrik sistemlerinde parmak izi, iris ve DNA tanımalarının süreklilik bakımından daha uzun süreli ve az değişikliğe uğradığını dikkate alsak, o zaman elektronik bankacılıkta bunlara daha çok başvurulduğunu anlamak o kadar da zor değildir. İnsan yaşamı boyunca bu özellikler sabit kalır ve her hangi fizyolojik ya da psikolojik bir etkene bağlı olarak değişmezler. Diğer tür tanıma sistemleri olan imza ve ses tanımada ise, imza ve ses biyometrikleri stres, heyecan, korku, kızgınlık,

---

[125] **Kent**, **S.,** "On the Trail of Intrusions Into Information Systems", **IEEE Spectrum**, Vol. 37, Is. 12, Y. December 2000, s. 53 vd.

[126] **Öztuna Cox, B.,** Avrupa Birliği Hukukunda Elektronik Ticaret ve Türkiye'deki Gelişmeler, Pusula Yayıncılık, İstanbul, 2002, s. 46.

üzüntü gibi emosyenel durum ve çevre koşulları ile etkinlendiği için anlık değişimlere bağlı olarak süreklilik arz etmezler. [127]

G. Güvenliğin Boyutları

1. Ağ Güvenliği

Ağ güvenliği elektronik bankacılık hizmetinin sunulması zaman olası saldırganların girmesini ve sistemi kontrol altına alarak her hangi hizmette aksamalara neden olacak girişimlerinin engellenmesi amacıyla sağlanır. Ağ güvenliğinin başında *"firewall"* teknolojisi gelir. Bunlardan ilki paket trafiği uygulamasıdır. Bu uygulamada *firewall"* teknolojisi paketlerin geçişine izin verilir. Paketlerde de filtrelenme oluyor. Bu filtreleme kaynak adresinde, hedef adresine ve portala göre yapılıyor. Bu ağ güvenliyinin sağlanmasında Proxy sunucularının da kullanılması görünmektedir. Burada proxy sunucuları ülke dışında "IP" numarası gösterir, diğer taraftan yerel ağ üzerindeki "İP" adreslerini gizleyerek bunları muhtemel saldırılardan korur. Diğer bir uygulama olan özel sanal ağlar ise "IP" geçitlerinin şifrelenmesini ifade etmektedir. Söz konusu özel sanal ağlar şifrelenmiş "IP" geçitleri veya herkese açık ağlar aracılığı ile oluşturulmaktadırlar[128].

2. Sistem Güvenliği

Sistem güvenliği, sistemin işleyişini bozacak ve işletmenin hizmet vermesini engelleyecek faktörlerin ortadan kaldırılmasıdır. Güvenlik sistemi, güvenliğin diğer iki boyutu olan ağ ve veri iletişim güvenliği ile ilgili tedbirleri ve uygulamaları da içerir. Güvenlikten sorumlu kişilere, sistem güvenliği ile ilgili politikalar ve kurallar açıklanır. Sistem güvenliğinin sağıanması için en önemli kurallarından biri, güvenlik önlemlerinde açıklandığı gibi, kullanıcılara kimlik numarası (*identification number - ID no*) verilmesidir. Kişiye verilen kimlik numarası onun yetki ve sorumluluğuna göre belirlenir. Kişinin internet ortamında erişeceyi dosyaya uygun farklı kimlik numaraları verilebilmektedir. Bu şekilde verilen erişim numaraları hem de

[127] **Yalçın, N./Gürbüz, F.,** Biyometrik Güvenlik Sistemlerinin İncelenmesi, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3 (2015), s. 410
[128] **Özmen**, s. 511.

kısıtlamalara maruz kala bilir. Bunun yanında takip edilecek bir kontrol sistemi de sağlanabilir.[129].

3. İşlem (*Transaction*) Güvenliği

Elektronik bankacılıkta gereken güvenliğin sağlanması bakımından iki önemli güvenlik programlarının gözden geçirilmesinde fayda vardır. *Secure Sockets Layer (SSL) ve Secure Electronic Transaction (SET).* Bunlar tez çalışmamızda ilerideki bölümlerde bilgi olarak yer alacaktır.

a. Güvenli Yuvalar Katmanı (*Secure Sockets Layer/SSL*)

SSL, internet ortamında en sık kullanılan güvenlik-şifreleme yazılımlarından biridir. SSL güvenli alışverişi garantiler. SSL sadece ödeme işlemleri için değil, internet ortamında verilerin de iletilmesinde kullanılır. Güvenli mesaj alışverişini sağlamak için geliştirilmiş olan SSL, sadece ödeme sistemlerinde değil, internette güvenlik gerektiren her türlü veri iletiminde kullanılabilir. "*Netscape yazılım şirketi tarafından geliştirilmiş bir şifreleme yazılımı olup, bütün yaygın web tarayıcıları (browser) ve sunucuları (server) tarafından desteklenen bir protokoldür*." SSL protokolünde, her iki taraf - hem istemci (bilgi alan), hem de sunucu (bilgi gönderen) bilgisayarın kimliği karşı tarafta doğrulanabilir (*authentication*). Böylece, SSL istemci kişi ile sunucu arasında güvenli bir hat açar. SSL protokolünde taraflar imzalanmış bir sertifikat kullanırlar. Sertifikanın noter onaylı olmasına özen gösterilir. Sertifika aslında, noter onaylı kimlik fotokopisinin dijital versiyonudur. Sunucunun sahibi olan şirket bir notere (sertifikat otoritesine) kimlik bilgilerini ibraz ederek başvurur ve noter damgalı bir dijital sertifika edinir[130].

b. Güvenli Elektronik İşlem (Secure Electronic Transaction/SET)

SET güvenlik protokolü olup, dünyada tanınan VISA, Mastercard, Netscape, GTE, IBM, SAIC, Terisa Systems ve Verisign gibi şirketlerden oluşan bir konsorsiyum tarafından geliştirilmişdir. Dijital ortamda tüm alışverişler SET

[129] **Özmen**, s. 512.
[130] **Özmen**, s. 474; 513-514.

protokolü ile gerçekleştirilir. İşlemler ilgili bilgileri yalnız ilgili taraflar görebilmektedirler. Meselâ, kredi kartı bilgisi hem banka, hem de satıcı tarafından görülür.

SSL'de olduğu gibi SET sisteminde de bilgilerin şifrelenmesi söz konusu olmaktadır. Çift şifre anahtarı kullanılmaktadır: Özel anahtar (*private key*) ve genel anahtar (*public key*). Bilgiler genel anahtar ile şifrelense de, özel anahtar ile çözülebiliyor. Bu niteliği itibariyle sistem yüksek güvenlik özelliğine sahiptir. Banka kredi kartı kullanılmasında öncelikle birer SET sertifikası alınmalıdır. Bu sertifika bilgisayara yüklenmelidir. Bilgisayara yüklenme zamanı kredi kartı bilgileri programa tanıtılmalıdır. Bir kart kullanıcısının geçrek kart sahibi olduğunu yalnız işlem sırasında SET sertifikası teyit ede bilir, bununla da bu sertifika aracılığı ile ödemeye ilişkin bilginin gizliliği, işyerinin banka ile anlaşmalı bir iş yeri olduğunu garanti altına alır.[131]

[131] Özmen, s. 476-478.

İKİNCİ BÖLÜM

ELEKTRONİK BANKACILIK HİZMETLERİ VE ELEKTRONİK BANKACILIKTA BANKANIN ÖZEN YÜKÜMLÜLÜĞÜNÜN HUKUKİ NİTELİĞİ, KONUSU, ÖLÇÜSÜ VE UYGULAMA HÂLLERİ

Elektronik bankacılıkta bankaların özen yükümlülüğünün hukuki niteliği ve uygulanma alanına ilişkin değerlendirmelere geçmeden önce "elektronik bankacılık hizmeti" kavramından ne anlaşılması gerektiği açıklanmalıdır. Zira bankanın özen yükümlülüğünün uygulanma alanı, büyük ölçüde, bu hizmetlerin sunulmasıyla ilgili olarak ortaya çıkmaktadır. Diğer yandan, elektronik bankacılıkta banka-müşteri ilişkisinin akdî niteliği çalışmamızın kapsamı çerçevesinde elektronik bankacılık hizmeti sözleşmesiyle ilgili bazı önemli noktalara temas edilmesini gerekli kılmaktadır.

§ 1. Elektronik Bankacılık Hizmetinin Tanımı ve Türleri

I. Tanımı

Son yıllarda internet, kamu ve özel bilgisayar ağlarında görülen çarpıcı genişleme finansal kuruluşlara geleneksel hizmetleri yeni elektronik araçlar vesilesiyle sunma imkânı tanımıştır. Geleneksel bankacılık hizmetlerinin teknolojik gelişmeler ve inovasyonlarla buluşması sonucunda karşımıza elektronik bankacılık hizmetleri çıkmaktadır. BBSEBHY'nin 3. maddesinin 1. fıkrasında elektronik bankacılık hizmetlerine verilmiş tanımdan hareketle, söz konusu hizmetlerin temel özelliklerini açıklayabiliriz.

Elektronik bankacılık hizmetlerinin ilk özelliği, geleneksel bankacılık hizmetlerinin elektronik ortamda[132] sunulmasıdır. Şöyle ki, alternatif dağıtım kanallarının kullanılmasıyla birlikte bankacılık faaliyetinin konusunda, kural olarak

---

[132] Elektronik ortam, kişilerin iradelerinin sayısallaştırılmış veriler aracılığıyla açıklandığı, kapalı veya açık bilgisayar ağlarını, aynı zamanda, elektronik fon transferi, elektronik veri değişimi gibi olguları da kapsayan her türlü platformu ifade eder (Sinan Sami Akkurt, "Elektronik Ortamda Hizmet Sunumu Ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri", AÜHFD, C. 60, S. 1, Y. 2011, s. 25-26).

değişiklik yaşanmamıştır. Ancak bankacılık faaliyetinin uygulanmasının usulü ve şartları açısından köklü değişim söz konusudur. Bu anlamda, elektronik bankacılık hizmetleri, geleneksel bankacılık hizmetlerinin müşterilere yeni "taşıtlar" kullanılmakla sunulmasını ifade etmektedir[133]. Çoğu elektronik bankacılık hizmetleri artık iki kişi (müşteri ve banka elemanı) arasında değil, ağırlıklı olarak elektronik sistemler yoluyla sağlanmaktadır. Başka bir deyişle, elektronik bankacılıkta müşteriler bilgi edinmek veya herhangi bir bankacılık işlemini gerçekleştirmek amacıyla banka şubesine gitmek zorunda değildir. Bu anlamda, elektronik bakacılıkta banka-müşteri ilişkisi mesafeli olarak yürütülmekte ve müşteri, deyim yerindeyse, bir çeşit banka elemanına "dönüşmektedir"[134]. Söz konusu dönüşümü, hiç şüphesiz, elektronik bankacılık teknolojilerini kullanmakla banka şubesinden dışarıda müşterilere çeşitli bankacılık hizmetlerinin sunulmasına imkân tanıyan otomatik banka sistemleri sağlamaktadır. Meselâ, elektronik havalede, müşterinin havale talimatı bankanın bilgi işlem sistemine ulaşmakta ve sistem, programlandığı şekilde gerekli şartların (mesela, müşterinin hesabında yeterli karşılık bulunup bulunmaması vb.) mevcut olup olmadığından hareketle bu talimatı yerine getirmektedir. Ancak bazı bankacılık hizmetleri istisna oluşturmaktadır. Meselâ, telefon bankacılığında müşteri banka temsilcisi ile görüşmekte ve istediği işlemi onun aracılığıyla gerçekleştirmektedir.

Elektronik bankacılık hizmetlerinin diğer bir özelliği, kural olarak, mekan veya zaman bakımından sınırsız olarak, çok geniş müşteri çevresine sunulabilmesidir[135]. Elektronik bankacılık hizmetlerinin kural olarak, zaman ve mekan açısından sınırsız olarak erişilebilirliği bu hizmetleri müşteriler için cazip kılan en etkili husus olarak karşımıza çıkmaktadır. Zira alternatif dağıtım kanalları, hizmet personelinden farklı olarak, çalışma saatlerine bağımlı olmaksızın 7 gün 24 saat çalışabilmektedir[136]. Ancak hemen belirtelim ki, bu özellik, tüm alternatif dağıtım kanalları açısından geçerli değildir. Meselâ, ATM veya POS cihazları

---

133 **Vitalyeviç, L. L., Primenenie Tekhnologiy Elektronnoqo Bankinga. Risk-Orientirovannıy Podkhod**, KNORUS Yayınevi, Moskva, 2011, s. 10.

134 **Lyamin,** s. 9; Fundamentals of Service Systems, **Ed. Jorge Cardoso** v.d., Springer, 2015, s. 37.

135 **Türk, A.,** Hukuki Yönden Banka Havalesi, Yetkin Yayınları, Ankara, 2007, s. 304.

136 **Cardoso**, s. 37.

aracılığıyla gerçekleştirilen hizmetler doğal olarak, mekan bakımından sınırlı olmaktadır; buna mukabil, internet bankacılığı açısından böyle bir zaman veya mekan sınırlaması söz konusu değildir.

II. Türleri

Elektronik bankacılık hizmetleri farklı kıstaslardan hareketle sınıflandırmaya tabi tutulmaktadır.

A. Hizmetten Yararlanan Müşterilere Göre

Elektronik bankacılık hizmetlerinden yararlanan kişilere göre yapılan bu ayrım uyarınca, bankacılık hizmetleri bireysel ve ticarî bankacılık hizmetleri olarak iki altbaşlık şeklinde incelebilir[137]. Bireysel bankacılık hizmetleri, tüketici gerçek kişiler tarafından kullanılan hizmetleri kapsamaktadır. Mesela, üniversite harç ödemesi vb.

Ticarî bankacılık hizmeterli ise, tacir tüzel kişiler tarafından kullanılan hizmetleri ifade etmektedir. Meselâ, vergi ödemesi, çeşitli yatırım işlemleri vb.

Böyle bir ayrımın önemi, taraflar arasındaki ilişkilere uygulanacak hukuk açısından da önem arz etmektedir. Zira 6502 sayılı Tüketicilerin Korunması Hakkında Kanun[138] (TKHK), tüketicilere ilişkin özel koruyucu hükümleri öngörmektedir.

B. Hizmetin Kapsamına Göre

Bu kriterden hareketle bankacılık hizmetleri bilgi sağlanmasına yönelik hizmetler ve işlem yapılmasına yönelik hizmetler olmakla sınıflandırılabilir[139]. Bilgi sağlanmasına yönelik bankacılık hizmetleri müşterilere finansal bilgiler

---

137 **Distançionnoe Bankovskoe Obslujivanie**, s. 11.

138 28.11.2013 tarihli, 28835 sayılı RG.'de yayımlanmıştır.

139 **Türk**, s. 306; **Distançionnoe Bankovskoe Obslujivanie,** s. 12; **Shah, M./Clarke, S.,** E-Banking Management: Issues, Solutions, and Strategies, Information Science Reference, New York, 2009, s. 2.

sağlanmasına ilişkindir. Meselâ, hesab bakiye sorgulaması, kredi başvurusunda bulunma gibi.

İşlem yapılmasına yönelik bankacılık hizmetleri çeşitli finansal işlemlerin gerçekleşmesine yönelik hizmetlerdir. Mesela, para transferleri ve ödemeler (hesaplar arası transfer, hesaba havale, isme havale vb.), kredi başvurusunda bulunma gibi.

C. Hizmetin Sağlanmasında Kullanılan Alternatif Dağıtım Kanalına Göre

Bu kriter uyarınca yapılan ayrımın temelinde bankacılık hizimetinin sağlanmasında kullanılan araç türleri (alternatif dağıtım kanalları) dayanmaktadır. Mesela, ATM'ler, Internet Bankacılığı, Satış Noktası Terminali (POS), Mobil Bankacılık vs. Yukarıda elektronik bankacılığa ilişkin temel kavramlar çerçevesinde bu konuda gerekli açıklamalar yapıldığından burada tekrara gidilmemiş ve yalnızca anılan açıklamalarımıza yollamada bulunulmakla yetinilmiştir.

D. Teknolojinin Hizmetin Sağlanmasındaki Rölüne Göre

Bu kriter uyarınca, elektronik bankacılık; teknoloji tarafından üretilen hizmetler[140] ve teknoloji-aracılık hizmetleri olarak gruplandırılabilir. Teknoloji tarafından üretilen hizmetlerde, banka elemanının yerini tümüyle teknoloji tutmaktadır[141]. Meselâ, kredi kartları, akıllı kartlar, kişinin bankadakı bir hesabından diğerine para aktarması, ATM'den para çekmesi gibi. Banka elemanının yerini tutan teknoloji, mekanik ve elektronik cihazların karışımı (ATM) veya tümüyle elektronik (ev/ofis bankacılığı) şekilde olabilir[142].

---

[140] **Türk**, bu tür hizmetleri interaktif bankacılık hizmetleri olarak tanımlamaktadır. Yazara göre, İnteraktif bankacılık hizmetleri, internet ortamında birey ile makine arasında herhangi bir banka yetkilisinin aracılığı olmaksızın iletişim kurulması suretiyle gerçekleştirilen hizmetlerdir (**Türk**, s. 303).

[141] **Cardoso**, s. 39.

[142] **Cardoso**, s. 39.

Teknoloji-aracılık hizmetlerinde, müşteriler ve banka yüz yüze iletişim hâlinde değildir. Bu tür hizmetler müşterilere mesafeli olarak (yani banka şubesine gelmeksizin, banka çalışanı ile yüz yüze gelinmeksizin) sağlansa bile hizmetin gerçekleştirilmesi sürecinde banka yetkilisinin direkt katılımını gerekli kılmaktadır[143]. Meselâ, uluslar arası havalelerde kullanılan ve elektronik bankacılığa dâhil olan S.W. I. F. T. sisteminde müşterinin doğrudan sisteme girmesi olanağı yoktur[144].

E. Sağlanan Hizmetin Konusuna Göre

Elektronik bankacılık çerçevesinde sağlanan hizmetler konuları açısından üç grupta toplanabilir[145]. Birinci grup hizmetlere temel bankacılık hizmetleri dâhildir. Meselâ, mevduatın kabulü, fon transferleri, hesap ekstreleri vb[146]. İkinci grup hizmetlere, internet üzerinden kredi başvurularının kabul edilmesi, tüketici veya ticari amaçla kredi verilmesi gibi cari hesapla bağlantılı işlemler dâhildir[147]. Nihayet, son grup hizmetler, internet üzerinden aracılık ve kıymetli evrak ticaretini kapsamaktadır[148]. Bu hizmetler çerçevesinde müşteri bankaya kıymetli evrakın alım-satımına ilişkin talimat vermekte, banka da internet üzerinden bu talimatları kendisi adına, ancak müşterisinin hesabına yerine getirmektedir.

§ 2. Elektronik Bankacılık Hizmetleri Sözleşmeleri

I. Genel Olarak

Bankalar tarafından sunulan çok çeşitli hizmetler ve bu hizmetlerden yararlanan müşterilerin farklılığı banka ve müşteri arasındaki sözleşme ilişkisini de etkilemektedir. Yalnız bir bankacılık işleminin gerçekleştirilmesine yönelik sözleşmeler (“Bir İşlem-Bir Sözleşme”) açısından her şey daha açık ve sade

---

143 **Cardoso**, s. 39.
144 **Türk**, s. 303.
145 **Gkoutzinis**, **A.,** Internet Banking And The Law In Europe, Cambridge University Press, 2006, s. 22-23.
146 **Gkoutzinis,** s. 22.
147 **Gkoutzinis,** s. 23.
148 **Gkoutzinis**, s. 23.

görünebilir; meselâ, bir turistin bankada döviz bozdurması gibi[149]. Fakat banka ve müşteri arasındaki sözleşme ilişkileri çoğu zaman bu kadar basit olarak karşımıza çıkmaz. Konuyu elektronik bankacılık açısından ele alırsak, müşterinin alternatif dağıtım kanalları aracılığıyla hesap bilgilerine ve çeşitli bankacılık hizmetlerine ulaşması ve müşterinin anılan kanallar yoluyla beyan ettiği talimatlarının banka tarafından yerine getirilmesi banka-müşteri ilişkisinde olağan (alışılagelmiş) bir unsur değildir. Elektronik bankacılık hizmetleri, banka ve müşterinin bu hizmetlere erişilmesi ve kullanılmasına ilişkin hak ve yükümlülüklerini düzenleyen ayrı bir sözleşmenin mevcudiyetini gerekli kılmaktadır. Elektronik bankacılık hizmetleri sözleşmesi olarak adlandırabileceğimiz bu sözleşme gereğince, banka, gerek bilgi sağlanmasına, gerekse işlem yapılmasına yönelik hizmetlerin sürekli olarak alternatif dağıtım kanalları aracılığıyla sağlanmasını, müşteri ise anılan hizmetler karşılığında belirli ücret veya komisyonları ödemeyi taahhüt etmektedir. Elektronik bankacılık hizmetleri sözleşmesi, alternatif dağıtım kanallarının müşterinin (vekalet verenin) farklı konulardaki (fon transferi, hesap hareketlerine ilişkin bilgi alınması, kredi kartı ödemesi vb.) talimatlarının bankaya ulaştırılmasında kullanılmasına imkân tanımaktadır. Doktrinde vurgulandığı gibi, banka ile müşteriler arasında sözleşme ilişkileri genel işlem şartları, standart sözleşmeler ve münferit sözleşmelerle tanzim edilmektedir[150]. Standart sözleşme şeklinde kurulan elektronik bankacılık sözleşmeleri kural olarak, erişim hakları, hesap sahiplerinin kimlik doğrulaması, güvenlik önlemleri, hizmetin sağlanmasında ortaya çıkabilecek aksaklıklar ve yetkisiz kullanım veya dolandırıcılık durumlarında sorumluluğa ilişkin hükümleri içermektedir[151].

Belirtmek gerekir ki, banka ile müşteri arasındaki tüm karmaşık sözleşme ilişkilerinde odak noktasını banka hesabı oluşturmaktadır[152]. Cari hesap, banka ile müşterinin birbirlerindeki alacaklarını belirli bir hesap dönemi süresince veya belli bir miktara kadar karşılıklı olarak ayrı ayrı istemekten vazgeçmeleri, dönem sonunda

---

149 **Wiegand, W.,** "Legal Aspects of the Bank-Customer Relationship in Electronic Banking", Legal Issues in Electronic Banking, Ed. Norbert Horn, Kluwer Law International, Netherlands, 2002, s. 165.

150 **Kaplan, İ.,** Banka Sözleşmeleri Hukuku, C. 1, Dayınlarlı Yayıncılık, Ankara, 1996, s. 22.

151 **Gkoutzinis**, s. 35-36.

152 **Wiegand**, s. 165; **Türk**, s. 312-313; **Gkoutzinis**, s. 30; **Tekinalp, Ü.**, Banka Hukukunun Esasları, Yeniden Yazılmış 2. bs.,Vedat Kitapçılık, İstanbul, 2009, s. 441 vd.

veya belli miktara ulaşınca, çıkan hesap bakiyesini alacak olarak talep etmeyi kararlaştırdıkları bir hesap türü olarak tanımlanmaktadır[153]. Elektronik bankacılık hizmetleri de istisna teşkil etmemektedir. Yani bankada cari hesabı bulunmayan müşterinin elektronik bankacılık hizmetlerinden faydalanması mümkün olmamaktadır. Uygulamada bankalar kural olarak, müşteri ile bankacılık hizmetleri sözleşmesi yapmakta ve bu sözleşme çerçevesinde müşteriye banka hesabı açılmaktadır. Söz konusu bankacılık hizmetleri sözleşmesi kapsamında elektronik bankacılık hizmetlerinin düzenlenmesine ilişkin kurallara da yer verilmektedir.

II. Hukukî Niteliği

Bilindiği üzere, kanunda düzenlenmiş olup olmamaları kıstasından hareketle sözleşmeler "isimli sözleşmeler" ve "isimsiz sözleşmler" olarak iki grupta toplanmaktadır. "İsimli sözleşme" kavramı, kanunda özel olarak, detaylı bir şekilde düzenlenmiş olan sözleşmeleri (satım, vekalet, eser ve s.) ifade eder. Buna karşılık, eğer kurulan sözleşmenin objektiv esaslı noktalarının kanunda düzenlenmiş bir isimli sözleşmenin objektiv esaslı noktaları ile örtüşmezse, "isimsiz sözleşme"nin varlığı söz konusu olur[154]. Doktrinde[155] "isimsiz sözleşmeler" üç ayrı başlık altında incelenmektedir: bileşik sözleşmeler, karma sözleşmeler ve kendine özgü yapısı olan (sui generis) sözleşmeler.

Hukukî nitelikleri acısından tamamen bağımsız olan sözleşmelerin tarafların serbest iradeleri ile (iktisadî) fonksiyon itibariyle birbirine bağlanmasıyla oluşan sözleşmeler bileşik sözleşmelerdir[156]. Bu durumda, bağımsız sözleşme niteliklerini

---

153 **Tekinalp**, s. 448 vd.; **Kaplan**, Sözleşme, s. 171-172.

154 **Aral/Ayrancı**, s. 53 vd; **Gümüş**, Özel Hükümler, C 1, s. 4; **Yavuz, C./Acar, F./Özen, B.,** Türk Borçlar Hukuku Özel Hükümler, Yenilenmiş 10. Bası, Beta Basım Yayın, İstanbul, 2014, s. 22 vd.; **Eren, F.,** "*İsimsiz Sözleşmelere İlişkin Bazı Sorunlar",* Prof. Dr. Turgut Akıntürk'e Armağan, Beta Basım Yayın, Ankara, 2008, s. 86; **Oktay, S.,** "*İsimsiz Sözleşmelerin Geçerliliği, Yorumu ve Boşlukların Tamamlanması*", İstanbul Hukuk Fakültesi Mecmuası, C. LV, 1996, s. 267-268.

155 **Eren**, İsimsiz Sözleşme, 90 vd.; **Oktay**, s. 272 vd.; **Aral, F./Ayrancı, H.,** Borçlar Hukuku Özel Borç İlişkileri, 11. bs., Yetkin Basımevi, Ankara, 2015, s. 56 vd.; **Yavuz/Acar/Özen,** s. 23 vd.; Gümüş, söz konusu isimsiz sözleşme tipleri yanında "eksik sözleşme" kavramını kullanmakta ve "eksik sözleşme"leri isimsiz sözleşme tiplerinden biri olarak kabul etmekdedir. Yazar'a göre, eksik sözleşme kanunda düzenlenmiş belirli bir sözleşme tipine ilişkin unsurları bir veya birkaç unsuru eksiğiyle içeren sözleşmelerdir. Mesela, müteahide ücret ödenmesi unsurunu içermeyen (ivazsız) eser meydana getirmeye yönelik sözleşme.Bkz. **Gümüş**, Özel Hükümler, C 1, s. 11.

156 **Yavuz/Acar/Özen**, s. 23; **Aral/Ayrancı**, s. 60; **Oktay**, s. 275.

koruyan iki veya daha çok sözleşme varlık, işleyiş ve geçerlilik yönünden birbirine bağlanmaktadır[157].

Karma sözleşmeler, kanunun düzenlediği çeşitli sözleşme tiplerine ait unsurların, özellikle aslî edimlerin yasanın tespit etmediği tarzda biraraya gelmesiyle kurulan sözleşmelerdir[158]. Doktrinde bazı yazarlar dar anlamda ve geniş anlamda karma sözleşmeler ayrımını yapmaktadırlar. Buna göre; geniş anlamda karma sözleşmeler, kanunda düzenlenmiş veya düzenlenmemiş sözleşmelere ait unsurların karışımı olarak ortaya çıkan sözleşmelerdir[159]. Buna mukabil, dar anlamda karma sözleşmeler, yalnız kanunda düzenlenmiş sözleşmelere ait unsurları içeren sözleşmeler olarak tanımlanmakta, geniş anlamda karma sözleşme kavramının kabulünün karma sözleşme ile kendine özgü yapısı olan (sui generis) sözleşmelerin birbirinden ayırt edilmesini zorlaştırdığı belirtilmektedir[160].

Nihayet, kendine özgü yapısı olan (sui generis) sözleşmeler, kanunda düzenlenen sözleşme tiplerinde öngörülmemiş unsur veya unsurları içeren, böylelikle de, tamamen yeni bir oluşumu yansıtan sözleşmelerdir[161].

Elektronik bankacılık hizmetleri sözleşmesinin hukukî niteliğine ilişkin değerlendirmeye geçmezden önce şu önemli noktaya temas etmekte fayda görüyoruz. Bankacılık uygulamasında elektronik bankacılık hizmetlerinin sağlanmasına ilişkin farklı sözleşmeler kullanılmaktadır. Meselâ, kart hamili, banka kartı sözleşmesi çerçevesinde verilmiş kartın yurtiçi ve yurtdışındaki üye işyerlerinde mal ve hizmet alımı karşılığı ödeme aracı olarak kullanabileceyi gibi, karttan otomatik vezne makinelerinde (ATM) ve diğer dağıtım kanallarında nakit çekim araçı olarak da fayadalanabilmektedir. Ancak banka kartı sözleşmesi müşteriye Internet bankacılık hizmetlerinden yararlanmak imkânı tanımaz. Çünkü banka kartı aracılığıyla ATM'den para çekilmesi bir elektronik bankacılık hizmeti olarak

---

157 **Eren**, İsimsiz Sözleşme, s. 101.

158 **Aral/Ayrancı**, s. 57; **Yavuz**, s. 25; **Oktay**, s. 273 vd; **Eren**, İsimsiz Sözleşme, s. 91.

159 **Aral/Ayrancı**, s. 57, dn. 22'de belirtilen yazarlar; **Eren**, İsimsiz Sözleşme, s. 91, dn. 28'de belirtilen yazarlar.

160 **Aral/Ayrancı**, s. 57; **Eren**, İsimsiz Sözleşme, s. 91-92; **Gümüş**, Özel Hükümler, C 1, s. 7;

161 **Gümüş**, Özel Hükümler, C 1, s. 9; **Eren**, İsimsiz Sözleşme, s. 99; Ancak diğer bir görüş uyarınca, kendine özgü yapısı olan (sui generis) bir sözleşme kısmen veya tamamen, kanunda düzenlenmiş sözleşme tiplerinde bulunmayan unsurlardan meydana gelir. Bu konuda bkz. **Yavuz/Acar/Özen**, s. 29; **Aral/Ayrancı**, s. 56.

nitelendirilebilir, ancak bu, Internet bankacılık hizmeti değildir. Aynı şekilde, müşteri yalnızca Internet bankacılık hizmetlerinden yararlanmak istiyorsa, banka ile banka kartı sözleşmesinin kurulması gerekmemektedir.

Görüldüğü üzere, müşterinin yararlanmak istediği elektronik bankacılık hizmetlerinin kapsamı kurulan elektronik bankacılık sözleşmesinin türünü belirlemektedir. Şu anlamda, müşteri, genel elektronik bankacılık sözleşmesi çerçevesinde gerek banka kartı elde ede, gerekse de Internet bankacılığını kullanabilir. Ancak müşteri daha dar kapsamlı elektronik bankacılık hizmetlerinden (mesela, Internet bankacılığından) faydalanmak istiyorsa, bu konudakı münferit sözleşmenin kurulması söz konusu olur. Şu açıdan baktığımızda, elektronik bankacılık hizmetlerinin sağlanmasına ilişkin tek bir sözleşmenin varlığından daha çok, sunulan hizmetin kapsamına bağlı olarak kurulan münferit elektronik bankacılık hizmetleri sözleşmelerinden bahsetmek daha doğru olur.

Nitekim doktrinde Internet bankacılığı sözleşmesinin hukukî niteliğine ilişkin farklı görüşler ileri sürülmektedir. Şöyle ki, bir görüş, Internet bankacılık sözleşmesinin karma nitelikte bir sözleşme olarak değerlendirmektedir[162]. Buna mukabil, diğer bir görüş, Internet bankacılık sözleşmesinin kendine özgü yapısı olan (sui generis) bir sözleşme olarak nitelendirilmesinin daha doğru olduğunu savunmaktadır[163]. Zira Internet bankacılık hizmetleri sözleşmesi kanunda öngörülmeyen akdî edimleri bir araya getirmektedir; hatta bu sözleşmeye hukuki özelliğini veren edimler kanunda yer almayan edimlerdir[164]. İsimsiz sözleşme tiplerine ait yukarıda değinilen görüşler doğrultusunda, Internet bankacılık hizmetleri sözleşmesinin kendine özgü yapısı olan (sui generis) bir sözleşme olduğu kabul edilmek durumundadır.

Kredi kartı sözleşmeleri açısından ise doktrinde farklı görüşler ileri sürülmektedir. Şöyle ki, doktrinde ileri sürülen bir görüş, kartı çıkaran kurumun kart hamiline karşı yüklendiği temel borç dikkate alınarak, kredi kartı sözleşmesini

---

162 Wolfgang Wiegand ve Mario Marti, **Türk**, s. 313, dn. 103'den naklen.

163 **Türk**, s. 313; **Yılmaz, S.,** Hukukî Açıdan Internet Bankacılığı, Yetkin Yayınları, Ankara, 2010, s. 85.

164 **Türk**, s. 313; **Yılmaz, S.,** s. 85.

hizmet sözleşmesi olarak nitelendirmiştir[165]. Diğer bir görüş uyarınca, kredi kartı sözleşmesi, içinde birden fazla sözleşme türüne ait edimlerin bir arada bulunduğu çerçeve niteliğinde sürekli, kendine özgü (sui generis) bir sözleşmedir[166]. Nihayet, başka bir görüş[167], kredi kartı sözleşmesine ilişkin hükümlerin TKHK'da (m. 22/2) öngörülmesinden sonra söz konusu sözleşmenin artık isimsiz sözleşme olarak değerlendirilmesini mümkün görmemektetir.

Fikrimizce, kredi kartı sözleşmesinin hizmet sözleşmesi olarak nitelendirmek isabetli olmaz. Şöyle ki, hizmet sözleşmesi acısından geçerli olan bağımlılık ilişkisi kredi kartı sözleşmesinde bulunmamaktadır. Zira bankanın, müşterinin denetimine bağlı olarak çalışması söz konusu değildir.

TKHK ile getirilen düzenleme sonrası kredi kartı sözleşmesinin artık isimli sözleşme olarak nitelendirilmesi gerektiğine ilişkin görüş tartışmaya açıktır. Şöyle ki, kanunkoyucu, tüketici kredisi sözleşmelerine ilişkin düzenleme getirmiş, kredi kartı sözleşmesini, tüketici kredisi sözleşmesi başlığı altında hükme bağlamıştır. Ancak TKHK'nın kredi kartına ilişkin düzenlemeleri söz konusu sözleşmelere özgü tüm unsurları içermemektedir. Dolayısı ile, kredi kartı sözleşmesini kendine özgü sözleşme olarak nitelendirmek daha isabetli olur.

Burada dikkat edilmesi gereken diğer bir husus, banka ve müşteri arasındaki borç ilişkisinde birbirinden farklı, fakat aynı zamanda bir biriyle sıkı ilişkide olan iki ayrı borç ilişkisinin varlığıdır. Şöyle ki, banka ve müşteri arasında kurulmuş olan herhangi bir sözleşme (meselâ, mevduat sözleşmesi) ilişkisi taraflar arasında farklı hak ve yükümlülükler doğurabilir. Taraflar arasında elektronik bankacılık hizmetlerinin kurulması ile birlikte, alternatif dağıtım kanallarının kullanılmasına ilişkin şartlar banka ve müşteri arasındakı diğer sözleşme (meselâ, mevduat sözleşmesi) ilişkisinden doğan hak ve yükümlülüklerle yan yana mevcut olmaya devam eder. Başka bir ifadeyle, banka, borç ilişkisi çerçevesinde sunduğu

---

[165] **Teoman Ö.**, Hukuki Yönden Kredi Kartı Uygulaması, 2. bs., Beta Yayımevi, İstanbul, 1996, s. 168; **Altıparmak Y.**, Kredi Kartı Sözleşmesi, 6502 sayılı Tüketicinin Korunması Hakkındaki Kanun Hükümlerine göre Tüketici Hukuku Uygulamalarında Tüketicinin Korunması, Ed. Sütçü S.S., Seçkin Yayınevi, Ankara, 2019, s. 215.

[166] **İşgüzar, H.,** Banka Kredi Kartı Sözleşmeleri, Yetkin Yayınları, Ankara, 2003, s. 67; **Zevkliler A./Özel Ç.,** Tüketicinin Korunması Hukuku, 1. bs., Seçkin Yayınevi, Ankara, 2016, s. 234.

[167] **Tüzüner, Ö.,** "Banka Kredi Kartı Sözleşmesinin Hukuki Niteliği ve Kart Hamili Bakımından Avantajlarının Sorgulanması", Bankacılık Sektöründe Tüketici Hukuku Uygulamaları, Ed. Hakan Tokbaş ve Ali Suphi Kurşun, Aristo, Yayınevi, İstanbul, 2015, s. 173.

hizmetlerin geleneksel değil, alternatif dağıtım kanalları aracılığıyla sağlanması yükümlülüğü altına da girmiş olur. Sonuç itibariyle, kavramsal olarak farklı bir sözleşme olan elektronik bankacılık hizmetleri sözleşmesi, alternatif dağıtım kanallarının kullanılması şartlarını banka ve müşteri arasında kurulmuş daha kapsayıcı bir sözleşmeyle bütünleştirmiş olmaktadır[168].

Diğer yandan, elektronik bankacılık hizmetleri sözleşmelerini işgörme amacı güden sözleşme olarak da nitelendirmek mümkündür[169]. Mesela, müşteri internet bankacılığını kullanarak ödeme talimatı verdiğinde, banka ödemeni gerçekleştirmekle işgörme edimini yerine getirmiş olur. Aynı fikir, banka kartı sözleşmesi bakımından da geçerlidir. Mesela, banka ATM'nin güvenliğini ve bakımını sağlamakla mükelleftir. Bu durumda, TBK'nın 502. maddesinin 2. fıkrası gereğince, vekalete ilişkin hükümler, niteliklerine uygun düştükleri ölçüde, elektronik bankacılık hizmetleri sözleşmesine de kıyasen uygulanır.

§ 3. Bankanın Özen Yükümlülüğünün Hukukî Niteliği

I. Genel Olarak

"Özen", kelime olarak günlük kullanımda "itina", "fazla dikkat etme", "bir işi yaparken gösterilen özel dikkat", "ihtimam" gibi anlamlara gelmektedir[170].

"Özen" kelimesinin[171] kullanılmasına rağmen TBK ve bankaların faaliyetini düzenleyen mevzuatta "özen" kavramının tanımına yer verilmemiştir. Doktrinde[172], "özen" kavramının tanımının kanunda yapılmamasının, kanun koyma tekniği açısından isabetli olduğu vurgulanmıştır. Zira anılan kavramın zaman, sosyal ve teknolojik gelişmeler karşısında değişime uğramaya elverişliliği dikkate alınırsa, bir

---

168 **Gkoutzinis**, s. 35.

169 **Kaplan'a** göre, "bankaların müşterilerin çeşitli hizmetlerini yürüttüğü sözleşmeler ise genellikle vekalet akdi niteliğindedir. ... diğer akitler hakkındaki kanuni hükümlere tabi olmayan işlerde dahi vekalet akdi hükümleri uygulanacaktır" (**Kaplan, İ.,** "Bankanın Hukuki Sorumluluğu", Prof. Dr. Haluk Tandoğan'ın Hatırasına Armağan, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1990, s. 455); Aynı yönde: **Tekinalp**, s. 504.

170 **Başpınar,V.,** Vekilin (Avukatın, Hekimin, Mimarın, Bankanın) Özen Borcundan Doğan Sorumluluğu, 2. bs., Yetkin Yayınları, Ankara, 2004, s. 122.

171 TBK'nın 66. maddesinde adam çalıştıranın sorumluluğu "Özen sorumluluğu" başlığı altında düzenlenmiş; 316. maddede kiracının kiralananı, sözleşmeye uygun olarak özenle kullanmak borcu öngörülmüş; işçinin (m. 396), yüklenicinin (m. 471) ve vekilin (m. 506) işi özenle görme borcu açık şekilde "özen" kelimesiyle ifade edilmiştir.

172 **Başpınar**, s. 123.

tanımlama yapılması sonraki süreçte kanun metninde değişiklikler yapılmasını gerektirebilirdi.

Özen kavramı, borçlunun yerine getirmesi gereken edimin kendisinden beklenen ve borcun ifası için irade, azim, itina ve dikkat gibi subjektif unsurlarla birlikte, görülen iş için borçlunun şahsiyetinde bulunması zorunlu olan bedeni ve fikri niteliklerin toplamını ifade eder[173]. Özen, kavram olarak daima bir edimi (asli veya yan) veya yan yükümlülüğü, yapma davranışını şart koşar. Bir başka deyişle özen, insani bir davranışın kriteridir[174]. Çünkü özen, genellikle olumlu özellikleri bünyesinde bulunduran bir kavramdır. Bu açıdan özen, "asıl borcun (vekaletin) ifası için, zaruri dikkat, itina, fikri ve bedeni yetenek gibi, borçludan istenen özelliklerin tamamı"[175] olarak tanımlanmaktadır. Gerçekten, özen kavramının bütün anlamlarında, bir işin yapılmasında, bir kimsenin normalden, yani olağandan daha üstün bir dikkat ve çaba göstermesi yatmaktadır[176].

II. Hukuki Niteliği

Özen yükümlülüğünün hukuki niteliğinin tespitinde onun borçlar hukuku alanında hangi yükümlülükler grubuna dâhil edileceği belirleyici olacaktır. Bilindiği üzere, modern borçlar hukuku doktrininde sözleşme tarafları arasındaki borç ilişkisinden ortaya çıkabilecek yükümlülükler farklı sınıflandırmalara tabi tutulmuştur. Bu sınıflandırmalara kısaca göz atmakta fayda vardır.

A. Edim Yükümlülüğü

Edim yükümlülüğü, borç iliskisinin asıl konusunu oluşturur, borçlunun alacaklı yararına borçlandığı ve gerçekleştirmek zorunda olduğu bir davranışı ifade eder. Borçlu, sözleşmeden doğan edimi sözleşmenin amacına ve ifa kurallarına göre yerine getirmeli, böylelikle de alacaklının ifa menfaatini gerçekleştirmelidir. Nitekim

---

173 **Aral/Ayrancı**, s. 418.
174 **Gümüş, M. A.,** Türk-İsviçre Borçlar Hukukunda Vekilin Özen Borcu, Beta Basım Yayın, İstanbul, 2001, s. 47.
175 **Başpınar**, s. 124.
176 **Başpınar**, s. 124.

TBK, esas itibariyle edim ve edimin ifasını, baska bir deyişle, edim menfaatini dikkate almıştır[177].

Asli edim yükümlülüğü, borç ilişkisinin doğrudan doğruya meydana getirdiği, bu ilişkiye hukuki özelliğini veya hukuki tipini veren yükümlülüklerdir[178]. Buna mukabil, yan edim yükümlülüğü, sözleşmenin esaslı unsurunu oluşturmayan, sözleşmenin tipini etkilemeyen yükümlülükler olmakla kanundan (TBK, m. 226/f. 1, m. 317 vd.), sözleşmeden (meselâ, satıcının kombinin kurulması ve bakımını üstlenmesi hâlinde) ve dürüstlük kuralından doğmaktadır[179]. Yan edim yükümlülükleri doğrudan veya dolaylı olarak asli edim yükümlülüklerinin sözleşmenin amacına uygun, tam ve doğru bir şekilde ifasına hizmet ederler. Asli edim ve yan edim yükümlülüklerinin ortak yanı borçlunun bu yükümlülüklerini yerine getirmemesi hâlinde alacaklının ayrıca ifa davasına konu olabilmeleridir[180].

B. Yan Yükümlülükler

Borç ilişkisinden doğan yükümlülükler, sadece aslî ve yan edım yükümlülüğü ile sınırlı değildir. Şöyle ki, borç ilişkisinden edim yükümü dışında kalan yan yükümler de doğmaktadır[181]. Anılan yükümlülüklerin ana kaynağını TMK'nın 2. maddesinde düzenlenen dürüstlük kuralı oluşturur. Yan yükümlülükler, edimin ifasının yerine getirilmesinde yardımcı olan yan yükümlükler ile borç ilişkisinin taraflarının ve belirli üçüncü kişilerin edim dışındaki can ve mal varlıklarını korumaya yönelik koruma yükümlülükleri olmakla ikili bir ayrıma tabi tutulmaktadırlar[182]. Ayrımın temelinde yan yükümlülüklerin işlevi kıstası dayanmaktadır.

---

[177] **Eren**, Genel Hükümler, s. 30; **Akıncı, Ş.,** Borçlar Hukuku Bilgisi, Genel Hükümler, 10. bs., Sayram Yayınları, Konya, 2017. s. 39.

[178] **Kocayusufpaşaoğlu**, **N.,** Borçlar Hukukuna Giriş – Hukuki İşlem – Sözleşme, Filiz Kitabevi, İstanbul, 2017, s. 7; Eren, **Genel Hükümler**, s. 31; **Kılıçoğlu**, s. 40; **Akıncı**, Borçlar Hukuku, s. 40.

[179] **Kocayusufpaşaoğlu**, s. 11; **Eren**, Genel Hükümler, s. 32-37; **Kılıçoğlu**, s. 41-42.

[180] **Kocayusufpaşaoğlu**, s. 11.

[181] **Oğuzman, M.K/Barlas,N.,** Medenî Hukuk, İstanbul, Vedat Kitapçılık, 2016, s. 315; **Kocayusufpaşaoğlu,** s. 11-12; **Akıncı**, Borçlar Hukuku, s. 40.

[182] **Eren**, Genel Hükümler, s. 37; **Kılıçoğlu**, s. 43; Belirtmek gerekir ki, doktrinde koruma yükümlülüklerini yan yükümlülüklerinden ayıran görüş de savunulmaktadır. Buna göre, yan yükümlülükleri koruma yükümlülüklerinden ayırıcı ölçüt sonuncunun yöneldiği korunan menfaattir.

Edimin ifasının yerine getirilmesinde yardımcı olan yan yükümlülükler, asıl edim yükümlülüğü dışında bir anlam taşımazlar; anılan yan yükümlülüklerin görevi alacaklıyı asli edim yükümlülüğünden sözleşmenin amacına uygun tarzda yararlanabilecek duruma sokmaktır[183]. Buna mukabil, koruma yükümlülükleri, bir hukuki işleme (borç ilişkisine) yönelmiş olarak aralarında sosyal temas gerçekleşmiş olan kişilerin bundan kaynaklanan özel güven ilişkisi nedeniyle birbirlerinin şahıs ve malvarlıkları üzerinde etkili olma imkânlarının artmasına paralel olarak, diğer tarafın zarara uğramasını önleyecek şekilde davranması gerektiğini öngören yükümlülüklerdir. Görüldüğü üzere, her iki yan yükümlülük açısından ortak olan taraf aynen ifalarının talep ve dava edilemeyecek olmalarıdır. İfaya yardımcı yan yükümlülükleri ihlâl eden borçlunun tazminat borcu doğar; bazı durumlarda, sözleşmenin karşı tarafı sözleşmeyi tek taraflı irade beyanı ile ortadan kaldırabilir. Koruma yükümlülüklerine aykırılık hâlinde ise borclunun tazminat borcu söz konusu olur. Anılan yükümlülükler arasındaki en önemli fark ise, ifaya yardımcı yan yükümlülüklerin edim ve özellikle asli edim yükümlülüklerine bağımlı bir niteliğe sahip olmaları ve asli edim yükümlülüğü dışında bir anlam taşımamaları, buna karşılık koruma yükümlülüklerinin ister fonksiyonel, isterse de doğuş açısından edim yükümlülüklerinden bağımsız olmalarıdır[184].

C. Özen Yükümlülüğünün Edim ve Yan Yükümlülüklerle İlişkisi

Türk özel hukuk doktrininde vekilin özen yükümlülüğünün hukuki niteliğine ilişkin görüş birliği bulunmamaktadır[185]. Ancak vekilin özen yükümlülüğünü inceleyen yazarların[186] çoğunluğu bu yükümlülüğü bir yan yükümlülük olarak

---

Şöyle ki, yan yükümlülükler ifa menfaatinin gerçekleşmesine hizmet ederken, koruma yükümlülükleri bütünlük-koruma menfaatine yönelik ihlâlleri önlemeyi amaçlar. Bkz. **Gümüş**, Özen Borcu, s. 123 vd.

[183] **Kocayusufpaşaoğlu**, s. 12.

[184] **Serozan**, Bağımsız Borç İlişkisi, s. 119.

[185] Bu konuda çeşitli görüşler için bkz.: **Başpınar**, s. 147 vd.; **Gümüş**, Özen Borcu, s. 161 vd.

[186] **Eren, F.,** Borçlar Hukuku Özel Hükümler, 4. bs., Yetkin Basımevi, Ankara 2017, s. 731; **Akipek, Ş.,** Alt Vekalet, Yetkin Yayınları, Ankara 2003, s. 57; **İşgüzar**, s. 104.

nitelendirmektedirler. Diğer bir görüş, vekilin özen yükümlülüğünün asli edim yükümlülüğü olması yönündedir[187].

Bir görüş, vekilin özen borcunun gerçek anlamda bir edim yükümü veya yan yüküm olarak, asli ve bağımsız bir varlığa sahip olmadığı yönündedir[188]. Bu anlamda, özen yükümlülüğü vekilin diğer borçlarını belirleyici niteliğe sahiptir[189].

Diğer bir yazar, vekilin özen yükümlülüğünü edim veya yan yüküm olarak tanımlanmasını mümkün görmemektedir. Şöyle ki, özen yükümlülüğü, vekilin yapma edimi içeren edim yükümlülüklerine (veya yan yükümlülüklere) eklemlenerek onların tamamlayıcı bir parçasına çevrilir ve bu yükümlülüklerin doğru ifası için gerekli olduğu ölçüde var olur[190]. Yazara göre, özen kavramı bir yönüyle asli edim yükümlülüğünün kötü ifa edilmesi durumunda sözleşme ihlâli; diğer yönüyle de kusurlu davranışın belirlenmesinde bir kıstas olarak çift boyutlu bir kavramdır. Yazarın fikrince, asli edimin gereği gibi ifa edilmesi özen yükümü sayesinde mümkündür, dolayısıyla sözleşmeye aykırılığın söz konusu olabilmesi için aynı zamanda bir özen yükümlülüğünün ihlâlinin de varlığı gerekmektedir. Bu bakımdan, tek başına özen yükümünün ihlâli, sözleşmenin ihlâl edildiği anlamına gelmez, özen yükümünün ihlâl edilmesi durumunda, dava ve tazminat hakkından da söz edilemez[191].

Başka bir görüş, özen yükümlülüğünün güvenden doğan yan yükümlülük olduğu yönündedir[192].

Nihayet, doktrinde bankanın internet bankacılığı sözleşmesinden doğan özen yükümlülüğünün yan edim yükümlülüğü olduğu da savunulmuştur[193].

Kanaatimizce, özen yükümlülüğünün, edim yükümlülüğü olarak nitelendirmek mümkün değildir. Zira özen yükümlülüğü sözleşmeye hukuki

---

187 **Topuz**, **S.,** "Türk Hukukunda Vekalet Sözleşmesinde Vekilin Özen Borcu", Yayımlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale 2001, s. 44.
188 **Başpınar**, s. 158.
189 **Başpınar**, s. 144.
190 **Gümüş**, Özen Borcu, s. 129.
191 **Gümüş**, Özen Borcu, s. 102-103.
192 **Battal, A.,** Güven Kurumu Nitelendirilmesi Işığında Bankaların Hukukî Sorumluluğu, Banka Ve Ticaret Hukuku araştırma Enstitüsü Yayınları, Ankara 2001, s. 134.
193 **Yılmaz**, s. 146.

özelliğini veren yükümlülük değildir. Aynı zamanda, alacaklı özen yükümlülüğünün ihlâli hâlinde ayrıca ifa davası da açabilmek imkânını haiz değildir.

Diğer taraftan, özen yükümlülüğünün bir koruma yükümlülüğü olarak kabülü de isabetli olmaz. Şöyle ki, söz konusu yan yükümlülük alacaklının ifa menfaati dışında kalan menfaatlerinin korunmasına yöneliktir. Aynı zamanda, koruma yükümlülüklerinin ifasında da bankanın özenle davranması gerektiği açıktır. Mesela, banka müşterisine ait kimlik bilgilerini özenle saklamak zorundadır. Bu anlamda, kötüniyetli kişilerin bankanın bilgi sistemine sızarak müşterilere ait bilgileri çalması ve bu bilgileri kötüamaçlı (mesela, kredi almak amacıyla) kullanması durumunda, bankanın koruma yükümlülüğünün ifasında özenli olup-olmadığı sorusu gündeme gelebilmektedir.

Özen yükümlülüğünün edimin ifasının yerine getirilmesinde yardımcı olan yan yükümlülük olarak tanımlamak isabetli olmaz. Zira banka yan yükümlülüklerin ifasını da özenle yerine getirmek durumundadır. Mesela, bankanın bilgilendirme yükümlülüğü bir yan yükümlülük olarak karşımıza çıkar. Ancak banka bilgilendirmeni de özenle yapmak zorundadır.

Bu açıdan baktığımızda, özen yükümlülüğünün, diğer yapma yükümlülüklerine eklenerek onların tamamlayıcı bir parçasına çevrilmesi ve bu yükümlülüklerin doğru ifası için gerekli olduğu ölçüde var olmasına ilişkin görüş daha isabetlidir. Şöyle ki, elektronik bankacılık hizmetlerinin sağlanmasına ilişkin banka ve müşteri arasında sözleşme görüşmelerinin başlanmasından itibaren bankanın müşteri karşısında farklı nitelikte yükümlülükleri doğmaktadır. Bu yükümlülükler, edim yükümlülüğü (bankanın şube dışındaki/alternatif dağıtım kanalları aracılığıyla müşteriye elektronik bankacılık hizmetlerini sunmak). Bankanın özen yükümlülüğü, söz konusu borç ilişkisi çerçevesinde bankanın yapma edimi veya yan yükümlülük şeklinde ifa etmesi gereken tüm yükümlülüklerinin sözleşmeye uygun yerine getirilmesi için bir kriter olarak karşımıza çıkmaktadır. Başka bir ifadeyle, bankanın diğer yükümlülüklerini doğru ifa etmesi özen yükümlülüğüne riayet ederek sağlanır[194].

---

[194] **Gümüş**, Özen Borcu, s. 142.

§ 4. Bankanın Özen Yükümlülüğünün Konusu ve Ölçüsü

I. Konusu

Vekil iş görme ile hedef tutulan sonucun başarılı olması için hayat deneylerine ve işlerin normal akışına göre gerekli girişim ve davranışlarda bulunmalı, başarılı sonucu engelleyecek davranışlardan kaçınmalıdır. Vekilin bu yöndeki davranışları özen yükümlülüğünün konusunu teşkil etmektedir[195]. Yargıtay'ın uygulaması da bu yöndedir[196].

Elektronik bankacılıkta bankanın belirli bir sonucu yahut sonuca yönelik özenli faaliyette bulunmayı borçlandığı tartışmaya açıktır. Mesela, müşteri internet bankacığı üzerinden EFT yaparak borcunu ödemek isterse, ancak bankanın sistemindeki hata nedeniyle işlemi gerçekleştiremezse, bankanın sorumluluğu sözkonusu olur. Ancak bu durumda banka, özenli faaliyette bulunmadığı, yoksa müşterinin istediği sonucu gerçekleştiremediği için mi sorumludur? Bankanın borcunun sonuç borcu olduğunun kabul edilmesi durumunda, internet bankacılığı sözleşmesine eser sözleşmesine ilişkin hükümlerin uygulanması gerekir. Zira vekalet sözleşmesinden farklı olarak eser sözleşmesinde yüklenici bir eseri meydana getirmeyi borçlanmaktadır[197]. Aslında müşterinin internet bankacılığı sözleşmesini akdetmekteki amacı gerekli işlemleri uzaktan gerçekleştirme imkânı kazanmak olduğu açıktır. Bu anlamda, verdiğimiz örnekte, EFT gerçekleştirme borcunun bir sonuç borcu olduğu söylenebilir. Ancak burada bir eserin meydana getirilmesi söz konusu değildir. Şöyle ki, her ne kadar banka hesabındaki paranın müşterinin talimatı

---

[195] **Tandoğan**, **H.,** Borçlar Hukuku Özel Borç İlişkileri, C. 2, 3. bs., Banka ve Ticaret Hukuku Araştırma Enstitüsü, Ankara, 1987, s. 410; **Aral/Ayrancı**, s. 448; **Başpınar**, s. 135; **Yavuz/Acar/Özen,** s. 1159; **Zevkliler, A./Gökyayla**, **E.,** Borçlar Hukuku Özel Borç İlişkileri, 16.bs., Turhan Kitabevi, Ankara, s. 650.

[196] "... müvekkil işin görülmesi tarzı hakkında talimat vermediği vakit, vekilin nasıl hareket etmesi gerektiği onun sadakat ve özen yükümlülüklerinden çıkarılabilir. Vekil işi sadakatla, yani müvekkilinin menfaatlerini en iyi koruyacak biçimde ve özenle görmelidir. Özen, borcu ise vekilin iş görme ile hedef tutulan sonucun başarılı olması için hayat deneylerine ve işin normal akışına göre gerekli girişim ve davranışlarda bulunmasıdır. Genellikle kendisine başvurulan vekil, uzman bir kişi olup yapılması veya yapılmaması gerekenlerin ne olduğunu özen ve sadakat yükümlülükleri çerçevesinde kendisi tayin eder." **Yarg. 3. HD**, T. 9.9.1985, E. 1985/2552, K. 1985/5380; Aynı yönde: **Yarg. 13. HD**, T. 13.5.2014, E. 2013/14015, K. 2014/15333 (Legalbank).

[197] **Akıncı Ş.**, Vekalet Sözleşmesinin Sona Ermesi, Sayram Yayınevi, Konya, 2004, s. 7; **Gümüş**, Özel Hükümler, s. 9.

üzerine diğer bir kişinin hesabına aktarılması sanal alemde (yani gayri-nakit olarak) bir değişiklik yaratsa da, bu değişikliğin eser olarak nitelendirmek isabetli olmaz. Zira bankanın parayı aktarma işlemini gerçekleştirmekteki amacı yeni bir şey oluşturmak değildir. Bu anlamda, bankanın özen yükümlülüğünü gereğince yerine getirmediği için, yani vekalet sözleşmesinin hükümleri uyarınca sorumlu tutulması gerekir.

Görüldüğü gibi, bankanın özen yükümlülüğünün konusu, müşterilere alternatif dağıtım kanallarını kullanmakla banka hizmetlerine kural olarak, sanal şekilde herhangi bir zaman veya mekân kısıtlaması olmaksızın[198] erişebilme imkânı tanımak için gerekli davranışlarda bulunma ve bu hizmetlerin sağlanmasına ilişkin başarılı sonucu engelleyecek davranışlardan kaçınma olarak ifade edilebilir. Yani banka, sonucu değil, elektronik hizmetlerin eksiksiz bir biçimde ve güvenli olarak sağlanmasını borçlanmaktadır[199]. Burada bankanın belirli bir sonuca yönelmiş özenli, her aşamada müşterinin çıkarlarını ön planda tutmayı gerekli kılan ve bu amaca ulaşılmasını riske edecek her türlü davranıştan sakınılmasını gerektiren bir iş görme borcu söz konusudur. Banka, bilgi sağlanmasına ilişkin hizmetler açısından müşterilerin bilgilendirilmesini sağlamaya yönelik davranışlarda bulunurken, işlem yapılmasına yönelik hizmetler bakımından müşterinin talimatının bankaya ulaşmasına ilişkin davranışta bulunmaktadır. Mesela, internet bankacılığı çerçevesinde müşterinin bankadaki hesabından üçüncü kişinin banka hesabına para aktarılması durumunda internet, müşterinin talimatının bankaya ulaşmasında bir araç olarak kullanılmaktadır; banka, deyim yerindeyse, bu "elektronik talimatı" aldıktan sonra vekâlet verenin yetkisine, hesabın yasal durumuna ve hesaptaki paranın kullanılabilirliğine ilişkin doğrulama işlemlerini yapacak, yalnız bundan sonra müşterinin vekili olarak gereken paranın alıcının hesabına yatırılmasını

---

198 Bazı hizmetler istsinadır, örneğin, ATM'den para çekme sanal değil, gerçek, mekan açısından sınırsız değil, sınırlı bir elektronik bankacılık hizmetidir.

199 "Vekilin iş görme ile amaç tutulan sonucun başarılı olması için hayat deneylerine ve işlerin normal akışına göre gerekli girişim ve davranışlarda bulunması ve başarılı sonucu engelleyecek davranışlardan kaçınması özen borcunun kapsamını oluşturur. Vekil iş görürken amaçlanan sonucun elde edilmemesinden değil, bu sonuca kavuşmak için yaptığı çalışmaların özenle görülmemesinden sorumludur. İş sadakatla ve özenle görülmüşse yönetilen sonuca erişilmemiş olsa bile gereği gibi ifa vardır. Vekilin gerekli özeni göstermesine rağmen sonucun elde edilmemesinin rizikosu vekile yüklenemez. Bu riziko müvekkilin üzerinde kalır" **Yarg. 13. HD**, T. 5.2.1991, E. 1990/7902, K. 1991/1070; Aynı yönde: **Yarg. 13. HD**, T. 26.6.2014, E. 2013/19061, K. 2014/21353 (Legalbank).

gerçekleştirecektir. Banka işlemi gerçekleştirdiği sırada da müşterisini bilgilendirmeyi de ihmal etmemelidir. Ancak bize göre, bankanın özen yükümlülüğünün konusu yalnızca bununla da sınırlı değildir. Zira yukarıda özen yükümlülüğünün yalnızca sözleşmeden doğan edim yükümlülüğünün değil, aynı zamanda banka ile müşteri arasındaki borç ilişkisinden ileri gelen diğer yapma yükümlülüklerinin de gereği gibi ifası açısından önem arz ettiği ifade edilmişti. Bu anlamda, gerek sözleşme öncesi aydınlatma ve sır saklama yükümlülüklerinin, gerekse sözleşme sonrası sır saklama yükümlülülüğünün gereği gibi ifası için gereken davranışlarda bulunulması ve olumsuz davranışlardan kaçınılması da bankanın özen yükümlülüğü kapsamında değerlendirilebilir.

II. Ölçüsü

Eski Borçlar Kanunu'nun 321. maddesinin 2. fıkrasında vekilin özen borcunun kapsamını belirlemek bakımından biri objektif diğeri ise subjektif olmak üzere iki kriter öngörülmüştü. Ancak TBK'nın 506. maddesinin 3. fıkrası ile subjektif kıstas terk edilmiş, vekilin özen borcunun kapsamının belirlenmesinde objektif kıstasın, yani benzer alanda iş ve hizmet üstlenen basiretli bir vekilin göstermesi gereken davranışın esas alınacağı hükme bağlanmıştır. Objektif kıstasın, sözleşmeye uygun görülecek işin çeşidini, güçlüğünü ve gerektirdiği öğrenim ve mesleki bilgi derecesini göz önünde tutmayı gerektirdiği, işin, güç veya vekâlet veren için taşıdığı önemi büyük olduğu oranda, gösterilecek özenin de fazla olduğu ifade edilmektedir[200]. Elektronik bankacılıkta bankaların özen yükümlülüğünün ölçüsü değerlendirilerken basiretli tacir gibi davranması gerektiği, özel denetime tabi olması, elektronik bankacılık hizmetlerinin teknoloji açısından bünyesinde taşıdığı risklere vakıf olması ve bunlara karşı gereken önlemleri alması gibi hususlar dikkate alınmalıdır. Özellikle de, elektronik hizmetlerin güvenli bir şekilde gerçekleştirilmesine yönelik tedbirlerin alınması açısından objektif kriter önem arz etmektedir.

---

[200] **Tandoğan**, Borçlar, s. 411; **Zevkliler/Gökyayla**, s. 650-651; **Aral/Ayrancı**, s. 449; **Eren**, Özel Hükümler, s. 731; **Yavuz/Acar/Özen**, s. 1161; **Donay, S.,** "Vekilin Talimata Uyma ve Dürüstlükle Hareket Etme Borcu", BATİDER, Aralık 1970, C. 5, S. 4, s. 738; **Akipek**, Alt Vekalet, s. 56.

§ 5. Elektronik Bankacılıkta Bankaların Özen Yükümlülüğünün Ağırlaştırılması

Bankalar, sahip oldukları vasıfları ve işlevleri sebebiyle özel düzenlemeye tabi tutulması gereken kurumlardır. Bu nedenle, bankaların özen derecesi belirlenirken, bankacılık mesleğinin ve sektörün kendisine özgü nitelikleri mutlaka dikkate alınmalıdır. Bu sebeple elektronik bankacılıkta bankanın özen yükümlülüğünün derecesinin belirlenmesinde bankanın basiretli tacir gibi davranması ve bir güven kurumu olmasına ilişkin kurallar önem arz etmektedir.

I. Güven Kuruluşu Olma Nedeniyle Ağırlaştırma

A. Genel Olarak

Türk hukukunda bankalar, özel kuruluş ve faaliyet izni ile çalışmakta ve kendine has usullerle denetime tabi tutulmaktadırlar. Her şeyden önce, sıradan bir işletmenin zarara uğraması ile güven kurumu olan bankanın açısından zararın meydana gelmesi karşılaştırılamaz. Şöyle ki, olağan bir işletmenin zarara uğraması ve çökmesi hâlinde bundan etkilenenlerin sayı sınırlı iken; bir bankanın çöküşü, büyük ihtimal, tüm toplum üzerinde etkili olacaktır. Zira bankalar, riske atarak zarara uğramasına neden olduğu kaynakların neredeyse tamamını halktan toplanan mevduat teşkil eder. Bu acıdan baktığımızda, bankanın uğradığı zarardan sadece banka tüzel kişiliği ve bankanın ortakları değil; aynı zamanda çok geniş bir kitlenin de etkilenmesi doğaldır. Kanun koyucu, zarar görecek kitlenin bu denli geniş olmasını, dikkate alarak bankaların faaliyetine özgü riskleri denetleyecek ve risklerin gerçekleşmesinden sonra yayılmasını önleyecek düzenlemeler getirmiştir.

Diğer yandan, belirtmek gerekir ki, bankaların faaliyetleri kamu düzeni ile yakın bağlantılıdır. Bu yakınlık doktrinde bankacılığın adeta bir kamu faaliyeti, bankaların da yarı kamu kuruluşu olduğu fikrinin ileri sürülmesine yol açmıştır[201].

---

[201] **Stoufflet**, "Bankacılıkta Sorumluluk", Mukayeseli Banka Hukuku İhtisas Dönemi, İstanbul 3-14 Aralık 1973, C. 3, TBB Yayınları, 1974, s. 6; **Yarg. 11. HD**, 7.10.1996 tarihli ve 6371/6535 sayılı kararında (yayımlanmamıştır) "bankanın bir kamu kurumu olup kamu kurumlarının güven müesseseleri olduğunu" belirtmiştir (**Battal**, s. 46-47); Amerikan mahkemelerinin bu yöndeki kararları için bkz. **Harrel**, **C.A.,** "The Bank-Customer Relationship: Evolution of a Modern Form?",

Diğer anonim şirketlere nazaran bankaların kurulması ve faaliyete geçmesi özel izinlerin alınmasını gerektirmektedir. Aynı zamanda, banka yöneticileri açısından özel şartlar aranmakta, bankaların faaliyet alanları sınırlı tutulmaktadır[202]. Bundan baska, kanun koyucu, bankaların malî yapılarıyla ilgili özel düzenleme getirmekte ve bankalar için sermaye yeterliği, likidite yeterliliği gibi konularda çeşitli standartlar öngörmektedir[203].

Her şeyden önce, 5411 sayılı Bankacılık Kanunu'nda[204] (BanK) bankalar için getirilmiş bazı özel şartlar bulunmaktadır. Başka anonim şirketlerden farklı olarak, bankaların faaliyet konuları yalnız BanK'nun 4. maddesinde sayılan hususlarla sınırlıdır. Diğer anonim şirket kurucularından farklı olarak, BanK'nun 8. maddesi ile banka kurucuları için oldukça farklı şartlar getirilmiştir. Banka kurucularında aranan şartların incelenmesi bizi şu sonuca götürür: söz konusu şartların getirilmesindeki en temel amac yönetim gücünün kötüye kullanılmasını önlemek, bankanın daha kurulduğu aşamada aşırı riskli bir yapıya sahip olmasının önüne geçmektir[205]. BanK'nun bankalar açısından öngördüğü diğer bir farklı düzenleme bankaların yönetim yapısına ilişkindir. Meselâ, 24. maddeye göre, bankalarda denetim komitesi kurulması zorunludur; 25. madde ile, diğer anonim şirketlerde bulunmayan genel müdürlük adında bir organ öngörülmüştür. BanK'nun getirdiği daha önemli bir düzenleme, bankaların tüm faaliyetlerinin BDDK'nın yoğun gözetim ve denetimine tabi tutulmasıdır (m. 65).

Görüldüğü üzere, bankaların toplum hayatında oynadığı rol ve ülke ekonomisi açısından sahip olduğu işlevler, aynı zamanda taşıdığı riskler, söz konusu risklerin gerçekleşmesi hâlinde meydana gelecek zararın ve bundan etkilenecek kitlenin büyüklüğü bankaların özel düzenlemelere tabi tutulması zaruretini doğurmuştur. Bu durum, müşterilerde bankaya karşı özel güven duygusu uyandırmaktadır. Bankanın özen yükümlülüğünün, güven kurumu olması nedeniyle

---

Okla. City U. L. Rev., 1986, Vol. XI, p. 643; **Plato-Shinar, R.,** "The Banking Contract As a Special Contract: The Israeli Approach", **Touro Law Review**, 2013, Vol. 29, p. 730.

[202] **Battal**, s. 45.

[203] **Battal**, s. 58 vd.

[204] 01.11.2005 tarihli 25983 sayılı R.G.'de yayımlanmıştır.

[205] **Gülerci**, **A.F.,** Sorumluluk Hukuku Bakımından Bankacılıkta Risk Kavramı, TBB Yayınları, İstanbul, 2015, s. 28.

ağırlaşmasının temelinde ise, müşteri ile arasındaki borç ilişkisinin niteliğinden ziyade, bu ilişkinin bir tarafında yukarıda belirtilen sebeplerden dolayı karşı tarafta (müşteride) özel güven uyandıran bankanın mevcut olması dayanmaktadır[206]. Diğer bir ifadeyle, banka ve müşteri ilişkileri, güven duygusunun kaynağını oluşturan manevî, ahlakî ve psikolojik faktörlerden etkilenmektedir. Sonuç itibariyle, güven kurumu olmak, bankanın borçlarında ve özellikle de özen yükümlülüğünün ölçüsünde bazı değişikliklere sebebiyet vermektedir[207].

B. Elektronik Bankacılık Açısından

Geleneksel banka-müşteri ilişkisi açısından yukarıda zikredilen hususlar elbette ki, elektronik bankacılık bakımından da geçerlidir. Fakat elektronik bankacılık açısından önemli olan husus, banka ile müşteri arasındaki güven ilişkisinin fiziki (maddi) ortamdan sanal ortama taşınmış olmasıdır. Bu açıdan bakıldığında, bankanın elektronik bankacılık hizmetlerinden yararlanan müşteriler karşısında ifade ettiği güvenilirlik oranı çok daha fazladır. Zira elektronik bankacılıkta müşteri, yaptığı işlemin bankanın kurduğu sistem tarafından yerine getirilip getirilmediğini denetlemek imkânına sahip değildir[208]. Ayrıca, kural olarak müşteri, yaptığı işlemle ilgili bilgiyi yalnız işlem gerçekleştikten sonra alabilmektedir[209]. Diğer yandan, banka ile müşteri arasında hizmetlerin sağlanması sürecine diğer aktörler (internet servis sağlayıcıları vb.) de katılmaktadır. Müşteri, bilinçli veya bilinçsiz olarak, bu aktörlere olan güvenini de bankaya olan güveni çerçevesinde değerlendirmektedir.

Bundan başka, müşteriler, her ne kadar uzaktan dağıtım kanalları aracılığıyla bankacılık hizmetlerinden yararlanılmasının güvenilirliğine ilişkin tereddütler yaşamış olsalar dahi, teknolojik ilerlemenin ve finansal hizmetler pazarının bu kadar iç içe geçtiği şartlarda söz konusu hizmetlerden faydalanma ihtiyacları ve eğilimleri artmaktadır. Elektronik bankacılık hizmetlerini sunan bankaların bu konuda uzman oldukları, gerekli altyapıyı oluşturdukları ve her alanda olduğu gibi bankaların bu

---

206 **Harrel**, s. 669, 680-681.
207 **Battal**, s. 106.
208 **Plato-Shinar**, Contract**,** s. 733.
209 **Plato-Shinar**, Contract**,** s. 733.

alandaki faaliyeti üzerinde de özel denetim ve kontrolün mevcudiyeti elektronik hizmetler alanında bankaların güvenilir kuruluş olmalarının bir görünümü olarak değerlendirilebilir.

Sonuç olarak, bankaların özel güven kurululuşu olarak nitelendirilmesinin elektronik bankacılık hizmetleri alanında da devam etdiğini söyleyebiliriz. Nitekim gerek elektronik bankacılık hizmetlerinin sağlanması için gerekli altyapının oluşturulması, gerekse bu hizmetlerin sağlanması ile ilgili sözleşme ilişkilerinin sona ermesinden sonra dahi bankalar için özel düzenlemeler[210] getirilmiştir.

II. Elektronik Bankacılıkta Bankaların Özen Yükümlülüğünün Basiretli Tacir Olmaları Nedeniyle Ağırlaştırılması

A. Genel Olarak

Türk Ticaret Kanunu uyarınca, tacir, bütün ticarî faaliyetlerinde basiretli bir iş adamı gibi hareket etmekle yükümlüdür (m. 18/f. 2)[211]. Basiret, sağduyu, ilim, tecrübe ve feraset ışığıyla görüp sezmeye ve bilip değerlendirmeye esas teşkil eden konuları etraflıca ve tam olarak kavrayabilmedir. Her tacir, tüm ticarî faaliyetlerinde basiretli bir iş adamı gibi hareket etmek, sağduyu sahibi olmak, ileriyi düşünmek ve işlemlerini ona göre organize etmek zorundadır. Yapacağı sözleşmelerin yerine getirilip getirilmeyeceğini hesaba katıp "basiretli bir iş adamı" gibi davranıp borcun yerine getirilmesini engelleyebilecek hareketleri önceden nazara alması gerekmektedir[212].

Doktrinde ileri sürülen bir görüşe göre, basiretli bir iş adamı gibi hareket etme yükümlülüğü, "külfet" niteliği taşıyan bir yükümdür[213]. Şöyle ki, söz konusu

---

[210] Bu konuda ayrıntılı açıklamalara aşağıda yer verilmiştir.

[211] **Gümüş**'e göre, tacirin ticari faaliyeti dışındaki faaliyet alanlarındaki sorumluluğu bakımından dahi ihmalin ölçüsünün objektifleştirilmiş olması karşısında, artık basiretli iş adamı ölçütüne gerek kalmamıştır (**Gümüş**, **M.A.,** "6102 Sayılı Türk Ticaret Kanunu (TTK) m.18/II'de Yer Alan "Basiretli İş Adamı (Tacir) Davranışı" Ölçütünün İyiniyetin (TMK m.3) Varlığının Belirlenmesindeki İşlevi", MÜHF-HAD, Özel Sayı, Prof. Dr. Cevdet Yavuz'a Armağan, Y. 2016, C. 2, S. 3, s. 1227).

[212] **Arkan**, **S.,** Ticari İşletme Hukuku, 23. bs., Banka Ve Ticaret Hukuku Araştırma Enstitüsü, Ankara, 2017, s. 147; **Poroy, R./Yasaman**, **H.,** Ticari İşletme Hukuku, 14. bs., Vedat Kitapçılık, İstanbul, 2012, s. 152-153; **Hüseyin Ülgen** v.d., Ticari İşletme Hukuku, 24. bs., On İki Levha Yayıncılık, İstanbul, 2015, s. 285-286.

[213] **Poroy/Yasaman**, s. 152; **Gümüş**, basiretli iş adamı gibi davranma yükümlülüğünün "külfet" olarak nitelendirilmesine şu gerekçe ile karşı çıkmaktadır: "... basiretli iş adamı gibi hareket etmenin bir külfet (yüklenti) olarak nitelendirildiği yerde basiretli iş adamı gibi davranma bakımından bir

yükümlülük, tacire objektif bir ölçüye kıyasla belirli durumlarda evvelden taahhüt etmemiş olduğu bazı edimler yükler veya kendisini daha geniş sorumluluk altına sokar.

Basiretli iş adamı gibi davranma yükümlülüğü, objektif bir özen ölçüsünü öngörmektedir. Bu anlamda, tacir, işletmesiyle ilgili faaliyetlerinde, kendi yetenek ve imkânlarına göre ondan beklenebilecek özeni değil, aynı ticaret dalında faaliyet gösteren tedbirli ve öngörülü bir tacirden beklenen özeni göstermek zorundadır[214].

Yargıtay'a göre, "Basiretli bir iş adamı gibi davranma yükümü aslında objektif bir özen ölçüsü getirmekte ve tacirin ticari işletmesiyle ilgili faaliyetlerinde, kendi yetenek ve imkânlarına göre ondan beklenebilecek özeni değil aynı ticaret dalında faaliyet gösteren tedbirli, öngörülü bir tacirden beklenen özeni göstermesinin gerekli olduğu kabul edilmektedir. Gerekli tedbirleri almadan sözleşme yapan ve borç altına giren tacirin alabileceği tedbirlerle önleyebileceği bir imkânsızlığa dayanması kabul edilebilecek bir durum değildir"[215].

Bankaların özen borcunun ölçüsünün belirlenmesi esnasında bankacılık mesleğinin ve sektörünün kendisine özgü niteliklerinin mutlaka dikkate alınması gerekir[216]. Bankacılık sektörünün, gerek banka yönetimi gerekse de hizmet verdiği kişiler yönünden bir bütün olarak riskli bir alan olması bankaların özen yükümlülüğünün bu riskin bir gereği olarak ağırlaştırılmasını zorunlu kılmaktadır[217].

B. Elektronik Bankacılık Hizmetleri Açısından

Teknolojik gelişmelerin bankacılık sektörünü değişime uğrattığında tereddüt etmemek gerekir. Bu gelişmeler çok sayıda yeni bankacılık hizmetlerinin sağlanması, bilgilerin toplanması, işlenmesi ve kullanılmasına ilişkin yeni yöntemlerin meydana çıkmasına imkân tanımıştır. Teknolojik gelişim bankaların hizmet sağlanmasındaki

---

yükümün veya mükellefiyetin varlığından bahsetmek pek de uygun olmasa gerekir. Bu yönüyle davranma basiretli iş adamı gibi davranma, en azından tacir için bir yüktür" (**Gümüş**, Basiretli İş Adamı, s. 1223).

[214] **Arkan**, Ticari İşletme, s. 147; **Ülgen vd.**, s. 285; **Poroy/Yasaman**, s. 152.

[215] **Yarg. HGK**, T. 07.05.2003, E. 2003/332, K. 2003/340 (Legalbank).

[216] **Tandoğan**, **H.,** "Türk Hukukunda Bankacının Hukuki Sorumluluğu", Mukayeseli Banka Hukuku İhtisas Dönemi, İstanbul 3-14 Aralık 1973, C. 3, TBB Yayınları, 1974, s. 104.

[217] **Battal**, s. 151; Bankacılık faaliyetine has riskler ayrıntılı bilgi için bkz. **Gülerci**, s. 37 vd.

maliyetlerini de köklü olarak değişime uğratmıştır. Fakat elektronik bankacılık hizmetleri beraberinde yeni nesil riskleri de getirmiştir. Basiretli tacir gibi davranmanın bankacılık hizmetlerinin sağlanmasında teknolojinin uygulanmasının getirdiği risklerin doğru yönetilmesi ile direkt bağlantısı olduğunu dikkate aldığımızda söz konusu risklere kısaca temas etmekte fayda görüyoruz. Bankacılık sektöründe ortaya çıkan bu riskler dört ana başlık altında incelenmektedir[218]: işlem riskleri, stratejik riskler, itibar riskleri ve uyum riskleri.

İşlem riskleri, bankanın hizmet sunumundaki problemlerden kaynaklanan zarar etme ihtimalini ifade etmektedir[219]. Teknolojinin söz konusu riskler üzerindeki etkisini şöyle özetleyebiliriz: uyumsuz iç ve dış sistemler hizmet sağlanmasını engellemekle banka için işlem riski oluşturabilir; iç kontrol, güvenlik tedbirleri, beklenmedik hâl planı veya denetim politikasının yetersizliği de işlem risklerine neden olabilir[220]. Bu riskler, dış kaynak kullanımı durumunda daha da artmaktadır; zira bu hâlde banka, kritik işlevleri üzerinde kontrolünü kaybetmektedir[221].

Stratejik riskler bankanın gelecek amaçlarına ilişkin etkisiz planlama veya karar alma sonucunda ortaya çıkan ve bankanın kazancına veya kapitaline yönelen riskleri içermektedir. Meselâ, banka yönetiminin yeterince bilgi ve beceri olmadan uyguladığı teknoloji müşterilerin ihtiyaçlarını karşılamayabilir veya güvenilmez olabilir[222].

İtibar riski, toplumda banka hakkında önemli ölçüde olumsuz kamuoyunun oluşması riski olarak tanımlanabilir[223]. Çeşitli faktörler bankanın itibar riski üzerinde etken olabilir. Mesela, müşteri hesapları üzerinde yetkisiz kişilerce tasarrufta bulunulması, kimlik hırsızlığı sonucunda bankaya olan güvenin sarsılması, hizmet kesintilerinin sıklığı nedeniyle güvenilir hizmetin sağlanamaması vs[224]. Teknoloji, bankanın itibar riskini farklı şekillerde olumsuz etkileyebilir. Meselâ, güvenlik

---

[218] **Douglas**, **L. J.,** "Cyberbanking: Legal and Regulatory Considerations for Banking Organizations", N.C. BANKING INST., 2000, Vol. 57, p. 64-65.
[219] **Douglas**, s. 64.
[220] **Douglas**, s. 65.
[221] **Shah/Clarke**, s. 107.
[222] **Shah/Clarke**, s. 67 vd; **Distançionnoe Bankovskoe Obslujivanie,** s. 103-104; **Douglas**, s. 65.
[223] **Kondabagil**, s. 13-14.
[224] BDDK'nın kabul ettiği "İtibar Riskinin Yönetimine İlişkin Rehber"in 3. bendi (RG., 21 mart 2016 tarihli 6827 saylı RG'de yayımlanmıştır).

ihlâlleri sonucunda müşteri sırlarının açığa çıkması, hizmet sağlanmasındaki aksaklıklar (kesintiler) veya basit tüketici korkuları banka hakkındaki olumsuz düşüncelerin meydana çıkmasına sebebiyet verebilir[225].

Nihayet, uyum riskleri banka faaliyetinin mevzuat, düzenleme ve standartlara uygun ve uyumlu olmaması sonucunda meydana çıkar[226]. Teknolojinin bankacılık hizmetlerinin sağlanmasında uygulanması uyum risklerini şöyle etkileyebilir: bankacılığa ilişkin yasal düzenlemelerin büyük çoğunluğu kağıt tabanlı işlemler göz önünde bulundurularak hazırlanmıştır; bu nedenle elektronik işlemlere başarılı bir şekilde uygulanmalarına olanak tanıyacak kadar gelişmemiş olabilirler[227].

Görüldüğü üzere, konuya bu açıdan yaklaşdığımızda, elektronik bankacılık hizmetleri sunan bankanın teknoloji bazlı riskleri, özellikle de güvenlik risklerini belirlemesinde ve yönetiminde, basiretli tacir gibi davranması gerektiği söylenebilir. Nitekim Yargıtay da, bir çok kararında, elektronik bankacılıkta gerekli güvenlik tedbirlerinin alınmasına ilişkin sorunları değerlendirirken bankanın basiretli tacir gibi davranması gerektiğinden hareket etmiştir[228].

---

225 **Douglas**, s. 65.

226 **Kondabagil**, s. 13.

227 **Distançionnoe Bankovskoe Obslujivanie, s.** 98; **Douglas**, s. 65.

228 "İnternet bankacılığındaki en önemli sorun, hiç kuşkusuz güvenlik sorunudur. ... Bu bağlamda, internet bankacılığı hizmetini müşterilerine bankalar sunduğuna göre, bu sistemin güvenliğine yönelik tüm tedbirleri almaları ve sistemi bilinen en son teknolojik gelişmeye uygun hâle getirmeleri büyük önem taşımaktadır." Yarg. HGK, T. 21.11.2011, E. 2012/11-550, K.2012/820.
"... basiretli bir tacir gibi davranma ve objektif iyiniyet kurallarına uyma yükümlülüğü bulunan davalı bankanın bu tür işlemlerin önüne geçmek için gerekli güvenlik önlemlerini alması gerekir" 11. HD, T. 20.02.2015, E. 2014/17568, K. 2015/2284.
"... davalı bankanın internet bankacılığında kendisinin ve müşterilerinin güvenliğini sağlayacak güvenlik enstrümanlarının kullanılmasını zorunlu kılmayıp, somut olayda davacının inisiyatifine bırakması zararın doğmasında başlıca etken olup, davalı bankanın zarardan sorumlu olduğu açıktır" **Yarg. 11.HD**, T. 17.01.2012, E. 2010/9949, K. 2012/268.
"... davalı bankanın basiretli bir tacir olarak internet bankacılığını müşterilerine sunarken her türlü güvenlik önlemlerini alması gerekir" **Yarg. 11. HD**, T. 19.02.2014, E. 2013/12210, K. 2014/2871.
"internet bankacılığı sistemini kullanan davalı bankanın, müşterilerinin hesaplarının korunması konusunda basiretli bir tacir ve güven kurumu olmasından kaynaklanan objektif özen borcunu yerine getirmediği, gerekli güvenlik tedbirlerini almadığı ..." **Yarg. 11 HD.**, T. 24.9.2014, E. 2014/12222, K. 2014/14425.

§ 6. Bankanın Özen Yükümlülüğünün Uygulama Hâlleri

I. Sözleşme Öncesi Aşamada Özen Yükümlülüğünün İfası

Sözleşme öncesi aşamada bankanın özen yükümlülüğünün uygulama hâlleri kural olarak, bankanın bilgilendirme ve sır saklama yükümlülüklerinin yerine getirilmesinde gerekli özenin gösterilmesi şeklinde kendini göstermektedir. Aşağıda yalnızca bilgilendirme yükümlülüğünün yerine getirilmesinde bankanın göstermesi gereken özene ilişkin açıklamalara yer verilmiştir. Ancak hemen belirtelim ki, bu açıklamalar başlıktan da anlaşıldığı üzere bilgilendirme yükümlülüğünün yalnız elektronik bankacılık hizmetlerinin sağlanmasına kadarki dönem dikkate alınarak yapılmıştır. Zira bilgilendirme yükümlülüğü sözleşmenin devamı süresinde, sır saklama yükümlülüğü ise gerek sözleşme öncesi, gerek sözleşmenin devamı, gerekse sözleşme sonrası, hatta kişinin ölümünden sonra dahi uyulması gereken yükümlülükler olarak karşımıza çıkmaktadır. Sır saklama yükümlülüğüne ilişkin açıklamaya ise, sözleşme sonrası aşamda bankanın özen yükümlülüğünün yerine getirilmesi başlığı altında yer verilmiştir.

A. Bilgilendirme Yükümlülüğünün Yerine Getirilmesinde Gösterilmesi Gereken Özen

1. Genel Olarak

Sözleşme hukuku hakkında klasik görüş için alışılmış olan sözleşme serbestisinin önemini vurgulamaktı. Zira söz konusu prensip sözleşme adaletinin vazgeçilmez garantörü olarak kabul edilmekteydi[229]. Klasik görüş, tarafların sözleşme kurup kurmamada serbest olması ve sözleşme taraflarının eşitliği karinesinden hareket etmekte ve böylelikle de, tarafların sözleşmenin içeriğinin belirlenmesinde aynı derecede etki edebileceğini kabul etmekteydi. Fakat bu görüşün gerçekliğe uymadığı çok geçmeden anlaşılmış ve bu durumun düzeltilmesi ihtiyacı ortaya çıkmıştır ki, bilgilendirme yükümlülükleri bu konuda önemli bir yere ve işleve sahiptirler. Aralarında önemli farklılıklar olmasına rağmen günümüzde hukuk

[229] **Micklitz, H-W./Stuyck, J./Terryn, E.,** Cases, Materials and Text on Consumer Law, Oxford and Portland, Oregon, Hart Publishing, 2010, s. 213.

sistemlerinin çoğunluğu sözleşme öncesi bilgilendirme yükümlülüğünü öngörmüştür[230]. Ancak, bu yükümlülük farklı hukuk sistemlerinde farklı doktrin veya ilkelerle temellendirilmektedir. Meselâ, bilgilendirme yükümlülüğü İskandinav ülkelerinde dürüstlük kuralına, Almanyada "culpa in contrahendo"ya dayandırılmaktadır. Fransa mahkemeleri Medenî Kanun'un 1134(3) maddesinde öngörülmüş "*sözleşmeler dürüstlük kuralına uygun ifa edilmelidir*" hükmünden hareketle anılan kuralın sözleşme öncesi bilgilendirme yükümlülüğüne de uygulanabileceği sonucuna varmaktadır[231].

Türk Hukuku'nda sözleşme öncesi bilgilendirme yükümlülüğünün hukuki temelini TMK'nın 2. maddesinin 1. fıkrası oluşturmaktadır. Anılan hüküm gereğince, "*Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır*". Görüldüğü gibi, bir sözleşmeye yönelik olarak görüşmelere başlayan taraflar, birbirlerine karşı dürüst davranma, sözleşmenin yapılması veya şartlarının tespiti hususundaki kararlarına etki edecek olgular hakkında birbirlerine bilgi verme ve görüşmeleri dürüst ve ciddi bir tavırla sürdürmekle mükelleftirler[232]. Bu anlamda, banka kendisinden talep edilmeksizin ve talep edilmesi gerekmeksizin, müşterinin kararı için önemli olduğu fark edilebilir olan, ancak müşteri tarafından vâkıf olunmayan hususlara ilişkin bilgileri müşteriye vermekle yükümlüdür[233]. Yargıtay'ın uygulaması da bu yöndedir[234]. Aynı zamanda, konuya ilişkin özellikle tüketici haklarının korunmasına ilişkin özel düzenlemeler getirilmiştir (TKHK, m. 4/f. 1; m. 23; m. 31/f. 4; m. 49/f. 2 vd).

---

230 **Micklitz/Stuyck/Terryn**, s. 217.

231 **Micklitz/Stuyck/Terryn, s.** 219.

232 **Oğuzman/Barlas**, s. 308-309; **Gürpınar**, **D.,** Sözleşme Dışı Yalnış Tavsiyede Bulunma, Öğüt Veya Bilgi Vermeden Doğan Hukuki Sorumluluk, Güncel Hukuk Yayınları, İzmir, 2006, s. 47; **Erbek, Ö.,** Tüketici Satımlarında Satıcının Sözleşme Öncesi Aydınlatma Yükümlülüğü ve İhlalinin Hukuki Sonuçları, Yayımlanmamış Doktora Tezi, DEÜ SBE, 2010, s. 96.

233 **Erbek**, s. 67.

234 " ... sözleşme bir süreçtir. Bir anda kurulup meydana gelen hukuki bir işlem değildir. Sözleşme kurulmadan önce taraflar sözleşmenin muhtevası, şartları, içerdiği hak ve yükümlülükler üzerinde görüşmeler yaparlar; bu görüşmeler kısa veya uzun sürebilir. Görüşmelerin başlamasıyla görüşmeciler arasında hukuki bir ilişki kurulur. Bu ilişki sözleşme benzeri bir güven ilişkisidir. Güven ilişkisi MK. m.2/1'de düzenlenmiş bulunan dürüstlük kuralına dayanır. Buna göre, görüşmeler esnasında görüşmecilerin sözleşmenin muhtevası ve şartları hakkında birbirlerini aydınlatması, dürüstlük kuralına uygun davranması, birbirlerinin kişilik ve mal varlığı değerlerine zarar vermemek için gerekli özeni göstermesi, koruma yükümlülüklerine uyması gerekir" **Yarg. HGK**, T. 13.2.2013, E. 2012/12-1220, K. 2013/239; Aynı yönde: **Yarg. HGK**, T. 1.12.2010, E. 2010/13-593, K. 2010/623; **Yarg. 11. HD**, T. 11.6.2015, E. 2015/10155, K. 2015/19267; **Yarg. 13. HD**, T. 13.11.1995, E. 1995/9375, K. 1995/9860 (Legalbank).

2. Elektronik Bankacılık Hizmetleri Açısından

Konuyu elektronik bankacılık hizmetleri açısından değerlendirmeden önce bir hususu vurgulamakta fayda vardır. Şöyle ki, yukarıda elektronik bankacılık hizmetleri sözleşmesine ilişkin yaptığımız açıklamada bu sözleşmeden doğan yükümlülüklerin banka-müşteri arasındaki diğer yükümlülüklerle yan yana mevcut olduğunu ifade ettik. Bu anlamda, elektronik bankacılıkta bankanın sözleşme öncesi aydınlatma yükümlülüğü bankacılık hizmetlerinin alternatif dağıtım kanalları aracılığıyla mesafeli olarak sunulmasına ilişkin hususları kapsamaktadır. Mesela, taraflar yatırım hizmetlerini elektronik bankacılık çerçevesinde sağlanması konusunda anlaşmış olabilirler. Bu durumda bankanın sözleşme öncesi bilgilendirme yükümlülüğü sağlayacağı hizmetin bir değil, iki hizmetten ibaret olması nedeniyle bilgilendirme iki farklı konuya ilişkin olacaktır: birincisi, yatırım hizmetine ilişkin bilgilendirme; ikincisi, yatırım hizmetinin elektronik bankacılık yoluyla sağlanması sebebiyle elektronik bankacılığa ilişkin bilgilendirme. Çalışmamız açısından ikinci konuda bilgilendirme yükümlülüğünün özenle yerine getirilmesi önem arz etmektedir.

Doktrinde savunulan bir görüşe[235] göre, bankanın bilgilendirme yükümlülüğünün biri dar diğeri geniş olmakla iki anlamda kullanılması mümkündür. Dar anlamda bilgilendirme yükümlülüğü, bankanın kurulmasına ilişkin görüşmelere başlanıldığı sözleşmeyle ilgili gerekli bilgileri müşteriye iletmesini kapsamaktadır. Geniş anlamda bilgilendirme yükümlülüğü, sözleşmeye ilişkin bilgilerle birlikte sözleşmenin esasına ve hukuki etkilerine ilişkin bilgilerin verilmesini ve bankanın, müşterinin sunulan bilgileri anlamasından emin olunması yükümlülüğünü de içermektedir[236]. Bu açıdan bakıldığında, banka elektronik bankacılık hizmetleri sözleşmesi dışındaki bilgilerle birlikte sözleşmenin çeşitli şartlarına ait bilgileri de müşteriye iletmelidir. Diğer yandan, sunulan bilgiler yalnızca olgularla sınırlandırılmamalı, gerekli durumlarda hukuki bilgileri de kapsamalıdır. Nitekim BBSEBHY'in 37. maddesinin 1. fıkrası uyarınca, banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin

---

[235] **Plato-Shinar**, **R.,** "The Bank's Duty of Disclosure – Towards a New Model", Banking & Finance Law Review, Vol. 27, Y. March 2012, s. 428.

[236] Shinar, **Duty of Disclosure**, s. 438.

şartlar, riskler ve istisnai durumlarda ilgili olarak açık bir şekilde bilgilendirme yükümlülüğü öngörülmüştür (m. 30/f. 5). Bundan başka, bilgilerin sunulması için müşterinin herhangi talepte bulunması gerekmemektedir. Zira banka dürüstlük kuralı gereğince gerekli bilgileri müşteriye sunmak zorundadır.

BBSEBHY'in 37. maddesinin 2. fıkrasında konuya ilişkin düzenlemelere yer verilmiştir. Bundan başka, yukarıda da belirtildiği üzere TKHK da tüketici olan müşterilerin bilgilendirilmesine ilişkin hükümleri öngörmüştür. Söz konusu hükümler müşterilerin sözleşme öncesi bilgilendirilmesi açısından üç konuya açıklık getirmektedir: (1) Müşteri ne zaman bilgilendirilmelidir?; (2) Müşteri nasıl bilgilendirilmelidir?; (3) Müşteri hangi konu(lar)da bilgilendirilmelidir?

B. Bilgilendirmenin İfası Zamanı, Yöntemi ve İçeriği

1. Sözleşme Öncesi Bilgilendirmenin Zamanı

Sözleşme öncesi bilgilendirmenin banka ile müşteri arasında sözleşme kurulmadan önce yerine getirilmesi gereken bir yükümlülük olduğunda tereddüt etmemek gerekir. Bu kuralın koyulmasındaki amaç, müşteriye akdedeceği sözleşmeye ilişkin bilinçli karar verme imkânını sağlamaktır. Sözleşme öncesi bilgilendirmenin önemli özelliklerinden biri, bilgilerin sağlayıcı için bağlayıcı nitelikte olmasıdır. Ancak sözleşme öncesi aşamada dahi, ilk önce bankanın bilgilendirme yükümlülüğünün, müşterinin ise bilgilendirilmek hakkından yararlanma anının belirlenmesi gerekir. Anılan hükümlerde genel bir bilgilendirme değil, sözleşme görüşmeleri (bazı durumlarda ise sözleşme kurulduktan sonra) sürecinde bankanın bilgilendirme yükümlülüğünün düzenlendiği aşikardır. Bu anlamda, banka bakımından bilgilendirme yükümlülüğü, müşteri açısından ise bilgilendirme hakkının doğumu için, öncelikle, tarflar arasında herhangi bir şekilde bağlantı kurulmuş olmalıdır. Bu sebeple taraflar arasında görüşmelerin başlamasına yol açan bir ilişki kurulduğunda, müşteri, mevzuatın öngördüğü bilgileri edinme hakkını haiz olacaktır. Diğer yandan, banka ile müşteri arasında daha önceden kurulmuş olan akdi ilişki çerçevesinde müşterinin elektronik bankacılık hizmetlerinden yararlanmak istemesi hâli de bu açıdan özellik arz etmeyecektir. Zira

bu durumda, geleneksel bankacılıktan elektronik bankacılığa dönüşüm söz konusu olmaktadır[237]. Bunun için taraflar arasındaki bankacılık sözleşmesinde değişiklik yapmak gerekecektir ki, bu değişiklik çerçevesinde banka müşteriye elektronik bankacılığa ilişkin gereken bilgileri verecektir. Bunlardan başka, üçüncü bir ihtimali de düşünebiliriz. Şöyle ki, taraflar arasında elektronik bankacılık hizmetlerine ilişkin hükümleri içeren bir sözleşme kurulmasına rağmen sözleşmenin kurulması sırasında müşteri, meselâ, internet bankacılık hizmetlerinden yararlanmak istemediğini bankaya bildirmiştir. Bu durumda banka BBSEBHY'nin 37. maddesinin 5. fıkrası gereği, internet bankacılığı hizmetini ilgili müşteri için kullanıma açamaz. Müşteri daha sonra internet bankacılığı hizmeti talebinde bulunursa, banka gerekli bilgilendirmeyi müşteri ile sözleşme kurulurken yaptığını ve sözleşmenin bir örneğinin de müşteride bulunduğunu gerekce göstererek müşteriyi bilgilendirmek zorunda olmadığını ifade edebilir mi? Bizce, bankanın böyle bir itirazda bulunması haklı sayılamaz. Zira, "BBSEBHY'in 37. maddesinin 1. fıkrası, banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnai durumlarda ilgili olarak açık bir şekilde bilgilendirilir" hükmünü içermektedir. Bize göre, anılan hüküm elektronik bankacılık hizmetlerinden yararlanmak isteyen müşterilerin bu taleplerini gerek banka ile sözleşme kurulduğu, gerekse de sözleşme kurulduktan sonraki bir aşamada ifade ettikleri hâlleri kapsamaktadır. Zira hükümde yer alan "elektronik bankacılık hizmetlerinden yararlanacak müşterilerin" ibaresini geniş yorumlamakla bu sonuca ulaşmamız mümkündür.

Bankanın sözleşme öncesi bilgilendirmenin sözleşmenin akdedilmesinden ne kadar süre önce yapılması gerektiğine ilişkin herhangi bir kural mevzuatta öngörülmemiştir. Ancak sözleşme öncesi bilgilendirmenin, adından görüldüğü üzere ve işlevi gereği, müşterinin sözleşmenin kurulmasına ilişkin iradesini açıklamasından önce yapılması gerektiği açıktır. Mevzuatta somut bir sürenin öngörülmemesinin sebebi, sözleşmenin kurulma anı ile aydınlatıcı bilgilerin verilmesi anları arasında bulunması gerekli zaman aralığının ne olacağı konusunda önceden belirli bir mutlak yasal ölçünün konulmasının çok güç olmasıdır. Bu anlamda, müşterinin

---

237 **Wiegand**, s. 177.

bilgilendirilmesi yükümlülüğünün yerine getirildiğini söyleyebilmek için her somut olayın özelliklerinin göz önünde bulundurulması ve ona göre sonuca varılması uygun görünmektedir. Eğer müşteriye serbest şekilde, bilinçli olarak sözleşmenin kurulması hakkında karar vermek için gereken bütün bilgiler yeterli bir zaman dilimi içerisinde verilmişse, bankanın kurala uyduğu söylenebilir. Bankanın sözleşmenin kurulmasından kısa süre önce bilgi vermesine rağmen tüketicinin uygun karar verme sürecine zaman tanımaması bankanın yükümlülüğünü gereğince yerine getirdiği sonucuna varmak için yeterli değildir. Bankanın, kasten önerinin geçerli olacağı süreyi azaltmak suretiyle tüketiciyi alelacele sözleşme kurmağa zorlaması (müşteri, özellikle de tüketici üzerinde baskı oluşturması) hâlinde de bilgilendirme yükümlülüğünün ihlâli söz konusudur. Diğer yandan, bankanın müşterinin özellik arz eden durumlarını (meselâ, engelli olması) de dikkate alması gerekir. Zira BHEY'ın 4. maddesinin 4. fıkrası gereğince, "*Banka, sunduğu bankacılık hizmetlerine yönelik erişim, kullanım ve güvenlik ile ilgili hususlarda engelli müşterilerini bilgilendirir. Yapılan bilgilendirmede müşterinin engel durumu dikkate alınır*". Belirtmek gerekir ki, BHEY uyarınca, 70 ve üzeri yaştaki fiil ehliyetine sahip kişiler de, müşterisi olduğu bankaya herhangi bir bildirimde bulunmaksızın BHEY kapsamında engellilere tanınan haklardan faydalanabilir. Başka bir deyişle, banka, 70 ve üzeri yaştaki fiil ehliyetine sahip kişilerin gerekli bildirimde bulunmadıklarını ileri sürerek onların BHEY kapsamı dışında oldukları itirazında bulunamaz.

2. Sözleşme Öncesi Bilgilendirmenin Yöntemi

Eski Tebliğ'de müşterilerin bilgilendirilmesi yöntemine ilişkin herhangi bir açık hükme yer verilmemişti. Buna mukabil, BBSEBHY bu konuda özel bir düzenleme getirmiştir. Şöyle ki, BBSEBHY'nin "Müşterilerin bilgilendirilmesi" başlıklı 37. maddesi gereğince, banka müşterilerin bilgilendirilmesine yönelik her türlü bilgi ve açıklamanın, bankanın gerek kendi sitesinde gerek internet bankacılığı hizmetini verdiği internet sitesinde, müşteri erişimine daima açık tutmakla mükelleftir. Uygulamada bankalar müşterilere sözleşme öncesi ön bilgilendirme

formları[238] imzalatmaktadırlar. Bu formlarda diğer bankacılık hizmetleriyle birlikte elektronik bankacılık hizmetlerine ilişkin bilgiler de yer almaktadır. Müşterinin banka şubesine geldiği durumlarda bankaların bilgilendirmeyi yazılı şekilde yapmaları kolaylaşmaktadır. Ancak yazılı bilgilendirme yeterli değildir. Başka bir deyişle, bilgilendirme formunda yazılanların sözlü olarak da müşteriye iletilmesi zaruridir.

Bundan başka, bilgilendirme formunda gösterilen bilgileri okuyan müşterinin, özellikle de tüketicilerin söz konusu bilgileri tümüyle anladığını ileri sürmek bazı hâllerde pek mümkün görünmemektedir. Bu durumda, yani müşterinin yapılan bilgilendirme sonucunda önemli hususlara ilişkin yeterli bilgi sahibi olmadığının ortaya çıktığı durumlarda banka elemanı, müşteriye açık ve anlaşılır bir şekilde ek açıklama yapmalı, müşterinin sunulan bilgileri anladığından emin olmalıdır[239]. Zira banka ve müşteri arasındaki güç farkı, elektronik bankacılık hizmetleri sözleşmesinin karmaşıklığı, bankanın müşteri üzerindeki bilgi üstünlüğü ve özellikle de, müşterilerin bankaya duydukları güven bankaların üzerine söz konusu açıklamada bulunmak yükümlülüğünü yüklemektedir[240].

Bilgilerin açık ve anlaşılır bir şekilde müşterilere sunulması gerekmektedir. Bunun için kesin (kuşkusuz), basit kelimelerin kullanılması, mümkün olduğunca hukuki ve teknik ticari terminolojiden kaçınılması zaruridir. Diğer yandan, bilgilerin sunuluş formatı da önem arz etmektedir. Meselâ, müşterinin ilgisini çekmek için bilgilendirmedeki konu başlıklarının duru bir dil ile ifade edilmesi gerekir; bilgilendirmenin punto büyüklüğüne dikkat edilmelidir. TKHK, bu konuda özel bir hüküm içermektedir. Şöyle ki, TKHK'nın 4. maddesinin 1. fıkrasında, "TKHK'da yazılı olarak düzenlenmesi öngörülen sözleşmeler ile bilgilendirmeler en az on iki

---

238 Vakıf Bank, Iş Bankası, HSBC gibi bankaların veb sitelerin bu tür bilgilendirme formlarına rastlanmaktadır. https://www.vakifbank.com.tr/2386.aspx/Controls/NewsModule/2/Controls/NewsModule/interaktif_faaliyet_raporu/2017/tr/interaktif_faaliyet_raporu/2016/tr/sozlesmeler-ve-bilgi-formlari.aspx?pageID=869; https://www.isbank.com.tr/sozlesme-ve-formlar; https://www.hsbc.com.tr/hsbc/bilgi-formlari-ve-sozlesmeler

239 İsviçre Federal Mahkemesi, bir kararında, hizmet sağlayıcısının, sunulan bilgilerin tüketici tarafından gerçekten anlaşıldığını kontrol etmesi gerektiğini ifade etmiştir (BGE 115 II 62, **Wiegand**, s. 175).

240 **Plato-Shinar**, Duty of Disclosure, s. 437.

punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir bir şekilde düzenlenir ...” denmektedir.

BBSEBHY’nin 37. Maddesinin 1'nci fıkrasının hükümleri gereğince, “*bilgi ve açıklamaların açık ve anlaşılır olması sağlanır, verildiği internet sitesinde dikkat çekici bir yere yerleşdirilir ve ilgili elektronik bankacılık hizmetinden yararlanmaya başlamadan once müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemsel kısıtlamalar uygulanır.”*

Bundan başka, bankalar engelli kişilerin özel durumlarını dikkate almak zorundadırlar. Zira BHEY, bu konuda açık bir hüküm içermektedir: “*Bankacılık hizmetlerine ilişkin sözleşmeler, hesap özeti, PIN, parola gibi müşteriye iletilen bilgi ve dokümanlar, talep hâlinde, gerekli güvenlik sağlanarak engelli müşterilere Braille alfabesi, sesli bilgilendirme, işaret dili çevirisi yapılmış video gibi farklı biçimlerde sunulur*” (m. 4/ f. 7).

3. Bilgilendirmenin İçeriği

BBSEBHY’nin 37. maddesinin 1. fıkrası elektronik bankacılık hizmetinin sağlanmasında müşterinin bilgilendirilmesine ilişkin ayrıntılı düzenlemeleri ıöermektedır. Anılan maddelerden hareketle sözleşme öncesi bankanın müşteriye sunması gereken bilgileri şu şekilde sınıflandırabiliriz:

Birinci grup bilgiler, banka hakkındaki bilgileri içermektedir. Bunlara, bankanın kimliği ve kanuni statüsü ile ilgili bilgiler dâhildir. Bu kapsamda asgari olarak bankanın ticari unvanı, genel müdürlük adresi, bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgileri müşterilere sunulmalıdır (BBSEBHY m. 37/f. 2).

İkinci grup bilgiler, elektronik bankacılık hizmetlerine ilişkin şartlar, riskler ve istisnaî durumlarla ilgilidir. Meselâ: elektronik bankacılık hizmetlerinin kullanımının taşıdığı riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler, verilen hizmetlerle ilgili olarak müşterilerin herhangi bir sorunla ya da dolandırıcılık vakasıyla karşılaşması durumunda neler yapması gerektiğine ilişkin yönlendirici bilgiler vs.

Görüldüğü üzere, bu grup bilgiler elektronik bankacılık hizmetlerinin taşıdığı riskler ve bankanın bu hususta izlediği politikaya ilişkin bilgileri kapsamaktadır. BBSEBHY 'de elektronik bankacılıkta karşılaşılacak risklere ilişkin müşterinin bilgilendirilmesine özel önem verilmiştir ki, bu da anlaşılabilir. Zira elektronik bankacılıkta en önemli husus güvenliğin sağlanması olarak karşımıza çıkmaktadır. Yargıtay'ın[241] uygulamasına baktığımızda uyuşmazlıkların büyük çoğunluğunun güvenlik sorunu ile ilgili olarak meydana çıktığını görüyoruz. Yargıtay bazı kararlarında[242] "internet bankacılığı hizmeti sunan bankaların aslî borcu, elektronik bankacılık işlemlerinin güvenle yapılabilmesini sağlamaktır. Bu yükümlülüğünü yerine getirmeyen bankaların asli kusurlu sayılması gerektiği açıktır" demekle bu hususun önemini vurgulamıştır.

Diğer taraftan, BBSEBHY, müşterilerin riskler konusunda bilgilendirilmesini yeterli görmemiş, ek olarak, söz konusu risklerin etkisini azaltmaya yönelik benimsenen güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler konusunda da müşterilere bilgi verilmesi yükümlülüğünü öngörmüştür. Belirtmek gerekir ki, BBSEBHY, internet bankacılık hizmetleri açısından güvenliğin tam şekilde sağlanabilme ihtimalinin mümkün olmadığı gerçeğinden hareket etmektedir. BBSEBHY'nin 37. Maddesinin 6. fıkrası bu sonuca ulaşmak için yeterli açıklıktadır. Şöyle ki, BBSEBHY'nin 37. Maddesinin 6. fıkrası gereğince, "Banka, yapacağı pazarlama faaliyetleri, reklâmlar veya yayınlarda, müşterilerine sunmakta olduğu herhangi bir elektronik bankacılık hizmetinin mutlak manada güvenli olduğu veya bu hizmetlerde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadeler kullanmaktan kaçınır". Bununla da müşteriler elektornik bankacılık risklerine ve tehditlerine karşı uyarılır ve bu hususlarda müşteri farkındalığı oluşturulması için azami özen gösterilir".

Elektronik bankacılık hizmetlerine ilişkin ikinci alt grup, müşterilerin elektronik bankacılık hizmetlerini kullanmalarına ilişkin bilgileri içermektedir. Bu grup bilgiler, birinci alt grupta yer alan bilgiler konusunda aydınlatılmış ve

---

[241] ***Yarg. 11. HD**, T. 22.01.2007, E. 2005/13857, K. 2007/638; **Yarg. 11. HD**, T. 26.02.2009, E. 2007/7474, K. 2009/2177; **Yarg. 11. HD**, T. 09.04.2009, E. 2007/9336 K. 2009/4347; **Yarg. 11. HD**, T. 07.04.2009, E. 2008/233, K. 2009/4242.*

[242] ***Yarg. 11. HD**, T. 09.03.2009, E. 2007/13816, K. 2009/2645; **Yarg. 11. HD**, T. 06.10.2008, E. 2007/8049, K. 2008/10661; **Yarg. 11. HD**, T. 18.03.2009, E. 2007/13990 K. 2009/3077.*

elektronik bankacılık hizmetlerini kullanmak kararına gelmiş müşterinin, bu hizmetlerden yararlanmak için ihtiyacı olan bilgileri kapsamaktadır. Meselâ, internet bankacılığı hizmetlerinin nasıl kullanılacağı; şifre veya değişken şifre seçiminde nelerin göz önünde bulundurulması gerektiği gibi. Bu bilgiler, bir yandan, müşterinin elektronik bankacılık hizmetinden yararlanmasına imkân tanımakta, diğer yandan müşteriden kaynaklanabilecek güvenlik risklerini asgari düzeye indirmekle hizmet sağlanmasında ortaya çıkabilecek uyuşmazlıkların önüne geçilmesine hizmet etmektedir.

Görüldüğü gibi, elektronik bankacılık hizmetleri, nitelikleri gereği, bazı riskleri bünyelerinde taşımaktadırlar. Diğer yandan, elektronik bankacılık hizmetlerinden faydalanmak isteyen müşterilerin bazı teknik bilgilere sahip olması gerekmektedir. Bu anlamda, banka, sağladığı hizmetlerin taşıdığı riskleri ve asgari teknik bilgilerin yokluğunun ne tür zararlara sebep olabileceğini tüm ayrıntılarıyla müşteriye bildirmek zorundadır. Nitekim banka kurum olarak yeni teknolojinin kullanılmasında sahip olduğu özel bilgi ve tecrübeyi müşterisine aktarmak zorundadır. Banka, yeni teknolojileri kullanma ve özellikle riskleri konusunda müşterilerini yeterli bir şekilde aydınlatmadığı durumlarda, bilgilendirme yükümlülüğünü özenle yerine getirmediği sonucuna varmak mümkündür. Gerkeçten de, bankanın kendi teknolojisi sebebiyle müşteriye göre bir bilgi üstünlüğü vardır. Böylelikle, tarafların sözleşme kurup kurmama konusundaki kararı üzerinde etkili olabilecek tüm hususların açıklanması oldukça önemlidir. Meselâ, ATM kartı verilmesiyle ilgili sözleşme müzakerelerinde de söz konusu olan bu açıklama yükümü, elektronik sistemleri kuran ve bu konuda müşterisine oranla daha fazla teknik bilgiye sahip olan banka tarafından yerine getirilir. Bankanın bu yükümü tam ve açık şekilde yerine getirmesinin büyük önemi vardır; zira çoğu kez gerçek kişi/tüketici olan müşteri, ATM kartları dolayısıyla kendisi bakımından söz konusu olabilecek özel rizikolar hakkında ayrıntılı bilgi sahibi değildir. Uygulamada bankalar, bu açıklama yapma yükümlerini, ilgili genel işlem şartlarının bir nüshasını müşteriye vermek suretiyle yerine getirmektedirler[243]. Aslında sözleşmenin

[243] Bu uygulama yeterli görmemekte, müşterinin ayrıca özellikle kartın çalınması, kaydedilmesi hâlinde söz konusu olabilecek rizikolar konusunda sözlü olarak uyarılması gereğine işaret etmektedir. Bkz. BIEBER, K.D., Rechtsprobleme des ec-Geldautomatensystems, Wertpapier

yapılması sırasında müşteriye açıklanması gerekli olan hususlar şöyle özetlenebilir: ATM aracılığıyla yapılabilecek işlemlerin neler olduğu; bu sistemler aracılığıyla yapılacak işlemlerde bir miktar sınırlamasının söz konusu olup olmadığı; yapılacak işlemler dolayısıyla müşterinin hesabına hangi tarihte alacak ya da zimmet kaydının geçirileceği; müşteriden talep edilecek masraf ve komisyon tutarı; kartın ve şifrenin özenle saklanması zorunluluğu ve bunların yetkisiz bir kişinin eline geçip kullanılması hâlinde müşterinin nasıl sorumlu olacağı; kartın çalınması, kaybolması hâlinde derhal bankaya haber verilmesi gereği, bu hâllerin bankaya iletilebilmesi için gerekli telefon numaraları, yetkili personelin adı ve adresi; sistemdeki teknik arıza nedeniyle işlemin zamanında ve gereği şekilde yapılamaması dolayısıyla bankanın nasıl sorumlu tutulacağı[244].

II. Sözleşme Süresinde Özen Yükümlülüğünün İfası

A. Bilgilendirme/Uyarma

Bankanın bilgilendirme yükümlülüğü, elektronik bankacılık hizmetleri sözleşmesinin kurulmasından sonra da devam etmektedir. Bankanın bilgilendirme yükümlülüğünün sürekli olmasının sebebi gerçekleştirdiği faaliyetten kaynaklanmaktadır. Her geçen gün internetin getirmiş olduğu yeni tehlikeler ortaya çıkmaktadır. Söz konusu tehlikeler hakkında müşteri, internet üzerinden yapacağı her bankacılık işleminden önce uyarılmalı ve bilgilendirilmelidir. Hatta müşterinin işleme başlamadan önce, bahsedilen uyarıları okumadan işlem yapması engellenmelidir[245]. Müşterinin sadece bir kere uyarılması, bankanın aydınlatma

---

Mitteilungen, Sonderbeilage Nr. 6/87 zu Nr. 41 vom 10.10.1987, s. 11, Arkan**, Elektronik Bankacılık**, 15'den naklen.

244 **Arkan,** Elektronik Bankacılık, s. 15.

245 **Yılmaz S.**, s. 146; İnternet bankacılığı giriş ekranında, müşterilere şifre ve PC güvenliği konusunda bilginin verilmesi, örneğin şifrenin kimseye söylenmemesi, hiçbir yere yazılmaması, isim gibi kolay tahmin edilebilecek şifreler kullanılmaması, virüslere karşı dikkatli olunması gibi uyarıların bankalar tarafından yerleştirilmesi lazımdır. Bkz. **Özdilek, A. O.,** Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, Vedat Kitapçılık, İstanbul, 2006, s. 82; Güvenlik açısından alınması gereken önlemlerin başında müşteri numarası ve şifrenin gizliliğini sağlamak ve üçüncü şahıslarla bu bilgileri paylaşmamaktır. Ayrıca uzun süre aynı şifreyi kullanmamak, alınacak güvenlik önlemlerinden biridir. E-mail aracılığıyla kesinlikle şifre/parola veya kişisel bilgiler gönderilmemelidir. Şifreler bir yere yazılmamalı, bilgisayara ya da tarayıcıya kaydedilmemelidir. Programlar bilinen kaynaklardan indirilmelidir. Bir uygulamayı çalıştırmak için, e-postaya eklenmiş bir dosya çalıştırılmamalıdır. Bkz. **Ceylan, E. E.,** "İnternet Bankacılığı ve Bankaların

yükümlülüğünü özenle ifa etdiği sonucuna varmak için yeterli değildir[246]. Banka sürekli olarak yeni tehlikelere ve virüslere karşı müşterileri uyarmak[247], yeni güvenlik tedbirleri konusunda sürekli aydınlatılmakla mükelleftir. Bununla da bankaların müşterileri ile elektronik bankacılık hizmetleri sözleşmelerinde ve müşterilerine yaptığı uyarılarda özellikle müşterilerin kendilerine verilen şifreleri iyi muhafaza etmeleri, bu şifreleri başka kişilere vermemeleri gerektiği belirtilmektedir[248]. Bu uyarılar, aslında elektronik bankacılık işlemlerini kullanan müşterilere bir özen yükümlülüğü getirmektedir. Burada uyarma yükümlülüğü ("Warnpflicht") müşterinin korunma menfaatine hizmet eder. Banka bu yükümlülük dolayısıyla kendi etki alanından kaynaklanan muhtemel tehlikeleri veya rizikoları ve ortaya çıkabilecek zararları diğer tarafın dikkatini çekmek zorundadır. Uyarma yükümlülüğünün özelliği her hangi bir talep gelmeksizin bankanın müşterisini uyarmasıdır. Bu özellik söz konusu yükümlülüğü bilgilendirme yükümlülüğünden ayırır[249].

Banka, bir taraftan özel hâllerin ve elektronik ortamın getirebileceği tehlikeler konusunda müşterisini sürekli aydınlatılmalı, diğer taraftan da müşterisini bazı özel

---

Hukuki Sorumlulukları", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2013, s. 98; Parolanın internet üzeri paylaşılmamasının temel nedeni sosyal mühendislik, şifre avcılığı gibi saldırılara uğramasıdır. Kimlik tanımlamada kullanılan statik ve dinamik şifre, dijital imza gibi yöntemler hakkında ayrıntılı olarak bkz. **Claessens, J. vd.**, "On the Security of Today's Online Electronic Banking Systems", Computers and Security, Vol. 21, Issue 3, Y. 2002, s. 259-261.

[246] **Memiş**, Elektronik Bankacılık, s. 878;

[247] Bu yükümlülük dolayısıyla banka kendi etki alanından kaynaklanan muhtemel tehlikelere ve zararlara karşı, diğer tarafın dikkatini çekmek zorundadır. Uy

[248] Uygulamada bankalar müşterilere parolalarını veya herhangi bir şifrelerini üçüncü kişilerle paylaşmamaları, bu bilgilere soranlara itibar etmemeleri, aynı zamanda tanımadıkları sitelerde kullanmamaları konusunda uyarıda bulunmaktadır. Banka yetkilisi müşterileri arayarak çeşitli nedenlerle kartın arkasındaki 3 haneli güvenlik kodunu, son kullanma tarihini, şifre bilgilerini talep eden üçüncü kişilere itibar edilmemesi uyarısını da ayrıca yapmaktadır. Bkz. https://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/bilgilendirme_mesajlari.page, (son erişim tarihi: 30.01.2021); Japonya'da bankalar müşterilerini, şifre ile kartın bir yerde tutulmaması, kartın üzerinde şifreyle ilgili bilginin yazılmaması, aynı zamanda şarhoş olduğu durumları düşünerek önceden kartını arabada ve yahut çalınmaya uygun ortamda bırakmamaya özen gösterilmesi konularında uyarmaktadır. Bkz. **Kaneko**, **H.,** "How Bank Depositors are Protected in Japan", Digital Evidence & Elec. Signature Law Rev., Vol. 8, Y. 2011, s. 100; **Noriko Kawawa**, "The Japanese Law on Unauthorized On-line Credit Card and Banking Transactions: Are Current Legal Principles With Respect to Unauthorized Transactions Adequate to Protect Consumers Against Information Technology Crimes in Contemporary Society?", Digital Evidence & Elec. Signature Law Rev., Vol. 10, Y. 2013, s. 76;

[249] **Akçaal,** s. 229-230.

hâllerin varlığında bilgilendirmelidir[250]. Meselâ, internet bankacılığı şubesine erişim anında önceki işlemler ya da son giriş tarihi, özel ve ayırt edilebilecek şekilde müşterinin karşısına çıkarılmalıdır[251]. Yine belirli tutarları aşan ödemelerin müşteriye kısa mesaj servisleri yardımıyla bildirilmesi gerekir[252]. Banka müşteri güvenliği açısından, gerekli gördüğü durumlarda, müşteri hesaplarındaki para çıkışı gerçekleştirildiği takdirde herhangi bir para transferi bilgilendirilmesini müşterinin belirlenmesine bakılmazsızın uygulamada kabul gören iletişim araçları (SMS, e-posta) ile gerçekleştirir. Mesela, açılış tarihinden bir yılı aşkın süre sonra işlem yapılan banka hesabı sahibine işlemin kendisi tarafından gerçekleştirilmesine ilişkin teyidi almak için banka tarafından iletinin gönderilmesinde olduğu gibi.

---

250 Gelişen teknoloji ile hacker'lar bir çok yöntemi suç işlemek için kullanmaktadırlar. Şifre ve hesap bilgilerinin çalınmasını önleyebilmek için: ***(i)*** Wintage ve Telnet programları bilgisayarda çalışır konumdayken IRC ve ICQ gibi programlar ile chat yapılmaması; ***(ii)*** Mail ile gelen .ini.,.com.,.exe. uzantılı dosyaların açılmaması ve internet sitelerinden bu uzantılı dosyaların bilgisayara indirilmemesi; ***(iii)*** Önemli trojanların kullanıldığı port numaralarının (in/out bound) bağlantılarının kontrol edilmesi, (bu kontrolün en iyi yolu kişisel bilgisayarı bir firewall ıle koruma altına almaktır. Bunun için lisanslı firewall ürünleri kullanılmalı, hiçbir şekilde internetten bu tip programlar bilgisayara kurulmamalıdır); ***(iv)*** İnternet cafe'lerde internet bankacılığı işlemleri yapılmaması ve hiç bir şekilde şifrenin kullanılmaması; ***(v)*** Bilgisayarda önemli bilgilerin tutulduğu dizinlerin şifrelenmesi; ***(vi)*** Trojan, virüs ve diğer casus programları tespit ederek bunları etkisiz hâle getiren programların kullanılması gerekmektedir. Bkz.: **Özdilek**, Örnek Olaylar, s. 71.

251 Uygulamada banka tarafından müşterilere parola ile girişlerinden sonra karşılarına çıkan güvenlik resimlerini ve kişisel bilgilerinin doğruluğunu kontrol etmeleri konusunda uyarıların yapıldığı da görülmektedir. Ayrıntılı olarak bkz. https://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/bilgilendirme_mesajlari.page, (son erişim tarihi: 30.01.2021); Son yapılan bağlantı ile ilgili müşterinin bir sonraki bağlanmasına müteakip sayfada yanıp sönen yazı ile bilgilendirilmesi de uygulamada kullanılmaktadır. Yaygın olaral son bağlantı tarihi, saati, bağlantı IP adresi gibi bilgiler müşteriye gösterilmektedir.

252 Memiş, **Elektronik Bankacılık**, s. 879; Müşteri internet bankacılığında yapacağı işlemleri miktar ve zaman bakımından kısıtlayabilir; bu işlemlerin haftanın belli gün ve saatlerde, belli miktarda sınırlı olmasını veya yapacağı işleme bildirdiği cep numarası gibi iletişim araçlarıyla bilgi ve onay verilmesini isteyebilir. Belirlenen zaman dışındaki bağlanmaların engellenmesi ve taraflarca kararlaştırılmış iletişim araçları ile bilgilendirilmesi mutlaka banka tarafından yapılmalıdır. Hatta hesaptan hesaba para aktarılmasını belli kurum veya kişilerle sınırlayabilir, IP kısıtlaması getirebilir. Bkz.: **Bilgen**, **Sözleşmeler**, s. 758; **Eralp**, s. 112; Garanti Bankasının İnternet Güvenlik Tanımlamaları menüsü müşterilerine şubelerden, Garanti İnternet'ten veya Alo Garanti'den tanımlamış olduğunu tutarın üzerinde hesaplarından para çıkışı olduğunda (havale, EFT/SWIFT/Western Union), onların belirlediği iletişim kanalından (sms, e-posta) işlemle ilgili bilgilendirme mesajı gönderilmesi, müşterinin rızası ile para transferi sonrasında bilgilendirme amacıyla iletilen e-posta içerisinde yer alan bilgilendirme ayarları adımından para transferleri bilgilendirmelerine ait işlem limitlerini değiştirme, ayrıca müşteri güvenliği gereği para transferi bilgilendirilmesine yönelik e-postalar her ayar değişikliğinde, yeni bir tanımlamada veya var olan tanımlamanın iptalinde de müşteri tarafına ileti gönderilmesi imkânı sunmaktadır. Garanti Bankasının İnternet Güvenlik Tanımlamaları ile ilgili bkz. https://www.garanti.com.tr/tr/ticari/subesiz/internet_bankaciligi/guvenlik/guvenlik_tanimlamalari.page (son erişim tarihi: 30.10.2021)

Şöyle ki, müşteri, lisanslı virüs tarama programlarını kullanmalı, bu programları zamanında güncellemeli, bilgisayarda kullanılan CD, DVD, USB Token vb. ek donanımlarda yer alan programların mutlaka virüs taramalarını yapmalıdır[253]. İnternet bankacılık hizmetlerinden yararlanan müşterilerin büyük çoğunluğu, genelde belirli bir bilgisayardan (meselâ, ev ya da işyerindeki bilgisayar gibi) işlemlerini gerçekleştirmektedir. Bu anlamda, sürekli kullanılan sabit bir IP adresi dışında başka bir adresten işlem yapılmaya başladığı hâllerde, müşterinin bilgilendirilmesi gerekir[254].

Burada cevaplandırılması gereken bir soru bankanın bilgilendirme yükümlülüğünü yerine getiriliş tarzına ilişkindir. Burada söz konusu yükümlülüğün yerine getiriliş tarzı bilgilendirme yapılacak konuların özelliğine bağımlı olarak şekillenir. Meselâ, elektronik bankacılık işlemlerinin son yapılış tarihinin sisteme girişte belirtilmesi yeterlidır. Sürekli kullanılan statik IP adreslerinin değişmesi hâlinde kişiye telefon ya da mesaj atılarak durumun bildirilmesi gerekir[255].

Özel tehlikenin gerektirdiği durumlara özgü ayrıca bilgilendirme araçlarının da devrede tutulması gerekmektedir. Banka, hatalı işlem yapan veya bilgilerinin çalındığını düşünen müşterilerin derhal arayabileceği telefon numaralarını açık tutmakla zorundadır[256]. Nitekim Banka Kartları ve Kredi Kartları Kanunu'nun (BKartK'nın) 8. maddesi uyarınca, "*Kart çıkaran kuruluşlar, kartların düzenli ve güvenli kullanımı ile bildirim, talep, şikayet ve itirazlara ilişkin gerekli tedbirleri almaya yönelik sistemi kurmak ve kesintisiz olarak açık tutmakla yükümlüdür*". Aynı şekilde elektronik bankacılığın diğer türlerinde de bankalar, müşteriyi koruyucu sistemleri kurmak zorundadır. Şöyle ki, BBSEBHY'nin 37. Maddesinin 3. fıkrasında, "*Elektronik bankacılık hizmetlerinden dolayı müşterilerin yaşayabileceği sorunları ve şikayetlerini iletebileceği ve takip edebileceği mekanizmalar oluşturulur. Oluşturulacak şikayet birimleri veya çağrı merkezlerinde müşteriyi*

---

[253] **Eralp**, s. 149.
[254] **Memiş**, Elektronik Bankacılık, s. 879;
[255] **Memiş**, Elektronik Bankacılık, s. 879; Bankacılık uygulamasına baktığımızda müşteriye bankacılık ürünleri neredeyse sadece en iyi yönleriyle sunulmaktadır. Reklamlarda, broşürlerde, web sitelerinde her ürünün tanıtımı yapılmakta, getirdiği yararlar anlatılmaktadır. Oysa ki, müşterinin ürünün ne olduğunu ve faydalarını öğrenmesi kadar önemli diğer hususlar da mevcuttur. Bunlar sistemin çalışma prensibi, hukuki altyapısı, teknik ve hukuki riskler gibi konular ile müşterinin kolayca bilgiye ulaşabilme hakkıdır. Bkz. **Özdilek**, Örnek Olaylar, s. 110.
[256] **Memiş**, Elektronik Bankacılık, s. 879;

karşılayacak menülerde ilgili elektronik bankacılık hizmetine ilişkin yaşanan dolandırıcılık vakalarının iletilmesi işleminin ana menüde ve ilk sıralarda müşterinin dikkatin sunulması ve bankaya ulaştırılan bildirimlerin en kısa sürede giderilmesine yönelik gerekli çalışmaların yapılması sağlanır" denilmektedir.

Müşterilerin farkındalığının ATM işlemleri sırasında da artırılması gerekmektedir. Banka müşterilerine, işlem sırasında ATM ekranını kendilerinden başka kimsenin görmemesi gerekliliği anlatılmalıdır. Müşteriler, ATM'de kart sıkıştığı sırada yakın çevresinde bulunan tanımadıkları kişilerin sözlerine inanmamaları ve vakit geçirmeden bankaya haber vererek kartı kapattırmaları gerektiği konusunda bilgilendirilmelidir. Banka kartları ile yapılan alışveriş zamanı karttan yapılacak tahsilatın, müşterinin gözlerinin önünde olması gerektiği, aksi takdirde, kartın manyetik alanının kopyalanabileceği konusunda bilgilendirme yapılmalıdır. Bilgilendirmeler banka personeli tarafından "debit kart" taleplerinin alınması sırasında olabileceği gibi, e-posta, mobil telefonlarla kısa mesaj (SMS) bilgilendirmeleri şeklinde de gerçekleştirilebilir[257].

B. Gerekli Tedbir /Önlem Alma Yükümlülüğü

1. Genel Olarak

Bir güven kurumu olan ve basiretli bir tacir gibi hareket etmesi gereken banka, elektronik bankacılık işlemlerinin güvenli bir şekilde gerçekleştirilmesini sağlama ve müşteri hesaplarının dolandırıcılık fiilerine karşı korunması için kendisinden beklenen her türlü önlemi[258] alma yükümlülüğü altındadır. Zira en başta kendi menfaatine ve gelir sağlamak amacıyla müşterilerine bu hizmeti sunan banka, hizmeti sunduğu müşterileri zarardan koruyucu önlemleri almak yükümlülüğü altındadır. Nitekim düşük maliyetli ve son derece basit önlemlerle, dolandırıcılık

---

257 **Eralp**, s. 86; BKartK'nın 8. maddesi uyarınca, "kart çıkan kuruluşlar, kartın verilmesi anında kart hamilini yeterli derecede bilgilendirmek ve talep edilmesi hâlinde, gerçekleştirilmiş işlemlere ait kayıtları otuz günü geçmemek üzere işlemin mahiyetine uygun bir süre zarfında sağlamakla yükümlüdür. Yurt dışı işlemlerinde bu süre altmış gün olarak uygulanır."

258 Burada kullanıcı müşterinin kendi egemenlik sahasında, nezaret ve denetimi altında bulunan kişiler vasıtasıyla şifrelerin, kullanıcı isimlerinin ve kredi kartı bilgilerinin ele geçirilmesi zamanı bankanın sorumluluğu söz konusu değildir. BKartK'nın 8. maddesi uyarınca, "kart çıkaran kuruluşlar, kartların düzenli ve güvenli kullanımı ile bildirim, talep, şikayet ve itirazlara ilişkin gerekli tedbirleri almaya yönelik sistemi kurmak ve kesintisiz olarak açık tutmakla yükümlüdür".

fiilerinin, tamamen olmasa da, büyük oranda önlenmesi mümkün olabilmektedir. Bu yükümlülüğe aykırı davranan banka, meydana gelen zarardan sorumlu olacaktır.

Dolayısıyla, bankalar elektronik ortamda müşterilerine işlem yapma imkânı verdikleri için sahip oldukları bu sistemin kesintisiz işleyişi ve ortaya çıkabilecek hataların önlenmesi konusunda gerekli tedbirleri almakla yükümlüdür. Buna ek olarak kişiselleştirilebilir güvenlik ayarları sayesinde kişiye özel ayrı bir sorunun sorulması da sağlanabilir. Bu bilgiler bankaların internet işlemleri için özel olarak hazırladığı güvenlik algoritmasından geçilerek şifrenlenmekte ve daha sonra şifrenlenmiş bilgi internet üzerinden bir SSL ile bir kez daha şifrelenerek merkez sisteme ulaşmaktadır. Kullanım aşamasında şifre ve/veya parola arka arkaya birkaç kez (3-5 kez arası) yalnış girildiğinde kullanıcı kodu otomatik olarak kullanıma kapatılmaktadır. Ayrıca belli bir süre (genellike 10 dakika) işlem yapılmadığında bağlantı otomatik olarak kesilmektedir.

Diğer taraftan, sisteme müdahalelerden korunabilmesi için müşterilerine güvenli ortam sağlayacak yazılımların ücretsiz sunulması, bu yazılımların güncellenmesi güvenliği şartlandıran faktörlerdir. Bu tür tedbir alma yükümünün ihmali hâlinde yukarıda da belirtildiği üzere bankanın kusurlu sayılması gerekir[259]. Bankanın internet bankacılığında işlem yapan kişilerin server bilgisayar numaralarının (IP loglama) kayıtlarının tutulması ve söz konusu havale işlemi yapılana kadar 3. şahıslarca arka arkaya 6 defa başarısız nakit avans çekme girişiminde bulunulması hâlinde sistemin kilitlenmesi[260] gerekli tedbirler sırasında yer almaktadır[261].

---

259 **Memiş**, Elektronik Bankacılık, s. 879.

260 "*Diğer taraftan yaşanmış bir dolandırıcılık olayında davacının internet şubesi hesabından 6 defa nakit avans çekme işlemi yapılmaya çalışılmış ancak davalıbankanın bu işlemin tamamlanması için gerekli addettiği şifre doğru girilmediği için bu işlem gerçekleşmemiştir. Burada sistemde yetkisiz bir kişinin işlem yapmaya çalıştığı açıktır. Genellikle bu durumlarda kabul edilen yöntem, sistem 2 defa şifrenin yalnış girilmesi durumunda sistemin kendisini kilitleyerek yeni bir şifre alınması için bankaya başvurulması yönünde bir uyarının müşteriye e-mail veya telefon yoluyla iletilmesidir. Nakit avans çekme konusunda 6 defa yapılan başarısız girişim sonucu sistemin kendisini kilitlemeyerek yetkisiz kişi veya kişilere davalı bankanın internet şubesinde işlem yapılmasına izin verilmesi davacının hesabından ..... USD'ının çekilmesine ve davacının bankada kayıtlı hesap bilgilerinin değiştirilmesine yol açmıştır"*. Bkz. **Özdilek**, Örnek Olaylar, s. 107.

261 Bu tedbiri almayan bankaların sorumluluğu hakkında ayrıntılı olarak bkz. **Özdilek**, Örnek Olaylar, s. 84;

Tedbir alma yükümlülüğünün kapsamı ise her geçen gün değişmekte ve gelişmektedir. Bu husus Yargıtay tarafından da vurgulanmaktadır[262]. Daha önce de belirtildiği üzere, şifre ve hesap bilgileri olan kişisel verilerin elde edilmesi yöntemlerinden biri de keylogger[263] yöntemidir. Bu yöntem internet bankacılığı kullanan müşterilerin mevduatında internet üzeri erişim zamanı rastlanmakta olup, dolandırıcılar tarafından ele geçirilen erişim şifreleri ile hesaptaki paranın diğer hesaba havale edildiği görülmektedir. Bankalar, internet bankacılık şubesine erişim zamanı şifre girilerken klavye yerine "Dynamic Keypad" kullanılacak şekilde sistemlerini güncellemektedirler. Ancak belirtmek gerekir ki, "Dynamic Keypad" ve benzeri programlar virüs, firewall gibi güvenlik programları ile desteklenmeyen ve güncel tutulmayan bilgisayarlarda yeterli korumayı sağlayamamaktadır[264].

Diğer taraftan, banka uygulamasında bir kart hamili müşteri elektronik bankacılık hizmetinden yararlanmak için şubeye başvurduğunda kendisine zarf içinde kullanıcı kodu ve şifresi verilmekte, müşteri uygulamayı ilk kullanmaya çalıştığında ise kart şifresini de girmesi talep edilmekte ve böylelikle müşteri ilk şifresini değiştirmeye zorlanmaktadır. Bundan amaç, müşterinin elektronik bankacılık hizmetini kullanmasından önce ilk şifrenin ele geçirilmiş olması ihtimalinde meydana gelecek tehlikenin önüne geçilmesidir[265].

---

262 " ... uluslararası kredi kartı uygulamasının ulaştığı aşama itibariyle davalı bankanın sahte kredi kartlarına p.o.s cihazının onay vermesini engelleyici teknik bir takım önlemler almasının mümkün olup olmadığı, eğer mümkünse bu önlemleri almaması nedeniyle sorumluluğu bulunup bulunmadığı araştırılarak sonucuna göre karar verilmesi gerekirken, eksik inceleme ile yazılı şekilde karar vermesi yerinde görülmediğinden, davacı vekilinin temyiz itirazlarının kabulü ile hükmün bozulmasına karar vermek gerekmiştir". **Yarg., 11. HD**, T. 14.11.2003, E.2003/7848, K. 2003/10886.

263 Bu şekil programlar internette yer alan hacker sayfalarından kolaylıkla elde edilebilmektedir. Özellikle internet cafelerde bu programın bilgisayarlara yüklenmesini engellemek ve bilgisayarlarda böyle bir programın var olup olmadığı konusunda sürekli teknik araştırma yapmak mümkün olmamaktadır. Örneğin, "bpk.exe" isimli keylogger programının "options (opsiyonlar)" bölümünde dolandırıcılar tarafından yapılan ayarlamalarda, kurbanın bilgisayarından bağlanacağı sitelere yapacağı şifre giriş kayıtlarının her 10 dakikada bir .....@.....com mail adresine gönderilmek üzere programlandığı belirtilmektedir. Bkz. **Özdilek**, Örnek Olaylar, s. 70.

264 **Özdilek**, Örnek Olaylar, s. 70; Belirtmek gerekir ki, uygulamada genel olarak anti-virüs programlarının bilgisayara yüklü olması ve güvenlik kalkanlarının endirilmiş olması, aynı zamanda bunların güncel tutulması gerekliliği genel olarak müşterilere bildirilmektedir. Zira, detaylı olarak söz konusu klavyenin hangi şartlarda kullanılması güvenli olur ve bu tür ortamı sağlamamaları hâlinde müşteriler ne tür zararlar görer konusunda bilgilendirme yapılmamaktadır (**Claessens vd., s.** 263).

265 **Özdilek**, Örnek Olaylar, s. 82;

Bankalar ATM sistemini ve banka kartlarının[266] teknik güvenliğinin sağlamak zorundadırlar. Bankalar, dünya üzerinde endüstri standardı olarak kabul edilmiş standartların altında teknik güvenlik önlemi sunamazlar. Bu anlamda, bankalar, maliyeti ne olursa olsun, tüm dünyada en son çıkan ve endüstri standardı olarak kabul edilen teknolojiyi[267] edinmeli ve bunu ülke içinde[268] yaygın hâle getirmelidirler. Banka, internet bankacılığı işlemlerinin gerçekleştirilmesi zamanı son güvenlik aşamasında kullanılması zorunlu olan tek kullanımlık güvenlik şifresini[269] müşterinin cep telefonuna kısa mesaj servisi aracılığıyla otomatik olarak göndermek zorundadır.

Görüldüğü gibi, internet üzeri bankacılık işlemlerinde olası dolandırıcılık hâllerinin karşısının alınması bakımından tek kullanımlık dinamik (hızlı) şifre yönteminin sunulması da banka tarafından gerekli tedbirler içerisinde yer almaktadır[270]. Bankalar tarafından sanal alışveriş işlemlerinin güvenliğinin

---

[266] Bankanın ayrıca, müşterinin, kartın kaybedilmiş ya da çalınmış olduğunu kendisine ihbar etmesinden sonra derhal bu kartın ATM'lerde kullanılmasını engelleyici önlemleri alması da gerekir. Bkz. **Arkan**, Elektronik Bankacılık, s. 17; BKartK'nın 16. maddesi uyarınca, *"kart hamili, kendisine tevdi edilen kartı ve kartın kullanılması bir kod numarası, şifre veya kimliği belirleyici başka bir yöntem kullanılmasını gerektiriyorsa bu bilgileri güvenli bir şekilde korumak ve başkaları tarafından kullanılmasına engel olacak önlemleri almak, kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi hâlinde kart çıkaran kuruluşu derhal haberdar etmek zorundadır."*

[267] Banka bankaların kullandığı ve tüm dünyada endüstri standardı olarak kabul edilen en son şifre yöntemini kullanmak zorundadır. Mesela, şifrelerin harici ortamda tutulmasını sağlayan kartlarla işlem yapılmasının çok daha güvenli olduğu tüm dünyada kabul edilmektedir. **Özdilek**, Örnek Olaylar, s. 93; İnternet üzerinden gerçekleştirilecek her bir bankacılık işlemi için, müşterinin cep telefonuna gönderilen tek kullanımlık şifre ile bankacılık işlemlerinin tamamlanması güvenlik önlemidir. Ayrıntılı bilgi için bkz. **Eralp**, s. 118;

[268] BBSEBHY'nin 42.6. maddesi uyarınca*, "ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağının veri güvenliğini, gizliliğini ve bütünlüğünü sağlayacak özellikte olması sağlanır. ATM üzerinde saklanan, iletilen, işlenen her türlü verinin gizliliği ve bütünlüğü uygun yöntemlerle korunur. PIN bilgisi, parmak izi bilgisi, kart bilgisi gibi kimlik doğrulamaya ilişkin kritik bilgilerin sayısallaştırılarak sisteme girildiği aşamadan itibaren gizliliği ve bütünlüğü sağlanır."*BBSEBHY'nin 42.3. maddesi uyarınca, "ATM cihazları üzerinde ön tanımlı olarak gelen her türlü parola, ATM cihazının bu ön tanımlı parolalarını bilen kötü niyetli kişiler tarafından yönetilmesini engellemek amacıyla, kolaylıkla tahmin edilemeyecek şekilde değiştirilir."

[269] Tek kullanmlık şifre kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele yaratılan alfabetik ve/ve ya rakamsal karakterler dizisidir. Bkz.: **Eralp,** s. 32; Tek kullanımlık güvenlik şifresi hızlı SMS yoluyla GSM şirketinin iletişim ağı üzerinden müşterinin cep telefonuna gönderilmektedir. Bankalar tek kullanımlık güvenlik şifresinin hızlı SMS yoluyla müşterilerine gönderilmesini temin etmek için Mobil haberleşme (GSM) şirketleri ile "Hızlı SMS Sözleşmesi" imzalamaktadır.

[270] Tek kullanımlık dinamik (hızlı) SMS şifre güvenlik aşamalarının en önemli ve son halkası sayılabilir. Nitekim bu yöntem kötü niyetli kişilerin hesaplara sızmalarını büyük ölçüde engellese de, tamamen yok edememiştir. Çünkü yaşanan bazı olaylarda kötü niyetli kişiler, müşterilerin bankadaki kayıtlı telefon numaralarına ait GSM operatörlerine müracaat ederek, kendilerini kart sahibiymiş gibi tanıtmakta ve kart/telefonlarını kaybettiklerini söyleyerek yenisini

artırılması için getirilen bir başka sistem ise 3D SECURE sistemidir. 3D SECURE sistemi, elektronik bankacılık dolandırıcılıklarının artması nedeniyle bankalar tarafından kullanılmakta olan güvenlik önlemidir. Nitekim hacker çeteleri bilgi sistemleri banka sistemlerinden daha hızlı ve kapsamlı güncellendiğinden teknolojinin saniyelik gelişmelerine cevap vermeyen bankaların güvenlik duvarları aşılabilmekte ve mağduriyetler doğabilmektedir[271].

Daha önce de belirtildiği üzere, interaktif bankacılık işlemlerinde, bir tarafta, kendisini alternatif dağıtım kanalları aracılığıyla bankacılık hizmetlerinden yararlanmak yetkisinin sahibi olarak tanıtan bir kişi[272], diger tarafta, bankanın otomatik olarak işlem yapmak üzere programlanmış bilgisayarı vardır. Bu anlamda, kimlik tespiti ve teşhis için elektronik ortamda sorulan soruların cevaplandırılması gerekir. Bilgisayar programından sorulan soruları cevaplayan herkes, yetkili şahıs gibi kabül edilir ve işlem yapmasına izin verilir. İnternet ortamının herkese açık olduğu dikkate alınırsa, müşteriye ayrılan işlem alanına yetkisiz kişilerin müdahele etmesi ve bilgileri ele geçirmek suretiyle usulsüz işlemleri gerçekleştirmesi söz konusu olabilir. BDDK'nın, bankacılık bilişim sistemi yönetiminde *"çok faktörlü*

çıkartmaktadırlar. Maalesef bunu da sahte belgelere dayanarak, nüfus idaresinden aldıkları soğuk damgalı nüfus cüzdanları ile yapmaktadırlar. Yeni Sim kartını alan kişiler hesabı boşaltmakta ve bu işlemi de bankanın bu yeni karta yolladığı tek kullanımlık şifreyi girerek yapmaktadırlar. Dolayısıyla bankalar tek kullanımlık şifre uygulaması ile rehavete kapılmamalı, bunun yanında başka sistemleri de devreye sokmalıdırlar. Bkz. **Savaş**, s. 153; Kişinin kimlik bilgilerini içeren belgeler ile varsa temsil yetkisini gösteren belgelerin özenli bir şekilde kontrolü sahtecilik hâlleri tespit edilebilir. Sahte kimlik veya vekaletname ile işlem yapılması hâlinde, özen eksikliğinden söz edebilmek için işlem yapan GSM çalışanının fark edebileceği düzeyde bir sahteliğin bulunması gerekir. Aksi takdirde, özen eksikliğinden söz edilemez. Sorumluluk açısından ayrıntılı bilgi için bkz. **Halil Akkanat,** "İnternet Bankacılığı Sistemi Üzerinden Bankalara Verilen Zararlardan GSM Operatörleri Sorumlu Tutulabilir mi?", Telekomünikasyon Hukuku, İstanbul, Filiz Kitabevi, 2017, s. 74.

[271] **Eralp**, s. 118;

[272] Banka kullanıcılara password, kullanıcı adı, giriş kodu, parola, şifre gibi isimlerle, kendilerini sisteme tanıtmalarına yarayacak bilgiler vermektedirler. Bu bilgilerin sisteme girilmesi durumunda banka başka kişise olmaması gereken bu bilgileri doğru giren kişinin kimliğini tespit etmiş olmaktadır. Bu amaçla, bankaların müşterilerine tanımadıkları kullanıcı adları ile şifreler, işlem parolaları, tek kullanımlık şifreler, smart kartlar, mobil/elektron imzalar, IP ve ISS kısıtlamalarına yönelik ek önlemler bu amaçla getirilmiş önlemlerden bazılarıdır. Bankalar bu önlemlerin kullanıcı adı ve şifresi olarak bilinenlerden başka bir ya da birkaç tanesinin aynı anda kullanılmasına imkân tanyarak sistemi daha güvenli hâle getirmeye çalışmaktadırlar.Onu da güvenlik açısından eklemek gerekir ki, bankalar özellikle kişilere ait olan sisteme giriş izni veren bu verileri de farklı katmanlarda ve ayrı ayrı saklamalıdır. Banka personelinin dahi bu verilere ulaşması mümkün olmamaktadır.Bkz. **Savaş**, s. 150.

kimlik doğrulama, e-imza[273]*, şifreleme"* gibi üç adet güvenlik önleminin öngörülmesine rağmen bunlardan sadece maddi külfetin en az olduğu düşünülen şifreleme; *"akıllı SMS, akıllı anahtar, şifrematik"* uygulamasını müşterinin kullanımına sunan bankanın kusurlu olduğu vurgulanmış, bu durumda mali külfeti daha az olan ve daha güvenli olan e-imza ile giriş tekniğinin müşterinin kullanımına sunulması gerektiği ifade edilmiştir[274].

Banka, dolandırıcılık hâllerinin tespiti ve gerekli önlemlerin alınması için şüpheli işlemleri bildiren program kurmakla yükümlüdür. Şöyle ki, BBSEBHY'nin 36. maddesinin 1. fıkrası uyarınca, "*banka, elektronik bankacılık hizmetleri kapsamında gerçekleşen olağan dışı, sahtekârlık amaçlı veya dolandırıcılık riski bulunan işlemleri tespit etmeye ve bunları önlemeye yönelik işlem takip mekanizmaları kurar.*"

Diğer yandan, bu madde ile işlem takip mekanizması kapsamında uygun olan durumlarda asgari olarak aşağıdaki risk unsurları belirlenmektedir:

- "*Finansal sonuç doğuran işlemlere yönelik bilinen dolandırıcılık yöntemleri*" (m. 36/1-a);

- "*Gerçekleştirilen her bir bankacılık işleminin tutarı ve bu tutarlara göre müşterinin konum bilgisi de kullanılarak normal dışı bir ödeme, fon transferi ya da davranış deseni gösterip göstermediği*" (m. 36/1-b);

---

[273] Elektron imzalı belgeler de el yazısı ile atılan imzan ile aynı hukuki ispat gücüne sahip olmalarına ilişkin görüşler için bkz. **Muzaffer Şeker**, Elektronik Ödeme Sistemleri, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl:11, Sayı 20, Güz 2012/2, s. 150.

[274] **Eyyup Ensar Ceylan**, "İnternet Bankacılığı ve Bankaların Hukukî Sorumlulukları", s. Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2013, 105; *BBSEBHY'nin 34*.1. maddesi uyarınca, *"bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç doğurmayan işlemler de dâhil olmak üzere elektronik bankacılık hizmetleri için bankaların müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır*." Tıpkı aynı düzenleme ATM'lerle ilgili konulara da uygulanmaktadır. Özellikle kart sisteminde güvenlik müşterinin "bildiği" ve fiziksel olarak "sahip olduğu" bileşenlerin varlığı ile sağlanır. Ayrıntılı olarak bkz. **Kaneko**, s. 99; Biyometrik yöntemler içerisinde banka tarafından en yaygın kullanılmakta olanı parmak izi ile kimlik tanımlamasının yapılmasıdır. Bkz.: **Claessens vd.**, s. 263.

- "*Kaybolmuş, çalınmış ya da yetkisiz kişilerce ele geçirilmiş kimlik doğrulama unsurlarının listesi*" (m. 36/1-c);

- "*Her bir kimlik doğrulama oturumuna yönelik olarak zararlı yazılımların bulaşmış olabileceğini gösteren belirtiler*" (m. 36/1-ç).

Bankacılık uygulamasında müşteri işlemleri sisteme tanımlanmış senaryolar aracılığı ile tespit edilir ve söz konusu işlemlere karşı banka personeli tarafından (müşteri aranmakla yahut karta bloke konulmakla[275], internet bankacılık hesabı veya IP kilitlemesi[276] yapılmakla) dolandırıcılık hâlleri önlenebilmektedir. Meselâ, internet bankacılığı işleminin gerçekleştirildiği IP adresine ilişkin bilgilere (sisteme ne zaman giriş yapıldığı, hangi işlemlerin yapıldığı) bankaların log kayıtlarının incelenmesi sonucunda ulaşmak mümkündür.

Yine banka, müşterilerin hesap hareketlerini belli istatistikler dâhilinde takip etmeli, daha önce yapılmış işlemlere nazaran farklılık arz eden, olağan dışı bir işlem olduğunda banka bu durumu farketmelidir. Meselâ, hiç havale yapmamış olmasına rağmen bu sefer yüklü miktarda havale yapan veya çok kısa aralıklarla ve çok sayıda havale işlemi gerçekleştiren bir müşteri işlemi hemen algılanmalı ve gerekli güvenlik tedbiri hemen uygulamaya konulmalıdır. Burada sayılan hususlar, sınırlı sayıda değildir[277].

---

[275] Alman Hukukunda (BGB, §675k) bloke konulması zamanı banka tarafından müşterinin bloke sebebi ile ilgili bilgilendirilmesi taleb edilmektedir. Aynı zamanda banka tarafından bloke sebebi aradan kalktığı anda blokeni kaldırması bir yükümlülük olarak bankanın üzerine konulmuştur. Bu tür bloke konulma ve bloke kaldırılma işlemlerine göre bankanın müşteriden her hangi hizmet tutarı talep etmesi yasaklanmıştır. Yalnız kayıp ve ya çalıntı banka kartının yenisinin siparişi için bir komisyon miktarının müşteriden alınması söz konusu ola bilir. Bkz. German Civil Code, Bürgerliches Gesetzbuch (BGB), Volume I, Books 1-3: Paragraph 1-1296, Article-by-Article Commentary, edited by Gerhard Danneman Reiner Schulze, Nomos, 2020, s.1321.

[276] Her seferinde başka IP numaralarından sisteme giriş yapan tabiri caiz ise gezgin bir müşteri söz konusu ise banka, IP değişikliğine bağlı herhangi bir kilitleme yapmamalıdır.

[277] **Savaş**, s. 153-154; ATM kart hareketleri ve trendleri, güvenlik bölümleri tarafından yardımcı bazı yazılımlar kullanılarak incelenmeli, müşterilerin olağan işlem akışına aykırı dışı nakit çekimleri veya alışverişleri mutlaka müşteriye sorulmalıdır. Bkz. **Eralp**, s. 86; BBSEBHY'nin 42.7. maddesi uyarınca, *"Banka, ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık oluşturan çalışmalarda bulunur."* Söz konusu maddeyi daha açmaya çalışırken, banka, ATM cihazlarına ilişkin hırsızlık, sahtekarlık, fiziksel saldırı gibi tehditlere ilişkin riskleri minimize edici önlemler tesis eder ve ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık yaratır. Diğer taraftan banka kartlarına günlük nakit çekimde kısıtlama getirilmesi de bankanın müşterilerinde üsulsuz işlemlere karşı farkındalık yaratmasının nedeni olarak da nitelendirilmektedir. Bkz. **Kaneko**, s. 101; Japonya mevzuatı gereğince, bankanın getirmiş olduğu nakit çekim kısıtlamasının değiştirilmesi imkânı müşteriye sunulabilir. Bkz.: **Kawawa**, s. 77;

Banka, ATM önünde çizgi çekerek elektronik bankacılık hizmetinden yararlanan müşteri dışındaki şahısların çizginin gerisinde kalmaları konusunda bir teamül oluşturabilir. Böylelikle de, ATM karşısında oluşması muhtemel kalabalığın yolaçabileceği risklere (meselâ, kart şifresinin öğrenilmesi vs.) karşı tedbir alınmış olur[278]. Daha önce belirtildiği üzere, elektronik işlemlerin ATM aracılığı ile yapılması da en çok kullanılan alternatif dağıtım kanallarından biridir. ATM'lerin sistem güvenliği ile beraber fiziki güvenliğinin de sağlanması bankanın yükümlülükleri sırasındadır. Banka, ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler almalı, cihaza yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasını sağlayacak bütün giriş noktaları erişime kapatmalıdır. ATM'ler üzerine, güvenlik açıklıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ek güvenlik tedbirleri uygulanır. Banka, ATM cihazlarının bulunduğu yerlere güvenlik kamerası koyar, ancak bu güvenlik kamerası, müşterinin klavye hareketlerini göremeyecek biçimde konumlandırılır. Güvenlik kamerası kayıtları en az iki ay süreyle saklanır ve kamera teçhizatçıları çalıştıklarına dair düzenli olarak kontrol edilir. Görüntüleme alanı bakımından ATM'yi kapsayan ve bir güvenlik kamerası altyapısının varlığı durumunda ATM'ye özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur[279]. Bankalar, özellikle şubelerin dış duvarlarına yerleştirdikleri ATM'ler aracılığıyla işlemi yapan müşterilerini, sokaktan geçen kötü niyetli kişilerin tecavüzlerine karşı korunmak üzere gerekli önlemleri de almak zorundadırlar. Bu çerçevede bankalar, müşterilerin ATM'yi, sokaktan geçen kişilerin

---

[278] **Eralp**, s. 86; Amerikan mahkemesinin Ognibene v. Citibank, N.A. davasında bankanın ATM ile ilgili fiziksel açıdan güvenlik tedbirlerini uygulamaması sebebinden müşterinin PIN bilgisi ATM'de işlem yaparken üçüncü kişi tarafından omuz arkasından izlenerek çalınmıştır. Mahkeme bankanı bu tedbirleri almamakla suçlamış ve sorumlu tutmuştur. Bu karadan sonra Citibank tarafından ATM önünde işlem yapan müşteriler arasında ara mesafenin sağlanmas açısından çizgiler konulmuş ve kırmızı bir dairenin içerisinde Citibank kartınızın kendiniz için değil başka işlemler için kullanılmasına izin vermeyiniz şeklinde müşterilere uyarıda bulunulmuştur. Bkz. **Mason, Stephen** Electronic Signatures in Law, SAS Humanities Digital Library, School of Advanced Study, University of London, 2016, s. 219.

[279] Bkz. *BBSEBHY'n*in 42.4 ve 42.9. maddeleri.

dikkatini çekmeden kullanabilecekleri bir ortam sağlamakla yükümlüdürler[280]. Aksi hâlde işlemin yapılması sırasında üçüncü kişilerin, müşterinin yanına yaklaşarak, çekilen parayı zorla almaları veya şifreyi öğrenmelerinden doğan zararlardan da koruma yükümünün gereklerini yerine getirmeyen bankanın sorumlu tutulması gerekir[281]. Dikkat edilmesi gereken hususlar ve alınması gereken önlemler bankaca tespit edilir, zira müşterilerden farklı olarak, bankalar internet bankacılığını başlatan ve idare eden taraftır, aynı zamanda, daha büyük ekonomik güce sahiptirler. Teknolojik şartlardaki değişmelere paralel olarak bankalar da bu tedbirleri geliştirmeli ve değiştirmelidir. Kanızımızca, dijitalleşen günümüzde gerekli tedbir almanın boyutu değişmelidir. Şöyle ki, elektronik bankacılık hizmeti veren bankalardan müşterilerine ücretsiz bir anti-virüs programı tahsis etmesi, internet güvenliğini sağlaması ve bu esnada buna ilişkin teknik güncellemeleri ücretsiz erişime açması beklenmektedir.

2. Alınması Gereken Önlemler

Bankaların gelişen teknolojiyi bankacılık hizmetlerine entegre etmeleri sonucunda, elektronik bankacılık bireysel ve kurumsal müşteriler için daha da ulaşılabilir hâle gelmiştir. Ancak elektronik bankacılık bilinen yararlarının yanında birtakım güvenlik risklerini de beraberinde getirmektedir. Bankaların söz konusu riskleri belirleyerek, internet bankacılık hizmetlerinin doğasından kaynaklanan güçlükleri tedbirli bir şekilde yürütmeleri beklenmektedir. Meselâ, internet bankacılığında alınabilecek güvenlik önlemleri aşağıdaki şekilde sıralanabilir[282]:

i. Elektronik ortamda gerçekleşen işlemler için uygun bir kimlik doğrulama mekanizması kurulmalıdır. Risk değerlendirmesi bankacılık işleminin niteliğine göre yapılmalıdır. Finansal işlemlerde, işlemin başlangıcından son aşamasına kadar kimlik doğrulamada yüksek güvenlik uygulanmalıdır.

---

[280] Mesela, ATM ile işlem yapılabilmesi için kapalı bir mekan sağlanması gibi. BKartK'nın 8. maddesi uyarınca, "*kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür*".

[281] **Arkan**, Elektronik Bankacılık, s. 17.

[282] **Ergüç**, s. 93-96.

ii. Güvenlik kontrollerinin yeterliliği yılda en az bir kez test edilmeli ve sızma testleri yapılmalıdır. Şüpheli işlemlerde takip mekanizması kurulmalıdır.

iii. Müşterinin internet bankacılığına giriş aşamasındaki kimlik kontrollerinin en üst güvenlik düzeyinde yapılabilmesi için bankalar tarafından uygun yapının kurulması gereklidir. Bu aşamada kullanılacak parola, karmaşık ve tahmini zor nitelikte olmalı ve sistem bunun için müşteriyi zorlamalıdır. Parolanın değişmesi en üst güvenlik düzeyinde yapılmalıdır.

iv. Bankaların güvenlik birimlerinde etkin bir izleme programı kullanılmalıdır. Müşterilerin alışkanlıkları dışında, şüpheli saatlerde ve ilk defa yapılacak işlemleri sistem tespit etmeli bu işlemleri onay aşamasında bekletmelidir. Gerekli güvenlik incelemeleri yapıldıktan sonra onay verilmelidir.

v. Banka tarafından sunulan internet bankacılığı hizmeti müşterilerin yanlış işlem yapmasını azaltacak gerekli kontrolleri içerecek şekilde düzenlenmeli ve başlattıkları işlemlere ilişkin riskleri tamamen anlamalarını sağlamalıdır.

vi. Bankalar tarafından internet şubesi kullanan müşterilerine belli dönemlerde otomatik olarak virüs tarayıcı programlar gönderilmelidir.

vii. Müşteriler internet şubesi başvurusu aşamasında bilgilendirmeli ve daha sonra da banka güvenlik önlemlerini hatırlatıcı uygulamalarda bulunmalıdır. İnternet şubesi başvuru formlarında güvenlikle ilgili özet bilgiler yer almalıdır. Ayrıca bankanın internet sayfasında da bu bilgiler müşteri finansal işleme başlamadan önce dikkat çekici yerlerde bulunmalıdır. Belli aralıklarla müşterilere sms, posta ve e-posta yoluyla güvenlik önlemleri hatırlatılmalıdır[283].

---

[283] Genel olarak internet bankacılığında yaşanan ve hem bankayı hem de müşterisini sıkıntıya sokan dolandırılıcılık eylemlerinin bir çoğu, genellikle müşterilerin bu konudaki bilinçsizliklerinden kaynaklanmaktadır. Bankaların öngördüğü güvenlik tedbirlerini kendi bilgisayarında sağlamayan, bu kriterlere uymayan ve bilgisayarlarında güvenlik açıkları yaratan kullanıcılar internet casuslarına davetiye çıkarmaktadırlar. Bu durum karşısında bankaların yapması gereken üç şey vardır: (i) ilk olarak müşterilerini internet bankacılığı riskleri konusunda daha çok bilinçlendirmeye ve farkındalık yaratmaya çalışmak; (ii) ikinci olarak, gelişen ve değişen teknolojiye bağlı olarak öngördüğü güvenlik çıtasını sürekli yükseltmek ve bu güvenlik önlemlerinin müşteriler tarafından kullanılmasını, müşteri için opsiyonel (seçimlik) kılmak yerine, mutlaka "zorunlu" kılmak; (iii) üçüncü olarak ise, her zaman bu tedbirleri müşterilerinin almalarını beklemek yerine, banka tarafından öngörülen koruma tedbirlerini almayan müşterilerin internet bankacılığını kullanmalarına izin vermemek, işlem yaptırmamak. Bkz. **Leyla Keser**

viii. Banka, internet bankacılığı faaliyetlerine ilişkin işlem ve kayıt tutma süreçlerini ve alt yapısını, delil üretecek ve bu delillerin bozulmasını önleyecek, yanıltıcı delilleri ayırt edebilecek ve taraflara sorumluluk yüklemede kullanılabilecek bilgileri sunacak şekilde yapılandırmalıdır.

ix. Banka, internet bankacılığı hizmetine ilişkin mevcut politika ve prosedürler ile dikkat edilmesi gereken hususlar konusunda müşterilerini bilgilendirmeli ve gerekli uyarılarda bulunmalıdır. Ayrıca banka, müşterinin talebi olmadan müşteri adına internet bankacılığı açmamalıdır.

x. Elektronik imza kullanımı ve yararları hakkında daha çok bilgilendirme yapılmalı ve müşterinin bu sistemi kullanımına teşvik edici faaliyetlerde bulunulmalıdır.

Bankaların yönetim kurulu ve üst yönetim tarafından uygun görülen kapsamlı bir risk yönetim sürecine sahip olması zorunludur[284]. Elektronik bankacılık ve elektronik para faaliyetlerinde yeni riskler teşhis edildikçe ve değerlendirildikçe, yönetim kurulu ve üst yönetim bunlar üzerinde kapsamlı bir inceleme yaparak, süreçteki risklerin değerlendirildiğini, kontrol edildiğini ve izlendiğini, alınan tedbirlerin yeterli olup olmadığını araştırmalıdır.

C. Sistem Aksaklıklarının (Hatalarının) ve Eksikliklerinin Giderilmesi

Daha önce de belirtildiği üzere, elektronik bankacılık işlemleri, büyük ölçüde, insan yerine bankanın bilgisayar sistemleri ve söz konusu sistemlere yüklenen programlar sayesinde gerçekleştirilmektedir. Meselâ, internet bankacılığında, bankanın en önemli yükümlülüğü web sitesi üzerinden yapılmasını taahhüt ettiği bankacılık işlemlerinin taahhüt ettiği şekilde yapılabilmesini sağlamaktır. Bu sebeple söz konusu yükümlülük bankanın asli edim yükümüdür. Gerçekten de, bankalar, web sitelerinde ve çeşitli medya kanallarında verdikleri reklamlarda, 7 gün 24 saat

---

Berber, İnternet Bankacılığında Banka ve Müşterilerin Sorumluluğu, beyazsapka. org (son erişim tarihi: 30.01.2021).

284 Banka yöneticileri, benzer işlem ve kararlarda meslektaşlarının çoğunluğu gibi bankacılık sektöründe davrandığı takdirde kendisinden beklenen özeni gösterdiği kabul edilecek, yaptığı işlemler nedeniyle sorumlu tutulamayacaktır. Bkz. **Açıkgöz**, s. 15.

internet bankacılığı hizmeti verdiklerini beyan etmektedirler. Bankalar vermiş oldukları beyanlara göre internet bankacılığının bir gereği olarak kendi web sitelerinin 7/24 çalışmasını sağlamalıdırlar. Banka, önceden müşteriye haber vermeksizin web sitesini bakıma almamalı, uzun süreli bakımda tutmamalıdır. Bu durumda ortaya çıkmış veya çıkacak zarara göre banka sorumludur. Mesela, müşteri vadesi gelmiş bir borcunu ödemek için İnternet'ten havale yapmaktadır. Ancak bankanın web sitesinin çalışmaması veya yavaş çalışması sebebiyle havale ya hiç veya zamanında yapılamamıştır. Bu gibi sorunlar genellikle, bankanın teknik altyapısının yeterli olmamasından kaynaklanmaktadır. Bankanın web sitesi, teknik alt yapısının kaldırabileceğinden daha fazla müşteri tarafından ziyaret edilmesi durumunda kilitlenmektedir. Böylece bankanın websitesi ya hiç çalışmamakta veya yavaş çalışmaktadır. Bu gibi durumlarda, bankanın edimini gereği gibi ifa ettiği söylenemez. Bu sebeple, müşteri bir zarara uğramışsa, zararını ispat etmesi hâlinde banka sözleşmenin ihlâli sebebiyle söz konusu zararları tazmin etmek zorundadır[285].

Almanya Itzehoe Asliye Mahkemesinin bir kararında "*sistem hatası sebebiyle zarara uğrayan müşterinin zararı, taraflar arasında yapılan sözleşme hükümlerinin ihlâline dayanarak çözülmüştür. Dava konusu olayda müşteri, davalı bankanın sistemlerindeki hata yüzünden 5 Nisan 2000 tarihinde saat 10:29 civarında almış olduğu 100 adet üzerindeki Morphosys hisselerini alış fiyatı üzerinden satmak istemiş, ancak saat 10:48'de hisseler 265 Euro limitinde iken satamamıştır. Müşteri, bir taraftan sistemi tekrar tekrar denemiş, bir taraftan da bankayı durumdan derhal haberdar etmiştir. Bütün çabalara rağmen bankanın sistemi ancak saat 11:03'de açılabilmiştir. Ancak bu süre içinde hisse değeri, saat 11:02'de 260 Euro'ya düşmüştür. Müşterinin hisse senetlerini satamaması tamamen bankanın bilgisayar sistemlerinin hatasından kaynaklanmaktadır ve müşteriye vaat edilen internet erişimi sağlanamamıştır. Bu durum sözleşmenin ihlâli olarak değerlendirilmiştir. Bu karardan anlaşıldığı üzere, müşterilerin, bankaların sistem hatalarından kaynaklanan zararlarından bankalar sorumludur*"[286].

---

[285] **Yılmaz S.**, s. 201-202.
[286] **Eralp**, s. 191.

III. Sözleşme Sonrası Aşamada Özen Yükümlülüğünün İfası

Sözleşme sonrası aşamada bankanın özen yükümlülüğü bir koruma yükümlülüğü olan sır saklama yükümlülüğünün yerine getirilmesinde uygulama alanı bulmaktadır[287]. Sır saklama sonraya etki eden bir yükümlülük olarak tanımlanmaktadır. Sır saklama gibi sonraya etki eden bir yükümlülük aslî edim yükümlülüğünün sona ermesinden sonraki varlıkları burada önem arz etmektedir[288]. BanK'nun 73. maddesi, "Sır saklama" başlığı altında bankaların sır saklama yükümlülüğünü düzenlemektedir. Maddede sır saklama yükümlülüğünün tanımına yer verilmemekle birlikte bu kavram hem müşteri sırrını hem de banka işletmesi sırlarını kapsayacak şekilde kullanılmıştır. Çalışmamız açısından önem arz eden hiç şüphesiz müşteri sırrıdır. Sır, açıklanması istenmeyen gizli bilgiyi ifade eder[289]. Bankanın müşterileri ile olan ilişkilerinde, sözleşme öncesi ve sonrası elde ettiği tüm bilgiler, müşterinin nakit ve mal varlığı durumu, kredi itibarı, yatırım faaliyetleri, kâr ve zarar hesapları, müşteri hakkındaki yasal takipler ve davalar müşteri sırrı kapsamındadır[290]. Kişilerin banka ile tek bir hukuki ilişkiye girmeleri müşteri sayılmaları ve sırların korunması için yeterlidir[291]. Doktrinde[292] bankanın sır saklama yükümlülüğü başlıca üç temele dayandırılmaktadır. Bunlar kısaca, dürüstlük kuralı, kişinin gizli (mahrem) alanına saygı gösterilmesi hususundaki mutlak kişilik hakkı ve bankaları düzenleyen ekonomik yönetim hukukundan doğan ve cezai yükümlülük de getiren mesleki bir görev olarak ifade edilebilir.

Elektronik bankacılıkta bankaların sır saklama yükümlülüğüne iki açıdan bakılabilir. Şöyle ki, bir yönüyle, bankaların sır saklama yükümlülüğü, müşteri bilgilerinin (sırlarının) üçüncü kişilere açıklanmasının bankaya yasaklanmasını ifade eder. Diğer yönüyle, söz konusu yükümlülük gereğince bankalar, müşterilere ait verilerin gizliliğine ilişkin gerekli tedbirleri almak zorundadırlar. BBSEBHY'nin 9.

---

[287] **Tekinalp'e** göre, banka sırrını açıklamama, sözleşme hukukunda temelini güven ilkesinde bulan biir yan yükümlülüktür. Bkz.: **Tekinalp,** s. 412

[288] Ayrıntılı bilgi için bkz. **Akçaal,** s. 178.

[289] **Battal**, s. 210.

[290] **Reisoğlu**, S., Bankacılık Kanunu Şerhi, C. 2, Gözden Geçirilmiş 2. bs., Yaklaşım Yayınları, Ankara, 2015, 1496 vd.; **Tekinalp,** s. 412.

[291] **Reisoğlu**, C. 2, s. 1497.

[292] **Stoufflet**, s. 10-11; **Battal**, s. 211-212; **Kaplan**, Sözleşme, s. 47-48; **Tandoğan**, Bankacının Hukuki Sorumluluğu, s. 118; **Kandıralıoğlu**, s. 91 vd; **Eralp**, s. 250.

maddesinde bu hususa ilişkin düzenlemelere yer verilmiştir. Şöyle ki, BBSEBHY'nin 9.1. maddesinde "*Banka, bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliğini sağlayacak önlemleri alır. Verilerin tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin gizlilik derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanır*."

BBSEBHY'nin 11/3 maddesinde bankalar tarafından gizliliği sağlamak üzere yapılacak çalışmalara ilişkin asgari talepler öngörülmüştür. *"Banka, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alır."* Bununla da sıfat ve görevleri gereğince banka veya müşteriye ait sırları öğrenenlerin bu bilgileri üçüncü kişilere aktarması ve onları kullanarak menfaat elde etmesi yasaklanmış olur. Mesela, banka müşterisiyle olan sözleşme ilişkisi bittikten sonra da sır saklamakla yükümlüdür. Sır saklama yükümlülüğünün sadece bir yapmama biçiminde davranışdan ibaret olması düşünülse bile, bunun yanında bu yükümlülük sırrın muhafazası için bazı davranışları gerekli kıla bilir[293].

Diğer taraftan BanK'nun "Sır saklama" başlığı altında 73. maddesi hükümleri gereğince, sıfat ve görevleri dolayısıyla bankalara veya müşterilerin ait sırları öğrenenlerin söz konusu sırları saklama yükümlülüğü açısından bir zaman sınırlaması bulunmamaktadır[294].

---

[293] **Akçaal, M.,** Sözleşme Sonrası Sorumluluk (Sözleşme Sonrası Yükümlülüklerin İhlâlinden Doğan Sorumluluk), 1. bs., Konya, Sayram Yayınları, 2018, s. 221-222.

[294] **Reisoğlu**, C. 2, s. 1485

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK BANKACILIKTA BANKANIN ÖZEN YÜKÜMLÜLÜĞÜNÜN İHLÂLİNİN HUKUKÎ SONUÇLARI

Elektronik bankacılık hizmetleri kapsamında birçok işlemin alternatif dağıtım kanalları aracılığıyla yapılması artık modern toplumun bir vazgeçilmezi hâline gelmiştir. Nitekim TBB'nin Haziran 2018 yılına ilişkin Dijital, Internet ve Mobil Bankacılık İstatistikleri'nde[295] "*aktif dijital bankacılık müşteri sayısının 39 milyon kişiye ulaştığı, toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısında bir önceki döneme göre 2 milyon kişi artış olduğu"* açıklanmıştır. Ancak internetin banka-müşteri ilişkisine aktif katılımı bankacılığa ait genel hukukî sorunların yanı sıra bazı ilave sorunların da ortaya çıkmasına sebebiyet vermiştir. Mesela, günlük ticaret işlemlerini internet bankacılığı üzerinden yapan müşteriler açısından bankanın ana bilgisayarına yeterli ve kesintisiz erişimin (servis sürekliliğinin) sağlanması büyük önem arz etmektedir. Bundan başka, müşterilere uygulanan kimlik doğrulama mekanizması ve güvenlik tedbirleri gibi konular elektronik bankacılık açısından karakteristik hususlardır. Bu anlamda, finansal işlemleri ve elektronik bankacılığın kabulünü tehlikeye atan oltalama (*phising*), yalnış alan adına yönlendirme (*pharming*) ve kimlik hırsızlığı (*identity theft*) gibi sorunların hukukî müzakerelerin ve yargı kararlarının odak noktası hâline gelmesi yadırganmamalıdır. Cevaplandırılması gereken diğer bir önemli konu *yapılan usulsüz elektronik bankacılık işlemleri açısından ispat külfetine ilişkindir.*

Elektronik bankacılıkta özen yükümlülüğüne aykırı davranan bankanın müşteri ile arasında olan sözleşme hükümleri gereğince sorumlu olacağı açıktır. Bu sebepten aşağıda sırasıyla bankanın sözleşmeden doğan sorumluluğunun şartları, özen yükümlülüğünün ihlâliının sonuçları ve nihayet tarafların ispat külfetine ilişkin konulara değinilmiştir.

---

[295] **TBB**, Dijital, Internet ve Mobil Bankacılık İstatistikleri Haziran 2018, Rapor Kodu: DT22, Temmuz 2018, s. i.

§ 1. Elektronik Bankacılıkta Bankanın Özen Yükümlülüğünün İhlâli Sebebiyle Sözleşmeden Doğan Sorumluluğu

I. Genel Olarak

Doktrinde[296] sorumluluk kelimesi iki anlamda kullanılmaktadır. Bunlardan ilki, bir kimsenin haksız fiilinden yahut borca aykırı hareketinden sorumlu olduğunu ifade eder ve bu durumda sorumluluk deyimi "... den sorumluluk" olarak karşımıza çıkar. İkinci anlamda "sorumluluk"tan amaç borcunu yerine getirmeyen borçlunun alacaklıya karşı malvarlığıyla mesul olmasıdır ki, bu durum da "... ile sorumluluk" olarak ifade edilebilir.

Diğer yandan, "sorumluluk" deyimi ile genel olarak sözleşme dışı sorumluluğun, özel olarak da sebep sorumluluğunun (kusursuz sorumluluk) belirtilmesi için kullanılır[297].

Çalışmamızda elektronik bankacılıkta özen yükümlülüğünü ihlâl eden bankanın borca (sözleşmeye) aykırı davranışından sorumluluğu inceleme konusu yapılmıştır. Ancak, TBK'nın 114. maddesinin 2. fıkrası gereğince, "*haksız fiil sorumluluğuna ilişkin hükümler, kıyas yoluyla sözleşmeye aykırılık hâllerine de uygulanır*". Bu anlamda, sorumluluk hukukunun zararın tazminine ilişkin kusur, uygun illiyet bağı, sorumluluğu hafifleten veya kaldıran sebepler kimi temel kurumlar bu çalışmayı da ilgilendirmektedir.

Ancak doktrinde borcun hiç veya gereği gibi ifa edilmemesi konusunda görüş birliği bulunmamakta, söz konusu kavramı ifade etmek maksadıyla farklı içerikli terimler kullanılmaktadır.

Şöyle ki, doktrinde ileri sürülen bir görüşe göre, borcun ifa edilmemesi (veya borç ilişkisinin ihlâli) kavramı kusurlu imkânsızlık, gereği gibi ifa etmeme ve

---

296 **Kocayusufpaşaoğlu**, s. 26; **Eren**, Genel Hükümler, s. 84; **Oğuzman/Öz**, C I, s. 16.

297 **Tandoğan**, **H.**, Türk Mes'uliyet Hukuku (Akit Dışı ve Akdi Mes'uliyet), Ajans-Türk Matbaası, Ankara, 1961, s. 3-4.

temerrütü kapsamaktadır[298]. Gereği gibi ifa etmeme ise, bir üst kavram olup, kötü ifa ile yan yükümlülüklerin ihlâli hâllerini içermektedir.

Diğer bir görüş[299] uyarınca, borca aykırılık hâlleri dört ana başlık altında toplanabilir: kusurlu sonraki imkânsızlık, kötü ifa (gereği gibi ifa etmeme), sözleşmenin müspet ihlâli ve temerrüt.

Doktrinde Alman hukukunda olduğu gibi tüm yükümlülük ihlâllerini kapsayan "ifa engelleri" kavramının kullanılması görüşü de savunulmaktadır[300]. Buna göre, ifa engelleri kavramı alacaklı temerrüdü, imkânsızlık (ifa edememe), borçlu temerrüdü (ifa etmeme), sözleşmenin müspet ihlâli (ayıplı ifa ve benzeri kötü ifa olguları) ve işlem temelinin çökmesini (imkânsızlığın bir altında yer alan, "ifanın beklenmezliği, yüklenmezliği" olgusunu) kapsamaktadır.

Doktrinde ileri sürülen başka bir görüşe[301] göre, borcun ifa edilmemesi, hiç ifa etmeme ve gereği gibi ifa etmeme olarak ikiye ayrılır. İmkansızlık ve borçlunun temerrüdü borcun ifa edilmemesi, kötü ifa ise gereği gibi ifa edilmeme olarak karşımıza çıkar. Kötü ifa, ifaya yardımcı yan yükümlülükler ile koruma yükümlülüklerinin ihâlini ve ayıplı ifaye da içine alan bir üst kavramdır[302].

Doktrinde akdin ihlâli kategorileri kavramı altında imkânsızlık, borçlu temerrüdü, geniş ve dar anlamda gereği gibi ifa etmeme hâllerini inceleyen inceleyen görüş de savunulmuştur[303]. Buna göre, geniş anlamda gereği gibi ifa etmeme hâlinde, borçlunun borcunu yerine getirmek amacıyla edimde bulunmasına rağmen, bu edim kanun veya sözleşmede öngörülen şartlara uymamaktadır. Bu anlamda bir yüküm ihlâli, borç ilişkisinin taraflarına, edimin muhtevasına, ifa yerine ve zamanına ilişkin olabilir[304].

Dar anlamda gereği gibi ifa etmeme ise edimin kanun veya sözleşme ile öngörülen vasıfları taşımaması (yani ayıplı ifa) hâlini kapsamaktadır. Burada gereği

---

[298] **Eren**, Genel Hükükmler, s. 1027 vd; **Oğuzman/Öz**, C. I, s. 369 vd.
[299] **Kılıçoğlu**, s. 663 vd.
[300] **Serozan**, İfa Engelleri, s. 133-134.
[301] **Akıncı**, Borçlar Hukuku, s. 225 vd.
[302] **Akıncı, Ş.**, Kötü İfa-Eksik İfa-Ayıplı İfa Ayrımı ve Bu Ayrımın Hukuki Sonuçları, 1926'dan Günümüze Türk-İsviçre Medeni Hukuku, C. 2, Yetkin Yayınları, Ankara, 2017, s. 1393.
[303] **Aral**, s. 67 vd.
[304] **Aral**, s. 74.

gibi olmama, edimin vasfına ilişkin olduğu için "nitelik yönünden gereği gibi ifa etmeme" hâli söz konusu olmaktadır[305].

Elektronik bankacılık hizmetleri sağlayan bankanın aslî edim borcu bankanın şube dışındaki dağıtım kanalları (ATM, dialog, internet bankacılığı, mobil bankacılık, SMS bankacılığı vd.) aracılığıyla müşteriye bankacılık hizmetlerini (hesap açılışları, para transferleri, yatırım işlemleri, ödeme işlemleri, kredi kartı işlemleri vs) sunmaktan ibarettir. Bankanın bu edim yükümlülüğünü hiç veya gereği gibi yerine getirmemesi nedeniyle, genel olarak borçlu için öngörülen müeyyidelere (aynen ifaya mahkûm etme, tazminat ödeme gibi) tâbi tutulması gündeme gelmektedir. Elektronik bankacılık sözleşmesinden kaynaklanan bu sorumluluk, genellikle müşterinin (alacaklının) ifa etmeme veya özensiz ifa nedeniyle bankaya (borçluya) yönelttiği aynen ifa ve (veya) tazminat talebi şeklinde ortaya çıkar.

Belirtmek gerekir ki, elektronik bankacılık hizmetleri açısından bankanın sorumluluk sebebi gereği gibi ifa etmeme şeklinde meydana çıkmaktadır. Gereği gibi ifa etmeme ise, sözleşme ile kararlaştırılmış aslî edim borcunun ifasında özensiz davranılması biçiminde görünebilir. Zira "özen" kavramsal olarak daima bir aslî veya yan edimi, davranışı şart koşar[306]. Ancak sözleşme ihlâli sadece aslî edim borcu bakımından değil, yan yükümlülüklerin, özellikle de koruma yükümlülüklerinin ihlâlinden de kaynaklanabilir[307]. Mesela, bilgilendirme veya sır saklama yükümlülüklerinin ihlâlinde olduğu gibi.

II. Sorumluluğun Şartları

A. Özen Yükümlülüğünün İhlâl Edilmesi

1. Genel Olarak

Çalışmamızın ikinci bölümünde bankanın özen yükümlülüğünün uygulanma başlığı altında bankanın yerine getirmesi gereken edimlere ilişkin gerekli açıklama

---

[305] **Aral**, s. 75 Yazara göre, temerrüt ve imkânsızlık dışında kalan sözleşme ihlâllerini akdin müsbet ihlâli üst kavramı altında toplamak, bu deyimi gereği gibi ifa etmeme deyimini tercih etmek gerekir. Bak. **Aral**, s. 105.

[306] **Gümüş**, Özen Borcu, s. 47; **Başpınar**, s. 56 vd.

[307] **Eren**, Genel Hükümler, s. 1046 vd.

yapılmıştır. Söz konusu bölümde belirtildiği üzere, banka elektronik bankacılık hizmetlerinin sağlanmasına ilişkin birçok yükümlülüğü taşımaktadır. Öyle ki, banka güvenli teknik ortamı sağlamalı, teknik ve güvenlikle ilgili güncel gelişmeleri takip etmeli, müşterisini bilgilendirmeli ve uyarmalı, elektronik bankacılık sisteminin kötüye kullanılmasını önleyecek tedbirler almalıdır. Söz konusu edimlerin ifasında gereken özenin gösterilmemiş olması durumunda bankanın sözleşmeye aykırı davranışı gündeme gelir. Zira görülen işteki nitelik eksikliği, borçlanılan edimden sapma özen eksikliği olarak ortaya çıkar[308]. Başka bir deyişle, özenin temelinde yatan şey, bankanın taahhüt ettiği işin gereği gibi sonuçlanması için belirli bir çaba sarf etmesi gereğidir[309].

2. Özen Yükümlülüğünün İhlâli Hâlleri

a. Sistem Güvenliğinin Sağlanmaması

Modern zamanda bankacılık faaliyetlerinin yürütülmesini elektronik makinelerin kullanımı olmadan düşünmek neredeyse imkânsızdır. Ancak elektronik makinelere güven bünyesinde bazı gizli riskleri de taşımaktadır. Vurgulanmalıdır ki, yalnızca mekanik (meselâ, 19. yüzyılda sigara üretiminde kullanılanlar gibi) makineler ve yazılımlara dayanan modern makineler (meselâ, ATM gibi) arasında önemli, ancak ihmal edilmiş farklılıklar vardır[310]. Yazılımlarda, yaklaşık, her 1000 kod satırı başına 5 kusur mevcuttur; makinelerin çalışmasında kullanılan yazılımların kod satırlarının milyonlarla ölçüldüğünü dikkate aldığımızda, ticari amaçla üretilmiş yazılımlarda binlerle tespit edilmemiş kusurların bulunduğunu tahmin etmek mümkündür[311]. Bu sebepledir ki, yazılım üreticileri yazılım güncellemelerini yapmak zorunluluğu hissetmektedirler. Söz konusu güncellemeler, isabetli bir şekilde, "güvenlik güncellemeleri" olarak tanımlanmaktadır, zira bazı kusurlar kötü niyetli kişiler tarafından dolandırıcılık amacıyla kullanılabilir[312].

---

308 **Başpınar**, s. 60 vd.
309 **Aral**, s. 112.
310 **Mason, S./Bohm, N.,** "Banking and Fraud", Computer Law and Security Review, The International Journal of Technology Law and Practice, Vol. 33, Iss. 2, April 2017, s. 237.
311 **Mason/Bohm**, s. 237.
312 **Mason/Bohm**, s. 237.

Görüldüğü gibi, elektronik bankacılıkta bankanın sorumluluğuna sebep olabilecek en önemli yükümlülük hiç şüphesiz, bankanın güvenli teknik ortamı sağlamasıyla ilgilidir. Zira elektronik bankacılık hizmetlerinin sağlanmasında kullanılan makinelerin yazılımlar sayesinde çalışmakta ve banka binası dâhilinde tüm makinelere entegre edilmiş daha büyük makine tarafından kontrol edilmektedirler. Söz konusu makinelerin de, çoğu zaman, internet bağlantısı bulunmaktadır. Bu durumda, yetkisiz kişiler, Internet üzerinden yazılımdaki kusurlardan yararlanmak suretiyle bankanın sistemini manipule etmek (meselâ, müşterinin sisteme dâhil olmadığı hâlde, dâhil olduğu veya sistemden çıkmadığı hâlde, çıkmış olduğu görüntüsü yaratmakla) imkânı elde etmektedirler[313]. Bu anlamda, banka, gerekli güvenlik altyapısını hazırlamakla mükelleftir[314].

Yargıtay bir kararında[315] bankanın elektronik bankacılık işlemlerinin güvenle yapılabilmesini sağlamasının bankanın asli borcu olarak nitelendirmiştir. Bu anlamda, elektronik bankacılık hizmetlerini sağlamak için bilgisayar sistemi kurmuş banka söz konusu sistemin güvenliği temin etmeli, yetkisiz kişilerin müdahelesini, virüs saldırılarını önlemelidir. Bu anlamda, bankanın aldığı güvenlik önlemlerinin yetersizliği bankanın özen eksikliği olarak değerlendirilebilir. Yargıtay 11. HD'nin 16.10.2017 tarihli kararına[316] konu olayda yerel mahkeme "... davalı bankanın ispat gücü açısından ıslak imzaya eşdeğer elektronik imza yerine hukuki ve teknik altyapısı olmayan bir şifre sistemi kullandığı, mevcut donanım, teknik eleman ve teknolojisiyle müşteriye göre çok daha avantajlı olması dolayısıyla bu tür profesyonel dolandırıcılıklarda önlem almada öncelikli durumda olduğu, somut olayda güvenlik tedbirindeki eksikliğinden dolayı objektif özen borcunu yerine getirmediği ..." gerekçesine dayanarak davalı banka aleyhinde hüküm tesis etmiş, karar Yargıtay 11. HD tarafından da onanmıştır.

---

313 **Mason/Bohm,** s. 238.

314 **Çeker, M.,** Hukukî Yönüyle Banka Mevduatı, Karahan Kitabevi, Ankara, 2004, s. 249.

315 ***Yarg. 11. HD.**, E. 2009/4017 K. 2010/10063 T. 11.10.2010* "... Ancak davalı bankanın olay tarihinde mevcut teknolojik imkânlar çerçevesinde, paranın ele geçirilmesini engellemek için gerekli güvenlik önlemlerini alması gerekmektedir. İnternet bankacılığı hizmeti sunan bankaların asli borcu, elektronik bankacılık işlemlerinin güvenle yapılabilmesini sağlamaktır. Birer güven kurumları olan bankalar, aldıkları mevduatları sahtecilere karşı özenle korumak zorundadırlar. Bu nedenle de hafif kusurlarından dahi sorumludurlar" *(Legalbank)*.

316 **Yarg. 11. HD**, T. 16.10.2017, E. 2016/7337, K. 2017/5353 (Legalbank)

Teknolojik gelişmelerin ve tehlikelerin devamlı inkişafı karşısında bu yükümlülüğün dinamik nitelik taşıdığı dikkate alınmalıdır. Başka bir deyişle, banka kendi güvenlik sistemini (bilgisayar yazılımlarını) değişen standartlara uygun hâle getirmek zorundadır, aksi durumda, bankanın özensiz davrandığı söylenebilir. BİSHY[317]'nin 11. maddesinin 3. fıkrası gereğince, bilgi sistemlerinin güvenilirliğinin sağlanması ve düzenli olarak güncellenerek gerekli değişikliklerin yapılması zorunludur.

Yine BBSEBHY'nin 5. maddesinin 1. fıkrası gereğince, "*banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir BS risk yönetim süreci tesis eder."* Anılan maddenin 5. fıkrası uyarınca, *"riskin kabul edilmesi için bilgi sistemlerinden sorumlu üst düzey yöneticinin onayının bulunması, riskin BS stratejisine ve mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine ilişkin onayının bulunması gerekir. Sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin eskiye nazaran artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı önceden kabul edilmiş olan riskler periyodik olarak gözden geçirilir"*.

Yargıtay bazı kararlarında[318] *"... davalı bankanın değinilen güvenlik önlemleri dışında başkaca yöntem ve teknikler varsa bunları zamanında kendi internet bankacılığı sistemine uyarlayıp uyarlamadığı*"nın araştırılması gerektiğini ifade etmiştir.

b. Sistemin Tasarlanması ve Organizasyonundaki Aksaklıklar

Elektronik bankacılık hizmetleri sağlayan banka öncelikle, sistemi gereği gibi çalışacak şekilde tasarlamak ve organize etmekle yükümlüdür. Banka sistemin tasarlanmasında ve organizasyonunda kapsamlı bir risk analizi yapmak suretiyle, teknik arızaya sebep olabilecek elektrik kesintisi, voltaj dalgalanması, yangın,

---

317 Bankaların İç Sistemleri Hakkında Yönetmelik (R.G., T.: 28 Haziran 2012, N 28337)

318 ***Yarg. 11. HD.**, E. 2005/13857 K. 2007/638 T. 22.01.2007; **Yarg. 11. HD.**, E. 2007/7474 K. 2009/2177 T. 26.02.2009 (Legalbank).*

rutubet, su baskını gibi dış etkenlere karşı elektronik bilgi işlem sisteminde koruma önlemlerinin almak zorundadır. Banka sistemini, olağandışı koşullarda da işlevini sürdürebilecek şekilde organize etmemiş ise, özensiz davranmış sayılır[319].

BİSHY[320]'nin 11. maddesinin 1. fıkrası gereğince, banka içinde tesis edilecek bilgi sistemlerinin yapısının bankanın ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması zorunludur. Sözügeçen maddenin 2. fıkrasında ise, bankanın bilgi sistemlerinin tesis edilmesi zamanı uyulması gereken asgari standartlar öngörülmüştür.

Doktrinde bankanın bilgi işlem sisteminin tasarlanması ve organizasyonu bakımından borçlandığı özenin ölçüsünün somut olayda bankanın kullandığı elektronik sisteme, büyüklük, etkinlik ve kullanım tarzı bakımından eşdeğer bir sistemdeki (son) teknolojik standartlar ve bankanın işletme organizasyonundaki masraf – risk dengesi dikkate alınarak belirlenmesi gerektiği ifade edilmiştir[321]. Buna göre, bankanın, gerçekleşme olasılığı düşük olan ve aşırı masraf gerektiren bir riske karşı, bilgi işlem sisteminin organizasyonunda önlem almamış olması, diğer bir ifadeyle, bankanın bu konuda teknik standartların varlığına rağmen bankanın riski göz ardı etmiş olması, başlı başına özensiz davranış teşkil etmez. Biz bu görüşe katılmak imkânı göremiyoruz. Şöyle ki, banka elektronik bankacılık işlemlerinin güvenli bir biçimde yapılabilmesi için gerekli teknik altyapıyı tesis etmek zorundadır. Aynı zamanda, bankanın gerekli teknik ortamı sağlaması onun internet bankacılık hizmetleri sunma riskinin bir gereğidir. Bu anlamda, banka, bir taraftan, sahip olduğu teknik, mali ve insan kaynakları sebebiyle riskleri müşterilere nazaran daha etkin kontrol etmek imkânını haizdir; diğer yandan, banka, tesis ettiği teknik altyapıya uygun elektronik bankacılık hizmetlerinin kapsamını belirlemede serbesttir. Nitekim BİSHY'nin 39. maddesinin 1. fıkrası da bu görüşü desteklemektedir. Anılan hükme göre, bankalar tarafından yeni sunulan ürün ve hizmetler dikkatli değerlendirmeye tabi tutulur. Bu ürün ve hizmetlerin sunulması için gerekli personel,

---

319 **Sonat, K. A.,** "Nakit Dışı Ödeme Usulleri Çerçevesinde Para Borcunun Banka Havalesi Yoluyla Ödenmesi", (Yayımlanmamış Doktora Tezi), Galatasaray Universitesi Sosyal Bilimler Enstitüsü, Şubat 2010, s. 276-277.

320 Bankaların İç Sistemleri Hakkında Yönetmelik (R.G., T.: 28 Haziran 2012, N 28337)

321 **Sonat**, s. 277.

teknoloji ve mali kaynakların bulunduğundan ve üst yönetim tarafından yeni ürün ve hizmetlerden kaynaklanacak risklerin tamamıyla anlaşıldığından emin olunur.

c. Bilgilendirme Sisteminde Aksaklıklar Yaşanması

BanK'nın 76. maddesinin 1. fıkrası uyarınca, "*Bankalar, müşterilerinin, verilen hizmetlerden kaynaklanan her türlü sorularına cevap verecek bir sistem kurmakla ve bu hizmetle ilgili bilgiyi müşterilerine bildirmekle yükümlüdürler*". Bu hükmün kapsamına, elektronik bankacılık hizmetlerinin de dâhil olduğunda tereddüt yoktur[322]. Nitekim BBSEBHY'nin 37. maddesinin 3. fıkrası bu konuda özel düzenlemeni öngörmektedir. Anılan hüküm gereğince, elektronik bankacılık hizmetlerinden dolayı müşterilerin yaşayabileceği sorunları ve şikâyetlerini iletebileceği ve takip edebileceği mekanizmalar oluşturur. Aynı zamanda, BBSEBHY'nin 37. maddesinin 2. fıkrasının (b) bendine göre, elektronik bankacılık hizmetlerinin kullanımının taşıdığı riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler konusunda banka müşterilerini kendi internet sitesinde veya internet bankacılığı hizmetini verdiği internet sitesinde bilgilendirir.

Görüldüğü üzere, müşterilerinin bilgilendirilmesinde yeterince özen göstermemiş banka bu davranışından dolayı sorumlu tutulabilecektir. Şöyle ki, müşterinin belirli bir zamana kadar yaptığı işlemlerden farklı ve olağan dışı bir işlemi bankanın uyarı sistemi tarafından fark edilmelidir. Bazı durumlarda, yapılan ödeme işlemi, müşteri açısından olağan görülebilir, ancak ödemenin yapıldığı kişinin de özellikleri dikkate alındığında yetkisiz işlemin önüne geçilebilir. Meselâ, mahalle bakkalının farklı kişilere belli miktarda ödemede bulunması makul görülebilir, ancak hurda araç satan bir şirkete yaptığı yüklü miktarda para havalesi, şüpheli bir işlem olarak değerlendirilmelidir[323].

Yargıtay 11. HD'nin 21.04.2011 tarihli kararına konu olayda yerel mahkeme "*... davalı banka tarafından müşterilerine alınacak ek güvenlik önlemleri konusunda bilgilendirme ve tavsiyelerde bulunulduğuna ilişkin herhangi bir delilin dosyaya*

[322] **Tekinalp'e** göre, anılan hüküm, bankaların hizmette müşterilerini tatmin edici modern sistem ve cihazlarla çalışmaları gerekliliğini emredici bir şekilde ifade etmekte, modern bir banka işletmesinin varlığını şart koşmaktadır. Bkz.: **Tekinalp**, s. 421.
[323] **Subramanian, R.**, Bank Fraud, Using Technology to Combat Losses, Wiley, 2014, s. 33.

sunulmadığı..." gerekçesine de dayanarak davalı banka aleyhinde hüküm tesis etmiş, karar Yargıtay 11. HD tarafından da onanmıştır[324].

Belirtmek gerekir ki, engelli müşterilere elektronik bankacılık hizmetleri sunan bankalar, aynı zamanda, BHEY'nin taleplerini dikkate almak zorundadırlar. Mesela, ATM üzerinden yapılan ödemeler hariç olmak üzere, kart ile yapılan çevrim içi ödemelerde; engel bilgisini bankaya iletmiş olan görme engelli müşteriler için, kart çıkaran kuruluş tarafından, ödenen tutar bilgisi, müşteriye ekran okuyucu program ile okunabilecek şekilde kısa mesaj üzerinden iletilir (BHEY, m. 9./f. 1).

d. ATM Güvenliğinin Sağlanmaması

Bilindiği üzere, alternetif dağıtım kanalları aracılığıyla, yani banka şubesine gitmeden bankacılık hizmetlerinden yararlanmaya imkân tanıyan elektronik sistemlerden ilki ATM'ler veya diğer yaygın ismiyle bankamatikler olmuştur. Kullanılmasına başlandığı ilk dönemde yalnızca para çekme işlemlerinin yapılması mümkün olan ATM'ler, zamanla teknolojik açıdan geliştirilerek çeşitli elektronik bankacılık işlemlerinin (hesaba para yatırma, havale, EFT, repo işlemleri vs.) gerçekleştirildiği "banka şubesi"ne çevrilmiştir. Ancak ATM'lerin yaygın kullanımı birçok hukukî problemi de beraberinde getirmiştir. Söz konusu hukukî sorunlar genellikle yetkisiz kişilerce ATM aracılığıyla müşterilere ait banka hesaplarına müdahele edilmesi (yetkisiz para çekilmesi, havale yapılması vs.) sonucunda ortaya çıkmaktadır. Bu anlamda ATM'lerin güvenliyinin (gerek fiziksel gerekse de teknik) sağlanması öne çıkmaktadır. Nitekim BBSEBHY'nin "ATM güvenliği" başlıklı 42. maddesi bu konuda detaylı düzenlemeyi getirmektedir. Şöyle ki, anılan madde gereğince banka, "*ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınır, uygulamaların ve uygulamalara ilişkin kritik servis ve verilerin bütünlüğü periyodik olarak doğrulanır. ATM'ler üzerine güvenlik açıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir.*

[324] **Karaman Coşgun, Ö.**, "Bankaların, Telekomunikasyon Şirketlerinin ve Mevduat Sahiplerinin İnternet Bankacılığından Doğan Sorumlulukları", Hukuk Biliminin Güncel sorunları, III. Uluslararası Kongre Bildiri Kitabı, C. 2 (Özel Hukuk), s. 179.

ATM'ler üzerinde çalışan işletim sisteminin gerekli olan en az yetki ve ayrıcalıklara sahip olarak çalışacak şekilde ayarlanmış, gerekli güncellemeleri ve yamaları yüklenerek sıkılaştırılmış, stabil ve günün teknolojisine göre güvenli bir işletim sistemi olması sağlanır. Banka, ATM'lerde, kaynağını ve bütünlüğünü onaylayamadığı uygulama ve kodların çalışmasını engelleyecek önlemleri alır." (f. 4). Aynı zamanda, "*ATM'lere yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasına imkân verecek bütün giriş noktaları erişime kapatılır ve ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ilave güvenlik tedbirleri uygulanır*." (f. 5) Diğer taraftan, BBSEBHY'nin 9. Maddesi gereğince, *"Banka, ATM cihazlarının bulunduğu yerlere müşterinin klavye hareketlerini göremeyecek uygun bir açıyla güvenlik kamerası yerleştirilir. Güvenlik kamerası kayıtları en az altı ay süreyle saklanır. Kamera kayıtlarındaki görüntünün delil niteliği teşkil etmesi ve görüntü kalitesinin ATM'deki müşterinin ve yakın çevresindekilerin eşkâllerinin belirlenmesini sağlayabilecek nitelikte olması esastır."*

Yargıtay bazı kararlarında[325] "*bankanın kötüniyetli üçüncü kişilerin ATM cihazlarına kolayca müdahelerini ve düzenek yerleştirmesini engelleyici tedbirleri almaması, kamera[326] vb. sistemler yerleştirmemesi ve yeterli denetim tedbirlerini almaması*"ndan hareketle bankanın sorumlu olduğuna karar vermiştir.

e. Servis Sürekliliğinde Aksaklıklar Yaşanması

Bilindiği üzere, internet bankacılığının en çok tercih edilme sebeplerinden birisi, kesintisiz ulaşılabilir olması, başka bir deyişle, zaman ve yer sınırlamasına tabi olmamasıdır. Bu anlamda, elektronik bankacılık hizmetleri sunan bankaların müşterilerin söz konusu işlemlere erişim hızını düşürecek aksaklıklara veya kesintilere karşı gerekli tedbir alması gerekmektedir. Servis sürekliliğinden amaç, müşterilerin dilediği an elektronik bankacılık işlemlerini yapabilmesi, herhangi bir

---

325 **Yarg. 13. HD**., T. 27.02.2009, E. 2008/12361, K. 2009/2549; **Yarg. 13. HD**., T. 30.05.2012, E. 2012/9055, K. 2012/13991; **Yarg. 13. HD**., T. 07.06.2012, E. 2012/9512, K. 2012/14945 (Legalbank).

326 BBSEBHY'nin 9. Maddesi gereğince, *"kameraların saatlerinin güncel, doğru olması ve ATM'de gerçekleştirilen işlem referans numarası, dekont numarası gibi parametrelerin zaman bilgisi ile uyumlu olması sağlanır. Kameranın herhangi bir sebeple görüntü kalitesinin düşmesi, görüntü alımının durması, lensinin dış bir etkenle kapatılması veya devre dışı kalması durumunu tespit edip gerekli aksiyonların alınmasını sağlayacak bir yapı kurulur."*

kesintinin yaşanmamasıdır[327]. Nitekim BBSEBHY'Nin 31. Maddesinin 1.fıkrasında bu konuda hükmü öngörmüştür. Anılan madde gereğince, *"Bankacılık faaliyetlerini yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetiminin ve planının bir parçası olan BS süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir BS süreklilik planı hazırlanır, BS süreklilik yönetimi süreci sorumlusu atanır ve BS Süreklilik Komitesi tesis edilir."* Bununla da banka, elektronik bankacılık servisi için beyan ettiği veya müşterilerine taahhüt ettiği düzeyde servis sürekliliğini sağlar. Servis kesintisinin doğurabileceği hukuki sorumlulukları en aza indirmek üzere banka gerekli önlemleri alır.

Servis sürekliliğinin sağlanmasının bazı istisnaları vardır. Şöyle ki, bankanın internet bankacılığı hizmetini etkin ve kesintisiz bir biçimde sunabilmesi için bazı durumlarda sistemin bakımına ve yazılım güncelleştirmelerinin yapılmasına ihtiyaç vardır; bu anlamda, banka daha iyi hizmet sunabilmek yahut sunduğu hizmetin kalitesini sürdürebilmek için, sistemini yenilerken, güncellerken veya bakımını yaparken geçici olarak hizmette bir kesinti yaşanabilir[328]. Ancak banka "*mücbir sebepler dışında müşterilerine önceden duyurmaksızın servis kesintilerine gidemez, internet bankacılığı servislerinde oluşacak kesintileri müşterilerine mümkün olduğunca önceden duyurur ve bu kesintilere ilişkin gerekçeleri de içerecek şekilde müşterilerini bilgilendirir*"[329].

Servis süreklilik ve kurtarma planları geliştirilirken servis dışı bırakma atakları da göz önünde bulundurulur, bunlara karşı gerekli önlemler alınır (BBSEBHY'nin, m. 28, b. fıkrası).

B. Zarar

1. Genel Olarak

Elektronik bankacılıkta özen yükümlülüğünün ihlâlinin bankanın sorumluluğuna sebep olması için müşterinin zarara uğraması şarttır. Geniş anlamda zarar kavramı, kişinin malvarlığında uğradığı (maddi) zararla birlikte şahıs varlığında

---

327 **Türk**, s. 323.
328 **Türk**, s. 323-324.
329 BBSEBHY'nin madde 37. ç. fıkrası gereğince, elektronik bankacılık hizmetlerinde iki saatten daha uzun süreli bir kesinti öngörülen planlı bakım ve değişikliklerde müşterilerin önceden banka tarafından bilgilendirilmelidir.

uğradığı zararı kapsamaktadır. Dar anlamda ise yalnızca maddi zarar dikkate alınır[330]. Maddî zarar, bir kimsenin malvarlığında rızası dışında meydana gelen azalmayı ifade eder. Bu azalma, malvarlığının aktifinin azalması veya pasifinin artması şeklinde ortaya çıkabileceği gibi, yoksun kalınan kazançtan da oluşabilir[331]. Manevî zarar, kişilik haklarına tecavüz edilmiş bir kimsenin duyduğu cismanî ve manevî acı ve ızdırabı, elemi ve böylece yaşama zevkinde bir azalmayı ifade eder[332].

Bankanın özen yükümlülüğünün ihlâli durumunda müşterinin maddi ve manevî zarara uğraması mümkündür. Meselâ, elektronik bankacılık hizmetleri sırasında hisse senedi işlemleri önemli paya sahiptir. Öyle ki, 2019 yılının haziran ayında yapılan hisse senedi işlem hacmi 48 milyar TL teşkil etmiştir[333]. Hisse senedi alım-satım işlemlerinin elektronik ortamda yapılması durumunda müşteri için bankanın hizmet sürekliliğini sağlaması büyük önem arz etmektedir. Bankanın sisteminden kaynaklanan herhangi bir hata nedeniyle müşterinin, almış olduğu hisse senetlerini daha yüksek bir fiyattan satarak kar elde etmesi engellenebilir. Diğer bir ifadeyle, elektronik bankacılık hizmetlerine sürekli erişimi sağlamak borcu altında olan bankanın söz konusu edimin ifasında özensiz davranması müşterinin maddî zarara uğramasına sebep olabilir. Aynı durum, internet üzerinden yapılan döviz alım satım işlemleri açısından da geçerlidir.

Bazı durumlarda müşterinin bankaya karşı manevi tazminat talebinin doğması için şartlar oluşabilir. Mesela, ATM'den para çeken müşterinin elektrik marpması sonucu vefat etmesi veya bedensel zarara uğraması gibi. Burada bankanın koruma yükümlülüğünü özenle yerine getirmemesi söz konusudur.

2. Banka Hesabı Üzerinden Yapılan Usulsüz İşlemler Sebebiyle Ortaya Çıkan Zararın Kime Ait Olduğu Sorunu

Elektronik bankacılık hizmetlerine ilişkin Yargıtay uygulamasına baktığımızda davaların büyük çoğunluğunun yetkisiz kişiler tarafından banka hesaplarındaki para üzerinde işlem yapılmasıyla ilgili olduğu görülmektedir. Burada

---

330 **Eren**, Genel Hükümler, s. 521.
331 **Oğuzman/Öz**, C. I, 390 vd.
332 **Oğuzman/Öz**, C. I, 391 vd.
333 **TBB**, Dijital, Internet ve Mobil Bankacılık İstatistikleri Haziran 2018, Rapor Kodu: DT22, Temmuz 2018, s. iii.

daha çok mevduat sahibinin hesabında kayıtlı bulunan paranın bir kısmı veya tamamının, hesap sahibinin rızası dışında başka hesaplara aktarılması, ATM'den yetkisiz kişiler tarafından para çekilmesi olayları söz konusudur. Bu hâlde, yetkisiz kişiler tarafından yapılan havale, ATM'den para çekme veya benzeri elektronik bankacılık işlemleri sonucunda ortaya çıkan zarara müşterinin mi yoksa bankanın mı katlanması gerektiği sorusu cevaplandırılmalıdır.

Bilindiği üzere, mevduat, gerçek veya tüzel kişiler tarafından, istenildiği anda veya belirli bir vade sonunda geri alınmak üzere bankaya yatırılan parayı ifade eder[334]. BanK, mevduatı "Yazılı ya da sözlü olarak veya herhangi bir şekilde halka duyurulmak suretiyle ivazsız veya bir ivaz karşılığında, istendiğinde ya da belli bir vadede geri ödenmek üzere kabul edilen para" olarak tanımlamaktadır (m. 3). Parayı bankaya yatıran kişi ("Mevduat Sahibi") ile "Banka" arasında mevduat sözleşmesinin bulunduğu kabul edilir[335]. Bu suretle mevduat sahibi, bankaya karşı hesabındaki para miktarı kadar alacaklı hâle gelmiş olur[336]. Bu anlamda, mevduat sahibinin hesabında bulunan para üzerinde herhangi mülkiyyet hakkı mevcut değildir; mevduat sahibi, hesabında kayıtlı para miktarında bankaya karşı bir alacak hakkına sahiptir. Kişiye tahsis edilmiş mevduat hesabı banka ile müşteri arasındaki alacak ilişkisinin içerik ve kapsamını belirlemeye hizmet eden bir araç niteliği taşımaktadır[337].

Görüldüğü gibi, mevduat sahibinin hesabında kayıtlı bulunan para miktarının bir kısmı veya tamamı üzerinde yetkisiz kişilerce tasarrufda bulunulması veya tahsil edilmesi sonucunda mevduat sahibinin bankaya karşı alacak hakkı mevcut olmaya devam etmekte, dolayısıyla, zarar bankanın malvarlığında meydana gelmektedir. Diğer bir ifadeyle, yetkisiz kişilerin, mesela, internet bankacılığı sistemini kullanarak

---

334 **Kaplan**, Banka Sözleşmeleri, s. 130; **Çeker**, Banka Mevduatı, s. 10 vd.; **Altaş, H.**, "*Mevduat Hesabından Yetkisiz Para Çekilmesinde Bankanın Hukuki Sorumluluğu*", ABD, 2001/3, s. 37 vd.

335 **Battal**, s. 34 vd.

336 **Yargıtay HGK**, T. 21.11.2012, E. 2012/11-550, K. 2012/820 (Legalbank); Doktrinde mevduatın üç tanım unsuru kabul görmüştür: *(1)* bir miktar paranın bu parayı kabule yetkili bir kuruma yatırılması; *(2)* paranın bankaya sınırsız sayıda gerçek ve/veya tüzel kişi tarafından yatırılmış bulunması, bu niteliği gereğince paranın kamusallaşması; *(3)* paranın hukuki bakımdan geri ödenecek olması. Bkz.: **Tekinalp,** s. 430 vd.

337 **Kaplan**, **İ.,** "*Banka Hesap Türleri, Hesap Sahibinin ve Hesap Türünün Tayininde Uygulanacak Kurallar*", AÜSBFD, C. 49, S. 1-2, s. 273-274.

tahsilat yaptıkları için ortaya bir zarar çıkacak olur ise, zarara uğrayan banka olacaktır[338].

C. Uygun İlliyet Bağı

Bankanın tazminat sorumluluğunun doğması için özen yükümlülüğünün ihlâli ve zararın varlığı yetmez; bu ikisi arasında uygun illiyet bağının kurulmuş olması gerekmektedir. Sözleşmenin ihlâli, olayların olağan akışına, genel hayat tecrübelerine göre somut olayda gerçekleşen türden bir zararı meydana getirmeye niteliği itibariyle elverişli olduğunda, sözleşme ihlâliyle zarar arasında uygun illiyet bağının varlığından bahsedilebilir[339].

Bankanın özen yükümlülüğüne aykırı davranışının, zararın olmazsa olmaz unsuru olduğu hususunu yani illiyet bağının varlığını ispat yükü genel kural (TMK m. 6) uyarınca müşteri üzerindedir[340].

D. Kusur

Bankanın özen yükümlülüğünün ihlâli sonucunda tazminatla sorumlu tutulabilmesi için, ihlâl oluşturan zarar verici davranışın kendi kusuruyla ortaya çıkmış olması veya bir üçüncü kişinin (ifa yardımcısı) bu sonuca yol açan davranışından yasa gereği sorumlu tutulmuş olması gerekmektedir. Nitekim TBK'nın 112. maddesi gereğince, "*Borçlu kendisine hiçbir kusurun yüklenemeyeceyiğini ispat etmedikce, alacaklının bundan doğan zararını gidermekle yükümlüdür*".

---

338 **Altaş,** s. 43; **Atamer**, Kredi Kartı, s. 1027; **Reisoğlu**, S., Bankacılık Kanunu Şerhi, C. 1, Gözden Geçirilmiş 2. bs., Yaklaşım Yayınları, Ankara, 2015, s. 1233; **Yarg. HGK**, T. 21.11.2012, E. 2012/11-550, K. 2012/820; **Yarg. 11 HD.**, T. 09.04.2009, E. 2007/9336, K. 2009/4347; **Yarg. 11 HD.**, T. 09.11.2009, E. 2008/7079, K. 2009/11540; **Yarg. 11 HD.**, T. 05.04.2010, E. 2008/12915, K. 2010/3753; **Yarg.11 HD.**, T. 14.10.2010, E. 2009/3988, K. 2010/10295; **Yarg.11 HD.,** T. 11.04.2011, E. 2009/11721, K. 2011/4153 (Legalbank); Aksi görüşde: **Gümüş**, Özen Borcu, s. 251. Yazar'a göre, bankanın yetkisiz kişiye yaptığı ödeme ile, müşteri için hiç bir zaman zararın doğmadığından bahsetmek doğru değildir. Zira hatalı ödeme, doğrudan müşterinin hesabına zimmet kaydedilerek bir malvarlığının azalması olarak yansıyacağı gibi; hesaptaki azalmanın hatalı ödenen bedel tutarı gibi doğrudan zararların dışında bir kısım dolaylı zararlara (mesela, müşterinin hesabının sergilediği görünüm sebebiyle yeni krediler bulamaması vs.) da yol açması mümkündür.

339 **Eren**, Genel Hükümler, s. 1059; **Akıncı**, Borçlar Hukuku, s. 152.

340 **Başpınar**, s. 210.

Elektronik bankacılık hizmetleri sağlayan banka davranışından dolayı kınanabiliyorsa kusurlu olduğundan söz edilir. Kınamanın sebebi, bankanın söz konusu durumda başka türlü davranmasının gerekli olması ve başka türlü davranma imkânını haiz olmasıdır[341]. Diğer bir ifadeyle, borca aykırı sonucu tasarlayarak ve arzu ederek veya bu sonucu göze alarak hareket eden bankanın bu davranışı kastî bir davranıştır. Borca aykırı sonuç, bankanın gerekli özeni göstermemesinden kaynaklandığı takdirde, bankanın ihmalinden söz edilir[342]. Ancak elektronik bankacılık açısından baktığımızda çoğunlukla bankanın zarar verici sonucu istemeksizin özen eksikliği nedeniyle söz konusu sonuca yol açtığını, yani bankanın ihmalinin söz konusu olduğunu söyleyebiliriz. İhmal zararlı sonucun doğmasını önlemek için hukuk düzeninin yüklemiş olduğu ödeve aykırı hareket etmek, gerekli önlemleri almamaktır[343]. Bu anlamda, durumun gerektirdiği özeni göstermeyen banka özen yükümlülüğünü ihlâl etmiş olur. Başka bir ifadeyle, bu durumda zarar verici sonucun meydana çıkmasının sebebi, bankanın gerekli özeni sarf etmemiş olmasıdır.

Burada cevaplandırılması gereken soru bankanın ihmalinin varlığına hükmetmek için "göstermesi gerekli özen"in hangi ölçütler esas alınarak belirleneceğine ilişkindir. Doktrinde ihmalin ölçüsünün objektif olduğu, başka bir deyişle, burada ihmalin "*orta seviyede, aklı başında (normal), makul bir kişinin, somut olayda durumun özellik ve gereklerine göre alması gerekli önlemlere, göstereceği özene, harcayacağı çabaya göre değerelendirileceği*" ifade edilmektedir[344]. TBK'nın 506. maddesinin 3. fıkrası da objektif özen ölçüsünü öngörnektedir. Ancak söz konusu hüküm, sarf edilmesi zorunlu olan özenin, bütün vekalet ilişkilerinde, bütün vekiller için genel bir ölçüyü ifade etmez. Burada daha çok, mesleki alana ya da mesleğe özgü özen ölçüsünün uygulanması gerekir[345].

Diğer yandan, TTK'nın 18. maddesinin 2. fıkrası uyarınca bankanın kusurunun belirlenmesinde basiretli tacir ölçüsünün de dikkate alınması gerekmektedir. Bu anlamda, bankanın davranışı elektronik bankacılık hizmetlerini

341 **Başpınar**, s. 211.
342 **Oğuzman/Öz**, C I, s. 405 vd.; **Akıncı**, Borçlar Hukuku, s. 153.
343 **Eren**, Genel Hükümler, s. 576.
344 **Eren**, Genel Hükümler, s. 577.
345 **Gümüş**, Özen Borcu, s. 324.

sağlayan ortalama bir bankanın yetenek ve niteliklerinin altındaki her özensiz davranışı onun kusurlu sayılmasına imkân tanıyacaktır.

§ 2. Bankanın Sorumluluğunun Hafiflemesi

I. Genel Olarak

Elektronik bankacılıkta müşteriler, bankacılık hizmetlerine uzaktan iletişim araçları vasıtasıyla, ulaşmakta, tabiri caizse, kendi kendilerine hizmet etmektedirler. Bunlar, farklı işlemler (mesela, kredi çekilmesi, ödemelerin yapılması, banka hesaplarını kontrol etme, kimlik bilgilerini değiştirme gibi) şeklinde karşımıza çıkmaktadır. Ancak elektronik bankacılık sözleşmesinin tarafı olarak bu tür hizmetlerden yararlanan müşterilerin belirli yükümlülükleri üstlenmeleri kaçınılmaz olmaktadır[346]. Zira klasik bankacılık hizmetlerinden farklı olarak elektronik bankacılık hizmetleri gerek banka gerekse müşteri açısından birçok riskleri beraberinde getirmektedir. Elektronik bankacılık hizmetlerinin güvenli bir ortamda sağlanmasının gerek banka gerekse müşteri için büyük önem arz ettiğinde şüphe yoktur. Bu anlamda, müşterilerin de söz konsuu güvenliğin sağlanması için gerekli tedbirleri almaları gerekmektedir. Mesela, müşterilerin kişisel verilerini özenle saklamak, banka kartının kaybı gibi kişisel verilerin haksız kullanımına sebebiyet verecek bir olayın gerçekleşmesi durumunda bankayı derhal haberdar etmek gibi yükümlülükleri bulunmaktadır. Belirtmek gerekir ki, bu yükümlülükler banka ve müşteri arasında kurulmuş sözleşmelerde de yer almaktadır. Bankalar sözkonusu yükümlülükleri sözleşmeye dâhil etmekle yetkisiz kişilerce yapılan işlemlerle ilgili sorumluluklarını hafifletmeyi veya tamamen ortadan kaldırmayı amaçlamaktadırlar[347]. Bu açıdan baktığımızda, elektronik bankacılık hizmetlerini

---

[346] Yargıtay HGK 2017/2224 E., 2018/1753 K. sayılı kararında "*Buna karşılık, hiç kuşkusuz, internet bankacılığı işlemlerinde müşteriler de kendilerinden beklenen her türlü tedbiri almak ve her türlü dikkat ve özeni göstermek zorundadırlar. Bu sebeple bilgisayarlarına başkalarının ulaşmasına imkân tanıyan her türlü gerçek ve sanal saldırıyı önleyici tedbirleri almaları ve bu konuda azami özeni göstermeleri gerekmektedir. Müşterilerin, internet bankacılığında kullanılmak üzere kendilerine verilen özel bilgilerini, banka ve kredi kartlarında olduğu gibi, üçüncü kişilerden özenle koruma ve saklama yükümlülüğü mevcuttur. Bu yükümlülüklerin ihlâl edilmesi hâlinde müşterinin kendi kusurundan kaynaklanan bu durumun sorumluluğuna kusuru oranında katlanması gerekmektedir*" denilmektedir.

[347] Mesela, Türkiye'de bankalardan birinin kullandığı "Bireysel Bankacılık Hizmetleri Sözleşmesi"nin genel işlem şartlarının 5.1.2. bendinde "Banka tarafından Müşteri'ye iletilen

kullanan müşterinin yükümlülükleri akdî niteliktedir. Elektronik bankacılık hizmetleri sözleşmesi çerçevesinde ortaya çıkacak zararlara hangi tarafın (banka yahut müşterinin) ve hangi oranda katlanacağı sözleşme taraflarının yükümlülükleri ve bu yükümlülüklerin ifasında gösterdikleri özenin derecesiyle doğrudan ilgilidir.

II. Müşterinin Yükümlülükleri

A. Kişisel Verileri Özenle Saklaması

Müşterinin özenle saklaması gereken kişisel veriler, kendisine tevdi edilen kart, kartın kullanılması bir kod numarası, şifre, kimliği belirleyici başka bir yöntemin kullanıldığı durumlarda, bunların yapılmasına imkân tanıyan bilgilerdir. Müşterinin özenle saklaması gerektiği kişisel verilerin dairesi, yetkisiz işlemlerin gerçekleştirilme usulüne bağlı olarak değişebilmektedir. Bazı durumlarda, mesela, ATM'den para çekme işleminde, ATM'nin kart ve şifreyi kullanarak işlemi başlatan kişinin yetkili kişi olup olmadığını kontrol etmesi mümkün olmadığından, kart ve şifrenin özenle muhafaza edilmesi büyük önem arz etmektedir[348]. İnternet bankacılığı işlemlerinde kartın fiziksel olarak yetkisiz kişide bulunması işlemin gerçekleştirilmesi için zorunlu olmadığından kartın özenle saklanıp saklanmadığı söz konusu olmayabilir; bu durumda, kredi kartı bilgilerinin (kartın üzerinde yazılı olan bilgilerin) muhafaza edilmesinde özenli davranıp davranılmadığı araştırılmalıdır.

Müşteriler kişisel verilerinin yetkisiz kişiler tarafından kullanılmasını önlemek amacıyla çeşitli tedbirler alabilirler. Mesela, kredi kartı bilgilerini banka yetkilisi dâhil, hiç kimseyle paylaşmamak; ATM'de işlem yaparken kredi kartı şifresinin üçüncü kişiler tarafından görülmesini engellemek; kredi kartı şifresinin, üçüncü kişiler tarafından ulaşılmasına imkân tanıyacak yerlerde not etmemek; kredi kartı ve kredi kartı şifresini aynı yerde (mesela, cüzdanında) muhafaza etmemek; bütün Spam'ları, banka veya diğer hesap bilgilerini talep eden e-postaları yanıtlamamak gibi. Ancak belirtmek gerekir ki, birçok sebepten dolayı kişisel

---

şifreler ve/veya parolalar ve diğer bilgiler in üçüncü kişilere karşı güvenliğinin sağlanması, bu noktada kendi uhdesinde virüs önleyici programlar dâhil her türlü güvenlik önlemlerinin alınması ve gereken dikkat ve özenin gösterilmesi Müşteri'nin sorumluluğundadır" denilmektedir.

348 **Arkan**, Elektronik Bankacılık, s. 17.

verilerin muhafaza edilmesi zorlaşmaktadır. Mesela, elektronik bankacılıkta kullanılan şifrelerin özel karakterlerden oluşturulması talebi karşısında müşterilerin sözkonusu şifreleri bir yere yazmak zorunda kaldıkları bir gerçektir[349]. Diğer yandan, farklı bankalarda birkaç tane banka hesabı bulunan müşterinin tüm şifreleri hafızasında tutması mümkün görünmemektedir. Bu sebepten dolayı müşterilerin farklı yöntemler (meselâ, elektronik bankacılıkta kullandıkları parolaları özel bir şekilde şifrelemeye tabi tutmak gibi) kullandıkları görülmektedir. Mesela, kredi kartı parolasını kâğıt üzerinde veya telefon defterinde numara olarak kaydetmek gibi. Bu anlamda, müşterinin kişisel verilerini muhafaza etmesi konusunda özenle davranması her olayın özelliğine uygun olarak belirlenmelidir. Mesela, Almanya'da Kassel Mahkemesi'nin 16 Kasım 1993 tarihli bir kararına konu olayda, kişi kredi kartı parolasını (PIN) telefon numarası olarak kâğıt üzerine not etmiş, ancak not ettiği kâğıdı kredi kartıyla beraber cüzdanında taşımıştır. Mahkeme kart hamilinin özensiz davrandığı (yetkisiz kullanımda ağır ihmalinin olduğu) yönünde karar vermiştir[350]. Buna mukabil, Hollanda'da kredi kartı şifresini telefon numaraları da kayıtlı olan telefon defterine kaydetmiş müşterinin bu davranışı özensiz olarak nitelendirilmemiştir[351].

Şöyle bir soru akla gelebilir: son dönemde insanlar şifrelerini cep telefonlarına yazıp şifreliyorlar. İnsanların böyle bir davranış sergilemesi, özensizlik olarak nitelendirilebilirmi? Bizce, sorunun cevabı olayın özelliği dikkate alınarak belirlenmelidir. Meselâ, kişi, kredi kartı şifresini cep telefonunun özel bir parola ile korunan bölümüne yazmışsa, gereken özeni gösterdiği sonucuna varabiliriz. Buna

---

349 Yapılan bir araştırmanın sonuçlarına göre, çoğu kullanıcı, çoklu şifreleri (multiple passwords), yani farklı uygulamalar için kullandıkları farklı şifreleri ve/veya şifre kullanma tarihinin bitmesi sebebiyle sık sık değiştirdikleri şifreleri hafızalarında tutmak zorundadırlar. Çok sayıda şifre, kişilerin hafıza yeteneğini olumsuz etkilemekte ve güvensiz çalışma pratiklerinin doğmasına imkân tanımaktadır. Mesela, anket katılımcılarının %50'si şifreleri kâğıt üzerine not etmişlerdi (Bu konuda bkz.: **Adams, A./Sasse M.A.**, "Users Are Not The Enemy", Communications of the ACM, December 1999, Vol. 42, No. 12, s. 42).

350 **Steennot**, **R.,** "Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping", Financial Law Institute, Working Paper Series, July, 2010, s. 5; Müşterinin kartını ve PIN bilgisini özenle saklaması ve özenin yerine getirilmesinde gerekli tedbirleri alması Alman Medeni Kanunu ve mahmeke içtihatı gereğince müşterinin bu alanda özel yükümlülüklerinden biri olarak nitelendirilmiştir. Bkz. German Civil Code, Bürgerliches Gesetzbuch (BGB), Volume I, Books 1-3: Paragraph 1-1296, Article-by-Article Commentary, edited by Gerhard Danneman Reiner Schulze, Nomos, 2020, s.1324.

351 **Steennot**, Allocating liability, s. 5.

mukabil, kişi kredi kartı şifresini telefon rehberine banka şifresi ismiyle kaydetmişse, gereken özeni gösterdiği söyelenemez.

Bundan başka, internet bankacılığı hizmetini kullanan hesap sahibinin üçüncü kişilerin bu alanda işlem yapmasına izin vermemesi, yetkisiz kişilerin bu alana dâhil olması ile sonuçlanabilecek davranışda bulunmaması gerekir. Meselâ, iş yerinde internet bankacılık işlemini yapan hesap sahibinin işlem alanından çıkış yapmasını unutması gibi. Yargıtay 2008 tarihli bir kararında[352] "*davalı bankanın uluslararası standartlarda bilgilerin gizliliğinin sağlanması, korunması ve müşteri kişisel bilgilerinin doğruluğunu doğrulaması aşamalarında uygulanan teknikleri internet bankacılığı sisteminde uyguladığı, sisteminde yeterli güvenlik tedbirlerini aldığı, davacının kimsenin bilmemesi gereken ve korumakla yükümlü olduğu şifresi gibi kişisel bilgilerini koruyamaması ve bunun sonucu olarak da, kişisel bilgilerin kötüniyetli 3.kişilerce elde edilmesi sonucu davaya konu havale işleminin gerçekleştiği*" gerekcesiyle ortaya çıkan zarardan müşterinin sorumlu olduğuna karar vermiştir. Yargıtay 2016 tarihli bir kararında[353] "*...davacının kart bilgilerini ve şifreleri karşı tarafa kendisi bildirdiğinden ve bu bilgilere göre işlem yapıldığı anlaşıldığından, bankanın zarardan sorumlu olduğu kabul edilemez*" gerekçesi ile aşağı mahkemenin kararını bozmuştur.

Belirtmek gerekir ki, üçüncü kişilerin de kullandığı mekanlarda kartın bırakılması kartın yetkisiz kişilerce kullanılmak rizikosunu önemli surette artırması itibariyle müşterinin sorumluluğuna yol açar[354]. Mesela, Brüksel Mahkemesi muayene sırasında kredi kartını hastane odasında bırakmış yaşlı kadının davranışını özensiz (ağır ihmal) olarak nitelendirmiştir. Mahkeme yaşlı kadının hastaneye yatırılma ile ilgili stres altında olma delilini dikkate almamış, zira yaşlı kadın parasını (kredi kartını değil!) emniyet kutusunda saklamayı düşünecek kadar aklı başında olmuştur[355]. Mahkeme 27 Kasım 2006 tarihli diğer bir kararında sabah kahvaltısı

---

352 Yarg. 19 HD., E. 2007/7397, K. 2008/3029, T, 27.03.2008.

353 Yarg. 19HD., E. 2016/446, K. 2016/6786, K. 19.04.2016. Karardan, davacının telefonla aranması sonucunda kart bilgilerini ve bunun sonucunda cep telefonuna gelen şifrelerini de yetkisiz kişilere bildirdiği anlaşılmaktadır.

354 **Atamer**, Kredit kartı, s. 1003.

355 **Steennot**, Allocating liability, s. 5; Almanya'da Bonn Mahkemesinin 2000 tarihli ("Hastane davası" olarak bilinen) bir kararına konu olan benzer bir olayda, kart ve şifresini hastane odasında sağlam kapalı kutuda saklamasına rağmen müşterinin ağır ihmalinin varlığı sonucuna ulaşmıştır.

yaptığı sırada banka kartını otel odasında bırakmış kişinin özensiz davrandığı sonucuna varmıştır; çünkü bu durumda kart sahibi odaya ulaşmaları ihtimal dâhilinde olan banka çalışanlarının kendisinin kart bilgilerine erişmelerine olanak sağlamıştır[356].

Yargıtay 12 Haziran 2014 tarihli bir kararında, minibüste seyahet hâlinde iken kartını çaldıran davacının kusurunun bulunmadığı sonucuna varmıştır. Mahkeme'ye göre; "*...hayatın olağan akaşına göre davacının minibüste seyahet hâlinde cüzdanını sürekli açarak kredi kartını kontrol etmesi mümkün değildir*."[357]

B. Kullandığı Elektronik Cihazların (Bilgsiyar, Mobil Telefon ve diğerleri) Sistem Güvenliğini Sağlama Yükümlülüğü

Belirtmek gerekir ki, bankaların bilgisayar sisteminin mükemmel olması itimalinde dahi müşterilerin internet bankacılığı hizmetlerinden yararlanmak için kullandıkları bilgisayarların belirli düzeyde güvenlik taleplerine cevap vermesi gerekmektedir. Söz konusu bilgisayarların bir bölümünün müşterilerin aile bireyleri tarafından farklı amaçlar doğrultusunda kullanılan ev bilgisayarı olması dikkate alındığında anılan yükümlülüğün önemi daha da artmaktadır. Uygulamada bankalar internet bankacılık hizmetlerinden yararlanmak isteyen müşterilerin kendilerinin gerekli donanım ve yazılım programının (firewall, anti virüs programları, internet koruma programları gibi) bulunmasnı talep etmektedir[358]. Sözkonusu denetimin uygulanabilmesi için ilave donanım ve yazılım yapılanmasına ihtiyaç olduğu açıktır.

Bkz.: **Haybäck**, **G.,** "Civil law liability for unauthorized withdrawals at ATMs in Germany", Digital Evidence & Elec. Signature Law Rev., 57, (2009), s. 60.

356 **Steennot**, Allocating liability, s. 6.

357 **Yarg. 13. HD.**, E. 2013/32840, K. 2014/18798; T. 12.06.2014.

358 Mesela, Türkiye'de bankalardan birinin kullandığı "Bireysel Müşteri Sözleşmesi"nin genel işlem şartlarının 6.1.1. bendinde "*Müşteri'nin söz konusu hizmetlerden azami ölçüde güvenle yararlanabilmesi için kendisinin gerekli donanım ve yazılım programının (firewall, anti virüs programları, internet koruma programları vb. gibi asgari güncel programların) bulunması, sahte, izinsiz kişisel bilgi saklayan veya güvenli olmayan ("https" formatında bağlantı sağlamayan ve/veya asgari 128 bit SSL güvenlik düzeyinde bulunmayan) internet siteleri ve kamuya açık alanlarda yer alan bilgisayar ve bağlantı noktaları (internet kafelerdeki bilgisayarlar ve güvenli olmayan kablosuz erişim ağları) üzerinden bu tür hizmetleri temin etmemesi gerekmektedir*" denilmektedir.

Ancak müşterilerin, özellikle de tüketicilerin ileri seviyede güvenlik tedbirleri alma konusunda yeterince bilgi sahibi olduğu söylenemez. Bu anlamda, güvenlik açısından müşterinin bilgisayarında orta düzeyde bir bilgisayar kullanıcısının kullanabileceği nitelikte bir lisanlı antivirüs programı bulunması gerekir[359]. Aksi takdirde, müşterilerin çok az kısmının bankanın talep ettiği seviyede güvenlik önlemi aldığı söylenebilir. Bu durum müşterilerin yetkisiz kişilerce yapılmış işlemlerden dolayı sorumlu tutulmasıyla sonuçlanırdı. Alman Yüksek Mahkemesi "Dialer" kararında, ortalama bir internet kullanıcısının bilgisayarında "dialer"i engelleyici yazılımları bulundurmak zorunda olmadığı ve bu kontrolün ondan beklenemeyeceği sonucuna ulaşmıştır[360].

Yargıtay 21.04.2011 tarihli bira kararında, bilgisayarına gerekli anti-virüs programını yüklememiş olması sebebiyle mevduat sahibine kusur yüklenemeyeceğini hükme bağlamıştır[361].

Görüldüğü üzere, müşteri internet bankacılığı hizmetlerini kullanırken kendi risk alanından doğan bazı tehlikere karşı belirli önlemleri almak zorundadır. Bu anlamda, sözkonusu hizmetlere erişebilmek için kullandığı bilgisayarında anti-virüs programı bulundurmayan veya lisanslı program kullanmayan veya lisans süresinin dolduğuna dair uyarıya rağmen programı yenilemeyen müşterinin bu davranışıyla aslında usulsüz işlemler sonucunda doğan zararlara kendisinin katklanacağının bilincinde olması gerekir.

Vurgulamak gerekir ki, müşterinin bilgisiyarına bulaşmış olan kötü amaçlı yazılımların hepsi, onun kişisel bilgilerinin çalınmasına imkân tanıyacak fonksiyonu haiz değildir. Meselâ, müşteri kendi bilgisayarına bedava program yüklemiş, ancak bu işlemi gerçekleştirirken de reklam yapma amaçlı "spyware" programının da

---

359 **Türk**, s. 326.

360 **Memiş**, s. 884; Slovakya Mahkemesi 2011 tarihli bir kararında "...orta düzeyde bir bilgisayar kullanıcısı olan tipik banka müşterisinin sahte banka internet sitesi oluşturabilecek virüsü farketme veya bankanın çalışma prosedürünün ayrıntılarını bilme konusunda uzman olamayacağı" gerekçesiyle bankayı sorumlu tutmuştur. Bkz.: **Rowan Legal**, "*Commentary: Slovak case law on the responsibility of a bank for unauthorised financial transactions*", Digital Evidence & Elec. Signature Law Rev., 12 (2015), s. 101-102.

361 **Yarg. 11. HD.**, E. 2009/11411, K. 2011/4781, T. 21.04.2011 (**Coşgun**, s. 194).

bilgisayarına yerleşmesine olanak tanımış olabilir[362]. Böyle bir davranış müşteri açısından kusur olarak nitelendirilemez.

Yapılan araştırmalar kullanıcıların saldırıya maruz kaldığından ve kişisel bilgilerinin çalındığından haberdar olmadığını ortaya koymaktadır. Bu nedenle mobil güvenlik ve mobil güvenlik risklerine karşı alınabilecek tedbirler konusunda kullanıcıların farkındalığının artırılması gerekmektedir. Yalnız kullanıcıların farkındalık düzeyinin artırılması ile mobil cihazlara yönelik güvenlik risklerine karşı mücadele edilebilir[363].

Kötü amaçlı mobil yazılımlar, özellikle de Trojan virusu işlem doğrulama kodunu içeren SMS mesajını ele geçirmek amacıyla tasarlanmıştır. Bu yöntemde, kötü niyetli kişiler kullanıcıların akıllı telefonlarına yüklemesini istedikleri uygulamalarda zararlı yazılımlar bulundurmaktadır. Uygulama yüklendikten sonra kötü niyetli kişiler kullanıcının cep telefonunu görüntüleyerek bankadan gelen SMS'lere erişmektedirler. Meselâ, ZITMO (Zeus In The Mobile) bu amaçla oluşturulmuş ilk kötü yazılımlardan biri tanesidir. ZITMO'nun sahip olduğu özelliklerden biri, SMS mesajını silme kabiliyetidir. Bu durumda, kullanıcı cep telefonuna SMS mesajının geldiğinden bile haberdar olmayabilir[364].

Yapılan araştırmalara gereğince, Google Play'de 200'ün üzerinde mobil cihazlar güvenli kullanımı için uygulamaların bulunmasına rağmen, bunlarda hiçbirisinin kullanıcılar tarafından ilgisini tam çekmediği tespit edilmiştir. Akıllı telefon kullanıcıları kişisel bilgisayarlara uyguladıkları antivirüs deneyimlerini akıllı telefonlara aktarmakta başarılı olamamış gibi görünmektedir. Bunun temel sebebi, mobil güvenlik riskleri konusunda kullanıcıların yeterli bilgiye sahip olmamasıdır.[365]

---

[362] **Özdilek, A. O.,** Ankara Barosu Uluslararası Hukuk Kurultayı 2008, 8 Ocak-11 Ocak 2008, C. 2, Ankara Barosu Yayınları, 2009, s. 95.

[363] **Sağıroğlu/Alkan,** s. 317; *Google Play*'de yaklaşık olarak 3,5 milyon uygulama bulunmaktadır. Bunların %13'lük kısmının düşük kaliteli olduğu ve yüksek güvenlik riski taşıdığı söylenmektedir. Cambridge Üniversitesi'nin 2015'de yapmış olduğu bir araştırma, Android akıllı telefonlarının %87'sinin bilgisayar korsanları tarafından istismar edilebilecek en az bir savunmasız noktaya sahip olduğunu ortaya koymuştur. Zimperium laboratuvarının araştırması Android cihazların %95'inin SMS vasıtasıyla en az bir kez saldırıya maruz kaldığını göstermektedir. Bkz. **Sağıroğlu/Alkan,** s. 317.

[364] **Mulliner/Borgaonkar/Stewin,** s. 152.

[365] **Sağıroğlu/Alkan,** s. 317-318.

Mobil cihazlarda kullanıcılar tarafında kötücül yazılımlardan korunmak için alınabilecek önlemlere ilk önce güvenlik yazılımını kurmak, daha sonra güvenli olmayan kaynaklardan veya marketlerden uygulamanın indirilmemesi ve son temel taleb mobil cihazda işletim sisteminin güncel tutulmasıdır[366].

C. Kişisel Bilgilerinin Çalınması/Kaybolması Durumunda Bildirimde Bulunma

Banka veya kredi kartı hamillerinin kartlarını ve bunlara ait şifreleri güvenli bir şekilde muhafaza etmesi ve üçüncü kişilerce kullanılmasına mani olacak önlemleri alması zorunludur. Müşterinin kartı, aldığı tüm önlemlere rağmen kaybolmuş veya çalınmışsa, bu durum, derhal kartı çıkaran kuruluşa bildirilmelidir. Müşterinin, kartının kaybolduğu veya çalındığı hâllerde, bildirimde bulunulması gereken yerlerin telefon numaralarını önceden öğrenmesi ve her zaman ulaşılabilecek bir yere not etmesi büyük önem taşımaktadır. Kartın çalındığı veya kaybedildiği fark edildiği an, hiç vakit kaybedilmeden kartı kullanıma kapatılmalıdır.

III. Müşterinin Özensiz Davranışının Bankanın Sorumluluğu Üzerinde Etkisi

A. Müşterinin Ortak Kusuru

1. Genel Olarak

Türk Borçlar Kanunu'nun 52. maddesinin 2. fıkrasında zarar görenin zarara etkisi (kusuru) tazminatta indirim veya tamamen kaldırılma sebebi olarak düzenlenmiştir. Bu hüküm uyarınca zarar gören, zararın doğmasında ya da artmasında etkili olmuşsa yahut tazminat yükümlüsünün durumunu ağırlaştırmışsa hâkim tazminatta indirime gidebileceği gibi tazminata hükmetmeme yetkisine de sahiptir. Hâkim somut olayın özelliklerine göre haklı gerekçelerle değerlendirerek tazminatın indirilmesine veya tamamen ortadan kaldırılmasına karar verme yetkisine sahiptir[367].

---

[366] **Sağıroğlu/Alkan,** , s. 335.

[367] Yarg. 3. HD, E. 2002/4330, K. 2002/4834, T. 06.05.2002 kararında *"Ortak kusurun varlığı hâlinde hâkim bunun tazminata etkisini, başka bir anlatımla bir tenkis sebebi mi yoksa zarar*

Zarar görenin kusurlu davranışıyla katkıda bulunduğu zarar bakımından sorumluluğu paylaşması, TMK'nın 2. maddesinin 1. fıkrasında öngörülmüş dürüstlük kuralının bir gereğidir[368]. Sorumluluk hukunda ise, dürüstlük kuralının özel bir görünümü, TBK'nın 52. maddesinin 1. fıkrasında yer alan düzenlemedir. Dayanağını yine dürüstlük kuralında bulan çelişkili davranış yasağı (*venire contra proprium factum*) zarar görenin kusuruna sonuç bağlanmasını şartlandırır. Zira kişinin ortaya çıkmasını engelleyebileceği zararların tazminini istemesi çelişkili davranış sayılır[369].

Görüldüğü üzere, makul bir insandan beklenen davranışı göstermeyerek zararın meydana gelmesinde veya artmasında etkili olmuşsa, zarar görenin ortak kusurundan söz edilir. Zarar görenin kusurunun hukukî niteliği konusunda baskın görüş[370] zarar görene zararın doğumuna ve artmasına katkıda bulunan davranışta bulunmama yönünde bir külfet yüklendiği yönündedir. Külfet, kendisine yüklenen bazı davranış ödevlerini yerine getirmeyen kişinin haklarını tamamen veya kısmen kaybetmesi, kendi yararına bir hukuki durumu elde edememesi olarak tanımlanmaktadır[371]. Zarar gören zararın doğmasına veya artmasına katkıda bulunursa, kendisine zarar veren kişiye karşı sahip olduğu hakları tamamen veya kısmen kaybeder. Zarar görene bu anlamda bir yükümlülük yüklenemez. Ondan böyle bir davranışının ifası talep ve dava edilemez. Aksine davranışta tazminat

---

ziyan hükmünden sarfınazar edilebilecek bir hâl mi olduğunu takdir edecektir. Ancak bu yolda takdir hakkı kullanılırken hak ve adalete uygun bir sonuca götürecek yol izlenmelidir. Zarar gören kendi davranışı ile zarara neden olmuş ise bu zarar başkasına yüklenmemeli payı ayrılmak suretiyle zarar verenin sorumlu olacağı miktar tespit edilmelidir. Böylece bu hükmün konuluş nedeni gözönünde tutulduğunda, amacın ortak kusura isabet eden payının indirilmesi olduğu zarardan tamamen vazgeçilmesinin ise istisnai bir durumda sözkonusu olacağı kabul edilmelidir" denilmektedir. (Yargıtay kararı veya kanundan yaptığın alıntıları kopyalayıp yapıştırırsan daha iyi olur. Çünkü alıntı yaptığın metin hatalı bile olsa değiştiremezsin. Aynen almak zorundasın. Kendin yazarsan farkında olmadan değişik yazabilirsin. Yukarıda düzelttiğim iki kelimeyi kontrol et, kararda nasıl geçiyorsa öyle yaz.)

368 **Baysal**, s. 29; Tandoğan'a göre, kendi kusuruyla sebebiyet verdiği zararın tazminini istemek hüsnüniyet kaidelerine aykırı olurdu. Bkz.: **Tandoğan**, Mesuliyet Hukuku, s. 319; Yarg. HGK, E. 1984/4767, K. 1986/437, T. 18.04.1986 kararında "Türk pozitif hukukunda Borçlar Kanununun 44/1. maddesinin (hiç bir kimse kendi kusurundan yararlanamaz) ilkesine dayandığı kabul edilmektedir. Bu ilke hak ve adalet düşüncesine de (M.K. md. 2) uygun düşmektedir" ibaresine yer vermekle bu görüşü benimsemiştir.

369 **Baysal**, s. 29.

370 **Kocayusufpaşaoğlu**, s. 33; **Nomer**, Maddi Tazminat, s. 85; **Baysal**, s. 30.

371 **Kocayusufpaşaoğlu**, s. 33; **Eren**, Genel Hükümler, s. 45.

talebinde bulunulamaz. Külfete uymayan zarar gören bu davranışının sonuçlarına katlanır[372].

2. "Zarar Görenin Ortak Kusuru" Kavramının Üçüncü Kişilerce Yapılan Hukuka Aykırı Elektronik Bankacılık İşlemleri Açısından Kullanılabilirliği Sorunu

Yetkisiz kişiler tarafından yapılan elektronik bankacılık işlemleri açısından "müşterinin ortak kusuru" kavramının kullanılmasının isabetli olup-olmadığı zararın müşterinin mi, yoksa bankanın mı malvarlığında doğduğu ile ilgilidir. Zira zararın bankanın malvarlığında meydana geldiği görüşünün kabulü durumunda müşterinin ortak kusurundan bahsedilmesi mümkün görünmemektedir. Buna karşılık, zararın müşterinin malvarlığında doğduğu fikrinin kabulü durumunda, müşterinin ortak kusurunun dikkate alınacağı söylenebilmektedir. Bu açıdan baktığımızda, yetkisiz kişiler tarafından müşterinin kredi kartından para çekilmesi veya internet bankacılığı üzerinden havale yapılması gibi durumlarda ortaya çıkan zararın banka yahut müşterinin malvarlığında doğduğunun belirlenmesi önem arz etmektedir. Doktrinde hâkim görüş[373] ve Yargıtay uygulaması[374] bu gibi durumlarda zararın bankanın malvarlığında ortaya çıktığı yolundadır. Buna mukabil, doktrinde savunulan diğer bir görüş uyarınca[375], kişisel bilgilerin kullanıcının kusuru ile üçüncü kişinin eline geçip geçmediği dikkate alınarak bir ayrım yapılmalıdır. Şöyle ki, kişisel bilgilerin üçüncü kişilerin eline geçmesinde kullanıcının bir kusuru yoksa doktrinde hâkim olan görüşe katılmak gerekir. Ancak kullanıcının kusurunun varlığı durumunda, kimlik doğrulama verilerini müşteriden ele geçiren dolandırıcı, sahte değil, doğru ve gerçek bilgileri girmekte ve bankanın sistemi tarafından müşteri (veya yetkili temsilci) gibi algılanmaktadır; bu anlamda, rizikonun yine de bankaya ait olduğu ve zararın onun

---

372 **Tandoğan**, Mesuliyet Hukuku, s. 319.

373 **Reisoğlu**, C. 2, s. 1267; **Kaplan**, Sorumluluk, s. 452; **Atamer**, Kredi Kartı, s. 1026; **Altaş**, s. 41; **Akkanat**, s. 58 vd; **Eralp**, s. 257-258; **Mason/Bohm**, s. 240, dn. 8.

374 **Yarg. 11. HD.**, E. 2009/4017, K. 2010/10063; T. 11.10.2010; **Yarg. 11. HD**., E. 2009/12767, K. 2011/5607, T. 09.05.2011; **Yarg. 11. HD.,** E. 2008/7079, K. 2009/11540, T. 09.11.2009; **Yarg. 11. HD.,** E. 2009/9420, K. 2011/2538, T. 10.03.2011; **Yarg. 11. HD.,** E. 2009/8125, K. 2011/1159, T. 03.02.2011.

375 **Tandoğan**, Bankacılık, s. 116; **Gümüş**, Özen Borcu, s. 251-252; **Kaneti, S.,** "Elektronik Banka İşlemlerinin Hukuksal Yapısı", Makalaler, On İki Levha Yayıncılık, İstanbul, 2011, s. 609; İşgüzar, s. 123-124; **İnal**, s. 368-369.

malvarlığında gerçekleştiği söylenemez[376]. Diğer bir deyişle, müşteri sistemin kendi tarafındaki ucunu korumakla mükelleftir, söz konusu ödeve kusurlu aykırılığın sonuçlarına müşteri katlanmalıdır[377].

Yargıtay uygulamasına baktığımızda, Yüksek Mahkeme'nin bazı kararlarında "müşterinin ortak kusuru" kavramına yer verdiğini görüyoruz. Şöyle ki, Yargıtay bazı kararlarında, "*davacının güvenliği sağlayıcı tedbirler almadığı*"[378], "*davacının kimsenin bilmemesi gereken ve korumakla yükümlü olduğu şifresi gibi kişisel bilgilerini koruyamadığı*"[379], "*davacının kart bilgilerini ve şifrelerini karşı tarafa kendisinin bildirdiği*"[380], "*kartın cihaza sıkışmasından sonra arka sırada bekleyen tanımadığı bir kişiden yardım isteyen davacının anılan kötü niyetli kişinin talimatı üzerine şifresini iki defa girdiği*"[381] gerekçesiyle yetkisiz kişiler tarafından yapılan işlemler sebebiyle meydana çıkan zararlardan müşterinin ortak kusuru oranında sorumlu olduğu sonucuna ulaşmıştır.

3. Bankanın Kusurunun Müşterinin Özensiz Davranışının Sonuçları Üzerindeki Etkisi

Yukarıda da belirtildiği üzere, yetkisiz kişiler tarafından yapılan işlemler sonucunda meydana gelen zararlar bankaya aittir. Bazı durumlarda, müşteri özensiz davranır, ancak bankanın kusuru, müşterinin özensiz davranışı ile ortaya çıkan zarar arasındaki illiyet bağını keser. Çünkü bankanın kusurlu davranışı, yoğunluğu itibariyle zararlı sonucun uygun sebebi hâline gelmiş ve zarar verenin davranışını arka plana atmıştır[382]. Böyle bir durumda, davranış ile zarar arasında uygun illiyet bağı kesildiği için müşteri sorumluluktan kurtulur. Yargıtay'ın da bu yönde kararları vardır. Mesela, Yüksek Mahkemenin, 22 Haziran 2006 tarihli kararına[383] konu olan olayda, müşteri kişisel bilgisiyarının güvenliğini sağlamamış, sanal klavye kullanmamıştır. Alt derece mahkemesi, "*yetkisiz kişiler tarafından internet*

---

376 **İnal**, s. 369.
377 **Kaneti**, s. 610.
378 **Yarg. 11. HD.**, E. 2005/13455, K. 2007/426, T. 18.1.2007;
379 **Yarg. 19. HD.**, E. 2007/7397, K. 2008/3029, T. 27.03.2008; Yarg. 11. HD, E. 2014/14284, K. 2015/31, T. 12.1.2015.
380 **Yarg. 19. HD.**, E. 2016/446, K. 2016/6786, T. 19.4.2016.
381 **Yarg. 11. HD.**, E. 2014/1093, K. 2014/8165, T. 30.4.2014.
382 **Eren**, Genel Hükümler, s. 563.
383 **Yarg. 11. HD.**, E. 2005/4748, K. 2006/7341, T. 22.06.2006.

bankacılık şubesi aracılığıyla 15 dakika içinde (16) ayrı işlemle para havalesi yapılmasını fark eden güvenlik sisteminin davalı bankada bulunmadığı, iki gün sonra sisteme girmeye çalışan davacının kullanıcı şifresinin değiştirilmesi nedeniyle girememesine karşın bankanın her hangi kilitleme yapmadığı" gerekçesiyle davanın kabulüne karar vermiş, Yargıtay kararı onamıştır.

Yüksek Mahkeme, 14 Haziran 2011 tarihli bir kararında384 şunları belirtmiştir: "*... davalı bankanın internet bankacılığında kendisinin ve müşterilerinin güvenliğini sağlayacak güvenlik enstrümanlarının kullanılmasını zorunlu kılmayıp, somut olayda davacının inisiyatifine bırakması zararın doğmasında başlıca etken olup, davalı bankanın zarardan sorumlu olduğu açıktır. Bunun yanında, davacıya güvenlik enstrümanlarını kullanmadan işlem yapma yetkisinin davalı banka tarafından verilmiş olması karşısında, bunları kullanmadan işlem yapan davacının meydana gelen zararda müterafik kusuru olduğunun kabulü de mümkün değildir*".

Görüldüğü üzere, müşteri özensiz (sanal klavye kullanmama, anti-virüs programını güncellememe) davranmış olsa bile, banka, internet bankacılığı sisteminin güvenliğini sağladığı sürece, müşterinin özensiz davranışı zararın ortaya çıkmasına sebebiyet verecek yoğunluğa ulaşamamaktadır. Başka bir deyişle, bankanın uyguladığı veya uygulaması gereken güvenlik tedbirleri, müşterinin özensiz davranışı sonucunda zararın ortaya çıkmasını engelleyebilmektedir. Bu anlamda, meselâ, sınırlandırılmış havale miktarına rağmen havalenin gerçekleştirilmesi sonucunda ortaya çıkan zarara banka katlanacaktır.

Amerikan Mahkeme uygulamasına baktığımızda, bankanın güvenlik sisteminin cevap vermesi gereken hukuki taleplerin (standartların) belirlenmesi

---

384 **Yarg. 11. HD.**, E. 2009/14338, K. 2011/7217, T. 14.06.2011; Ancak Yargıtay'ın aksi yönde kararı da mevcuttur: Mesela Yargıtay 30 Ocak 2013 tarihli bir kararında[384] şu gerekcelerle alt derece mahkemesinin kararını bozmuştur: "*... kartının çalındığını ileri süren davacı, kartın kötüniyetli kişilerin eline geçmesine sebebiyet verdiğine göre, olayda kusurludur. Ne var ki, davacıya ait kredi kartıyla aynı gün, arka arkaya, aynı üye işyerinden standarda uygun olmayan alışverişe izin veren ve bu hususta davacıyı bilgilendirmeyen bankanın da olayda müterafik kusurlu olduğunun kabulü gerekir. ... Davacıya ait kredi kartıyla aynı gün, arka arkaya, aynı üye işyerinden standarda uygun olmayan alışverişe izin verilmesi, davacının da kartını çaldırması ve bunu 3 gün sonra fark ederek davalı bankaya bildirmesi üzerinde durularak mahkemece her iki tarafın kusuru oranı belirlenmek suretiyle aralarında bankacılık konusunda uzman bir bilirkişinin de bulunduğu bilirkişi heyetinden rapor alınarak, sonucuna uygun bir karar verilmesi gerekirken, yazılı şekilde davanın reddine karar verilmesi usul ve yasaya aykırı olup, bozma nedenidir*" (**Yarg. 13. HD.**, E. 2012/23483, K. 2013/1906, T. 30.01.2013).

açısından "*Patco Construction Co. v. People's United Bank*" davasında kabul edilmiş karar büyük önem arz etmektedir[385]. Davaya konu olayda, 7, 8, 11, 12 ve 13 Mayıs 2009 tarihlerinde Patco şirketinin banka hesabından yetkisiz kişiler tarafından birkaç para transferi işlemi yapılmış ve sonuçta hesaptan 580.000 ABD doları miktarında para çalınmıştır. Yetkisiz kişiler, başlangıçta, şirketin hesabından 50.000 dolar para çekmiş, bu işlemi gerçekleşitirirken de şirket işçilerinin kimlik bilgilerini (kimlik kartı bilgisi, şifre ve kimlik doğrulama sorularının cevapları) kullanmışlardır. İlk para çekme işlemleri, paraların birkaç belirsiz şahsın banka hesaplarına aktarılması ile gerçekleştirilmiştir. Bankanın güvenlik sistemi bu işlem için risk düzeyini 1.000 üzerinden 790 puan (750 puandan fazla puanlı işlemler yüksek riskli işlemler olarak kabul ediliyordu) olarak belirlemiştir. Ancak yüksek riskli işlem olmasına rağmen banka çalışanları işlemi kontol etmediği gibi şirkete de şüpheli işlem bildiriminde bulunulmamıştır. Amerikan Temyiz Mahkemesi bankanın güvenlik sisteminin "ticari açıdan makul" ("commercially reasonable") olmadığı kanaatine varmıştır[386]. Mahkeme'ye göre; birincisi, bankanın güvenlik sisteminin miktarı bir dolar veya daha çok olan tüm işlemler için kimlik doğrulama soruları sorması dolandırıcılık riskini artırmıştır. Şöyle ki, bu durum, yetkisiz kişilerin kötü amaçlı yazılımlar (malware) kullanmakla soruların cevaplarını ele geçirmesine imkân tanımıştır. Aynı zamanda, işlem miktarı talebini bir dolara indiren banka, bununla da tüm sistemi temel işlevselliğinden yoksun bırakmıştır[387]. İkincisi, Mahkeme, bankayı yüksek riskli işlemleri uygun bir şekilde gözlemleme ve müşterileri söz konusu işlemler hakkında bilgilendirme açısından başarısız bulmuştur. Şöyle ki, şirket hesabı üzerinden yapılan işlemin risk puanının 790, yani şirketin tipik risk puanının üzerinde olmasına rağmen, banka şirketi bu konuda uyarmamıştır[388].

Amerikan mahkemesinin *Pickman v. Citibank* davasında Pickman'ait hesaptan 1981 yılının 06 şubat tarihinde 150 ABD dolları, 03 mayıs tarihinde 150 ABD dolları, 09 mayıs tarihinde 2 adet 150 ABD dolları, 10 mayısda 10 ve 120 ABD dolları miktarında müşteri

---

385 Kararın metni için bkz.: Patco Construction Co. v. People's United Bank, 684 F. 3.d 197 (1st Cir 2012); Karar incelemesi için bkz. **Burrow**, **K.R.,** "Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank", N. C. Banking Inst., Vol. 17, Iss. 1, 381-400.

386 **Burrow**, s. 390.

387 **Burrow**, s. 390.

388 **Burrow**, s. 391.

hesabından kart işlemlemleri yapılmıştır. Mahkeme'ye göre, *Pickman* şubat ayı için hesab bakiyesini aldığında artık işlemlerin usülsüz yapıldığı bilgisini haizdir. Mahkeme kararı elektronik fon transferlerine ilişkin Milli Komisyonun son raporundaki tavsiyeleri esas almıştır. Buna göre müşteri bankanı zamanında ihtilafli işlemle ilgili haberdar etmiş olsaydı, önlenmesi mümkün olan usülsüz işlemlerden dolayı sorumluluğu aradan kalkmış olurdu. Mahkeme'ye göre, *Pickman* şubat ayı için hesab özetini aldıkdan sonra 30 gün süresinde bankayı haberdar etmediği için o yalnız ilk usülsüz işleme ilgili ortaya çıkan tazminini bankadan talep ede bilir. Ancak müşteri sonraki usülsüz işlemlere ilişkin bankaya karşı her hangi tazminat talebinde bulunamaz. Çünkü müşteri ilk usülsüz işlemle ilgili bankanı haberdar etmemiş ve bunu sonucunda banka güvenlik sistemindeki zaafiyetini aşkar etmemiştir[389].

Yargıtay da bir kararında aynı sonuca ulaşmıştır. Karara konu olayda müşterinin banka hesabında çok kısa bir süre içerisinde 12 ayrı işlem gerçekleştirilmiştir. Yüksek Mahkeme'ye göre; *"... 26.07.2006 günü farklı IP adreslerinden davacının hesabına birden fazla erişim sağlanarak, en son saat 13:52-15:06 arası davacı hesaplarında inceleme, bağlı hesapları değiştirme, döviz bozma, vadesiz hesaba aktarma, havale ve EFT talimatları oluşturma işlemleri yapılarak, davacı hesabından 3. şahıslarla ilgili banka şubelerine elektronik ortamda 12 ayrı işlemle 75.800 YTL para çıkışı yapıldığı ... anlaşılmaktadır. Çok kısa bir süre içerisinde 12 ayrı işlemle internet yolu ile davacının haberi olmadan davalı banka nezdindeki hesabından fazla miktarda para çıkışına neden olan ve tek kullanımlık şifre, telefon mesajı ile ilgili bilgi verme gibi ek güvenlik önlemlerini uygulamayan davalı bankanın tam kusurlu ve sorumlu bulunduğunun kabülü gerekir*"[390]. Yargıtay 12.06.2012 tarihinde, *"... aynı gün kısa aralıklarla davacının hesabına defalarca giriş yapılmış olmasına rağmen dava konusu hesabın uzun süre açık kalmasının banka güvenliği tarafından fark edilmemiş olmasından dolayı davalı banka olayın meydana gelmesinde kusurludur*" şeklinde karar vererek bankayı sorumlu tutmuşdur[391].

---

[389] **Mason, Stephen** Electronic Signatures in Law, SAS Humanities Digital Library, School of Advanced Study, University of London, 2016, s. 217.

[390] **Yarg. 11 HD.**, E. 2008/5526, K. 2010/1892, T. 18.02.2010.

[391] **Yarg. 11. HD.**, E. 2011/3961, K. 2012/10319, T. 12.06.2012.

Ancak, Yargıtay, hesaba bloke konulduğu tarihe kadar yapılan usulsüz işlemlere dolayısıyla, bankaya ait müşteri hizmetleri numarasını arayarak kartını bloke ettirmeyen müşteri ile birlikte, çekilen meblağın yüksek olması, işlem sıklığı, ve işlem yapılan yerlerin iki farklı il olmasına rağmen müşterisini uyarmayan bankanın eşit oranda kusurlu olduğuna hükmederek ilk derece mahkemesinin kararını onamıştır[392].

Bazı durumlarda bankanın özensiz davranışına rağmen müşterinin kusuru da zararın doğmasında etkili olduğundan bankanın ortak kusuru söz konusu olmaktadır. Bir olayda Yargıtay; "... *ATM cihazlarındaki kart yuvalarını kötüniyetli üçüncü kişilerin kolayca müdahalelerine imkân tanıyacak şekilde bırakan ve yine, ATM cihazlarına kötüniyetli üçüncü kişilerin telefon düzeneği yerleştirmelerini engelleyecek ve bu konuda yeterli denetim tedbirlerini almayan davalı bankanın olayda asli kusurlu olduğunun kabulü gerekir. ... Kartı ATM cihazına sıkışan davacı daha güvenli yollardan kart çıkaran bankayı haberdar etmek yerine kötüniyetli kişilerin talimatı ile hareket edip kart ve bilgilerinin onların eline geçmesine sebebiyet verdiğine göre, olayda davacının da müterafik kusurlu olduğunun kabulü zorunludur. Öyle olunca mahkemece, tarafların olaydaki kusur ve sorumluluklarının yukarıda belirtilen ilkeler çerçevesinde belirlenmesi ve hasıl olacak sonuca uygun bir karar verilmesi gerekirken, yazılı şekilde hüküm tesisi usul ve yasaya aykırı*" gerekçesiyle ilk derece mahkemesinin kararını bozmuştur[393].

Görüldüğü gibi, ATM cihazlarının fiziksel güvenliğini sağlamadığı için bankanın özensiz davrandığında tereddüt yoktur. Ancak bankanın bu davranışı zararın doğmasında tekbaşına etkili değildir. Şöyle ki, yetkisiz kişilerin ATM cihazına düzenek yerleştirmekle banka kartının kopyalaması tekbaşına ATM'den para çekme işleminin kısa sürede gerçekleştirilmesi için yeterli değildir. Yargıtay kararına konu olayda olduğu gibi, müşteri banka kartı şifresini tanımadığı (yetkisiz)

---

392 **Yarg. 11. HD.**, E. 2015/9064, K. 2016/4231, T. 18.04.2016.

393 **Yarg. 13. HD.**, E. 2008/12361, K. 2009/2549, T, 27.02.2009; Aynı yönde: **Yarg. 11. HD.**, E. 2009/11424, K. 2011/4290, T. 12.04.2011; **Yarg. 11. HD.**, E. 2009/12515; K. 2011/5034, T. 26.04.2011; **Yarg. 11. HD.**, E. 2010/15730, K. 2012/5666, T. 09.04.2012; **Yarg. 11. HD.,** E. 2011/15762, K. 2013/335, T. 10.01.2013; **Yarg. 11. HD.**, E. 2013/11722, K. 2014/1360, K. 22.01.2014; **Yarg. 11. HD.**, E. 2013/18094; K. 2014/5891; T. 26.03.2014.

kişilerle paylaştığı için ATM'den usulsüz para çekme işlemi gerçekleştirilmiş olmaktadır.

B. BKartK'nın Öngördüğü Sistem

1. Genel Olarak

Yukarıda belirtildiği üzere kart hamilinin kart kullanımında uyması gereken bir özen yükümlülüğü vardır. Kart hamilinin özen yükümlülüğüne aykırı davrandığı tespit edilebiliyorsa, meydana çıkan zarardan kart hamilinin sorumlu olup olmadığı sorusu gündeme gelir. Kart hamilinin özensiz davranışı nedeniyle kartın yetkisiz kişinin eline geçmesi durumunda hamil açısından sözleşmenin müspet ihlâli söz konusu olur ve bu ihlâl kusur oranında tazminat borcu doğurur[394].

BKartK'nın 12. maddesi bu konuda özel bir düzenleme getirmektedir. Anılan hüküm gereğince, "*kartın ya da 16'ncı maddede belirtilen bilgilerin kaybolması veya çalınması hâlinde kart hamili, yapacağı bildirimden önceki 24 (yirmidört) saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan 150 (yüzelli) Yeni Türk Lirası ile sınırlı olmak üzere sorumludur. Hukuka aykırı kullanımın, hamilin ağır ihmaline veya kastına dayanması veya bildirimin yapılmaması hâllerinde bu sınır uygulanmaz*". Ancak BkartK 'nın 43. maddesi bu konuda bir istisna getirmektedir. Sözkonusu maddeye göre, "*tacirlere verilen kurumsal kredi kartları hakkında uygulanmaz*".

2. Kartın Haksız Kullanılma Şekilleri

Kartın haksız kullanılması farklı şekillerde gerçekleşebilir. Birincisi, kart hamili kendisi kartı haksız kullanmış veya kullandırmış olabilir. İkincisi, kartın taklidinin (sahte kart) yapılmasıdır. Üçüncüsü, kartın kendisi çalınmış veya kaybedilmiş olabilir. Dördüncüsü, yetkisiz kişi kart bilgilerine ulaşmış ve internet üzerinden işlemleri gerçekleştirmiş olabilir. Bu durumda, kartın kendisi kart hamilinin zilyetliğinde bulunur.

---

394 **Atamer**, Kredi Kartı, s. 1007.

a. Kart Hamili Tarafından Haksız Kullanım

Kart hamilinin kendisinin haksız kullanım sebebiyle doğan ekonomik sonuçlara katlanması gerektiği açıktır. Bu gibi durumlarda, mesela, kart hamili kendine ait kredi kartıyla ATM'den para çektikten veya yaptığı internet bankacılığı işleminden sonra derhal bankayı arayıp kartını kaybettiğini veya çaldırdığını beyan ederek işlemleri geçersiz kılmaya çalışmaktadır. Aynı şekilde, kart sahibi kendi kartını başka kişilere kullandırabilmektedir[395]. Bu şekilde kredi kartıyla kendisi işlem yapmamış gibi gösterip bankaya karşı işlemlerin sahte olduğu iddiasıyla dava açmaktadır. Bu gibi durumlarda, bankanın, kart hamilinin kendisinin kartı haksız kullandığını isbat etmesi her olayda mümkün görünmemektedir.

b. Sahte Kart Kullanımı

Kötü niyetli kişiler, müşterinin kart bilgilerini ele geçirmek suretiyle sahte kart oluşturabilirler. Orjinal kart bilgilerinin ele geçirilmesi için farklı yöntemler kullanılır. Meselâ, kart verisinin ATM veya POS cihazları üzerine yerleştirilen ya da özel bir cihazla kopyalanması gibi. Yahut kart bilgilerinin depolandığı veri tabanındaki kart numaralarının ele geçirilmesi ve bu verilerden sahte kartların oluşturmak amacıyla kullanılması gibi.

Sahte kart kullanımı sonucunda doğan zararlara bankanın katlanması gerektiği söylenebilir. Zira banka kartın taklidinin yapılmasını engellemek için gerekli tedbirleri almakla mükelleftir ve eğer, bunu sağlayamamışsa, zararlı sonuçlara katlanması gerekmektedir. Bu kural, etki alanı teorisinin bir uygulaması

---

[395] Yarg. 19 HD. E. 2016/14402, K. 2017\4674, T. 07.06.2017 kararına konu olan olayda, *"davacı, bankanın kendisine verdiği kredi kartını iradesi dışında elinden çıktığını, dava dışı 3. şahıs tarafından harcama yapıldığını, bankanın kusurlu olduğunu iddia ederek bankaya yaptığı ödemelerin iadesini istemiştir. Dosyada bulunan telefon kayıtları çözümlemesinden ve diğer delillerden davacının kredi kartını arkadaşına verdiği, yapılan harcamalardan bilgisinin olduğu anlaşılmıştır."*. Yarg. 19 HD. *"... kart hamili bankanın kendisine verdiği kredi kartını ve şifresini muhafaza etmekle yükümlü olup kendi isteği ile 3. kişiye vermesinden abnkaya izafe edilebilecek bir kusur bulunmamaktadır. Davacı kendi kusurundan kaynaklanan zarara katlanmak zorundadır. Mahkemece davanın reddine karar verilmesi gerekirken yazılı şekilde karar verilmesinin doğru olmadığı*" gerekçesi ile ilk derece mahkemesinin kararını bozmuştur.

olarak da görülebilir. Zira bu teoriye göre, banka, kendisinin etki alanında kalan ve aslında çözebileceği problemlerden doğan zararlara göre sorumludur[396].

Diğer yandan, BBSEBHY'nin 42. maddesinin 4. fıkrası bu konuda bankalar açısından açık bir yükümlülük içermektedir. Anılan hüküm gereğince, banka tarafından, *"ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınır, uygulamaların ve uygulamalara ilişkin kritik servis ve verilerin bütünlüğü periyodik olarak doğrulanır. ATM'ler üzerine güvenlik açıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM'ler üzerinde çalışan işletim sisteminin gerekli olan en az yetki ve ayrıcalıklara sahip olarak çalışacak şekilde ayarlanmış, gerekli güncellemeleri ve yamaları yüklenerek sıkılaştırılmış, stabil ve günün teknolojisine göre güvenli bir işletim sistemi olması sağlanır. Banka, ATM'lerde, kaynağını ve bütünlüğünü onaylayamadığı uygulama ve kodların çalışmasını engelleyecek önlemleri alır."*.

Aynı zamanda, "*ATM'lere yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasına imkân verecek bütün giriş noktaları erişime kapatılır ve ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ilave güvenlik tedbirleri uygulanır*." (BBSEBHY'nin m. 42, f. 5)

c. Kayıp/Çalıntı Kart Kullanımı

Bazı durumlarda kötü niyetli kişiler, kart hamilinin zafiyetinden faydalanarak veya el çabukluğu ile banka kartını, şifresi ile birlikte ele geçirebilirler. Aynı zamanda, kaybolan bir kart üçüncü bir kişi tarfından da kullanılabilir. Bu gibi durumlar, kart hamilinin bilgisi dışında gerçekleştiği ve hamilin olayın farkına varması bazen zaman aldığın için bankaya haber verilinceye kadar, banka kartının haksız kullanılması mümkün olabilmektedir.

---

396 **Memiş**, s. 881; **Steennot**, Allocating liability, s. 2.

3. Kartın Haksız Kullanılmasından Doğan Zararın Paylaştırılması

a. Bildirimden Önce

BKartK'nın 16. maddesi gereğince, kart hamili, kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi hâlinde kart çıkaran kuruluşu derhal haberdar etmek zorundadır. BKartK'nın 12. maddesine göre, *"kart hamili, yapacağı bildirimden önceki yirmidört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüzelli Türk Lirası ile sınırlı olmak üzere sorumludur."*

Görüldüğü gibi, BKartK, *"kart hamili açısından bildirimde bulunduğu andan önceki yirmidört saatlik dönem için sınırlı (yüzelli türk Lirası miktarındasorumluluk getirmektedir."* Yirmidört saatlik süre sınırı, gerek kart sahibinin kayıp/çalıntı bildirimini en kısa zamanda yapmasını sağlama gerek taraf menfaatlerini dengeleme gerekse de kart sahibinin sorumluluğunu sınırlandırma işlevleri sebebiyle yerinde sayılabilir[397].

Bildirim anı ile kartın kaybolduğu/çalındığı an arasındaki sürenin yirmidört saatten az olması durumunda, kart hamilinin kartın haksız kullanımından doğan zararın yalnız yüzelli Yeni Türk Lirası miktarındaki kısmına katlanacağı açıktır. Ancak bu sürenin, yani kayıp/çalıntı ve bildirim arasındaki sürenin yirmidört saatten fazla olduğu ve haksız kullanımından bu (yirmidört saatlik süreden önceki) dönemde gerçekleşdiği durumlarda, sorun daha karmaşık hâle gelecektir. Şunu belirtelim ki, biz burada, kart hamlinin kast veya ağır ihmalinin bulunduğu yahut bankanın da kusurlu sayılabileceği (mesela, ATM güvenliğinin sağlamadığı) durumları kast etmemekteyiz. Diğer bir ifadeyle, kart hamilinin bildirimde geç bulunduğu, ancak bunun kart hamilinin kast veya ağır ihamli sonucunda gerçekleşmediği durumlarda, sınırlı sorumluluğun uygulanıp uygulanamayacağına ilişkin sorun sözkonusu olabilir.

BKartK'nın 12, 15 ve 16. maddelerinin getirdiği düzenlemeler karşısında, genel kuralın, bildirim anından geriye dönük yirmidört saatlik sürenin bittiği andan itibaren bankaların sorumluluğunun sona erdiği ve bu andan önce yapılan kullanımlardan doğan zarara kart hamilinin katlanacağı yönünde olduğunu söylemek

---

[397] **Bahtiyar, M.,** "Banka Kartları ve Kredi Kartları Kanunu'na göre Kartın Haksız Kullanımından Dolayı Hukuki Sorumluluk" İÜHFM, C. LXXI, 2013, s. 82.

mümkündür[398]. Ancak hâl ve şartların varlığı durumunda, bu kurala istisna tanınabilir. Nitekim BKartK'nın 16. maddesi kart hamilinin bildirimde bulunma yükümlülüğünü "*kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi*"ne (bilmesine) bağlamıştır. Şüphesiz, bilme hâlinin ispat zorluğu dikkate alındığında, müşterinin kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi bilmesi gerektiği durumlar da "bilme" kapsamında değerlendirilebilmelidir. Bu anlamda, kart hamilinin, bildirim anından geriye dönük olarak yirmidört saatlik sürenin bittiği andan evvelki dönemde gerçekleşmiş herhangi bir haksız işlemi veya kartının kaybolması/çalınmasını bilmemesini haklı kılacak bir sebep varsa, onun sınırlı sorumluluk kuralından yararlanabileceğinin kabülü gerekir. *Mesela,* Alman Federal Mahkemesinin 1984 tarihli bir kararına konu olan olayda mahkeme, ilkbahar 1981'den Ağustos 1981 sonuna kadar Amerika ve Kanada'da bulunan bir iş adamının ancak dönüşünde kredi kartını hukuka aykırı kullanımına ilişkin olarak yaptığı itirazı kabul etmişdir[399]. Brüksel Mahkemesi 2002 tarihli bir kararında, banka kartını bir ay önce kaybetmesine rağmen bunun farkında olmayan kart hamilinin ağır ihmalinin olmadığına kanaat getirmiştir[400]. Aynı Mahkeme 2005 tarihli kararında, kart sahibinin cebinden düşmüş cüzdanı geri aldıktan sonra cüzdanını derhal kontrol etmemesini ağır ihmal olarak nitelendirmemiştir[401].

Şüphe yok ki, kart hamilinin ağır ihmalinin varlığı hâlinde, BKartK'nın 12. ve 16. maddeleri uygulama alanı bulur ve haksız kullanım sonucunda ortaya çıkan zarara kart hamili katlanır. Bu durumda iki ihtimalin ayrı ayrı incelenmesi gerekir. Şöyle ki, banka kartının kaybolması veya çalınması hâlinde, durumdan haberdar olan kart hamilinin bankaya derhal bildirimde bulunmaması, ağır ihmal olarak nitelendirilebilir. Bize göre, bu (yani müşterinin bildirimde bulunması gereken andan bildirimde bulunduğu ana kadar yirmidört saatlik sürenin bitmediği) ihtimalde dahi,

---

398 **Bahtiyar**, s. 83.

399 **Atamer**, Kredi kartı, s. 1009, dn. 78.

400 **Steennot**, **R.,** "Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market", Computer Law and Security Report, 24 (2008), s. 557.

401 **Steennot**, Directive, s. 557.

yüzelli türk lirası miktarındaki sınırlı sorumluluk uygulama alanı bulmaz, zarara müşterinin tek başına katlanması gerekir.

İkinci ihtimalde, mesela, müşterinin kartının 5 Mayıs tarihinde kaybolduğunu, müşterinin bundan 10 Mayıs'ta haberdar olduğunu, ancak bankaya 12 Mayıs'ta bildirimde bulunduğunu, 5-10 Mayıs tarihleri arasında kartını kaybettiğini bilmediğini ve bilmesi gerekmediğini (yani haklı bir sebebin varlığını) farz edelim. Bu ihtimalde haksız kart kullanımı 10-12 Mayıs tarihleri arasında gerçekleşmiş olursa, müşterinin ağır ihmalinin olduğu, bu sebeple de zarara tek başına katlanması gerektiği kabul edilecektir. Ancak haksız kart kullanımının 10 Mayıs tarihinden önceki dönemde gerçekleşdiği ihtimalde, müşterinin geç bildirimde bulunması BKartK'nın 12. ve 16. maddelerinin uygulanmasına imkân tanımaz.

b. Bildirimden Sonra

Banka bildirimden sonra gerçekleşen haksız kullanımdan doğan zararlara katlanmak zorundadır. Bu da mantıklıdır. Zira banka, bildirimden sonra gerekli tedbirleri alarak kartın haksız kullanımının engelleme imkânına sahiptir. Bu kural, Etki alanı teorisinin uygulanmasının bir görünümü olarak anlaşılabilir[402]. Alman Federal Mahkemesine göre, kredi kartının kaybedilmesinde kart sahibinin ağır kusuru olsa dahi, kayıp bildiriminin yapılmış olmasıyla birlikte, kartın kötüye kullanılması engellenmiş bulunduğundan, bildirim tarhinden sonra doğacak zarara kartı çıkaran kuruluş katlanmalıdır[403]. Yargıtay'ın uygulaması[404] da bu yöndedir.

4. Bankanın Müşteriye karşı Talebinin Hukukî Dayanağı

Müşterinin özensiz davranışı yetkisiz kişilerce banka hesabındakı paranın farklı yöntemlerle çekilmesi ve böylelikle de, bankanın zarara uğraması sonucunu doğurmaktadır. Bu sebeple de, bankanın müşteriye karşı talep hakkının hukuki dayanağının belirlenmesi gerekmektedir. Şu ihtimalde, bankanın söz konusu

---

402 **Steennot**, Allocating Liability, s. 3.
403 **İşgüzar**, s. 121.
404 **Yarg. 19 HD.**, E. 1993/4373, K. 1994/3904, T. 18.04.1994; **Yarg. 19 HD.**, E. 2012/1512, K. 2012/11091, T. 04.07.2012.

talebinin hukuki temelinde vekilin (bankanın) yaptığı giderlerin karşılanması ve ya tazminat talepleri dayanabilir[405]. Bu dayanakları ayrılıkta incelemekte fayda vardır.

a. Giderlerin Karşılanması Talebi

Bankanın, elektronik bankacılık hizmetlerini müşteri ile yaptığı sözleşme uyarınca yaptığında tereddüt yoktur. Elektronik bankacılık sözleşmesinin tarafları arasındaki münasibetlere TBK'nın vekalet sözleşmesine ilişkin hükümleri uygulanmaktadır. Şu hâlde, bankanın vekalet sözleşmesinin hükümleri çerçevesinde vekalet alan olarak masrafların karşılanmasını talep hakkını haiz olup olmadığı sorusu ortaya çıkabilir. Zira TBK'nın 510. maddesinin 1. fıkrasına göre, "*Vekâlet veren, vekâletin gereği gibi ifası için vekilin yaptığı giderleri ve verdiği avansları faiziyle birlikte ödemek ve yüklendiği borçlardan onu kurtarmakla yükümlüdür*".

Yetkisiz kişiler tarafından gerçekleştirilen bankacılık işlemlerinde müşterinin bankaya yönelik hiçbir talimatı olmadığı için vekalet sözleşmesine ilişkin hükümlerin uygulanması gündeme gelmez. Ancak banka verilen talimatın gerçek veya sahte (usülsüz) olduğunu ayırt edemediği durumlarda, bankacılık işleminin kimlik doğrulama araçları kullanılmakla gerçekleştirildiğini ve bu sebeple de müşterinin talimatı ile hareket ettiğini ileri sürebilirmi?[406] Alman Hukukunda bazı yazarlar[407], elektronik bankacılık açısından gelişmiş teknik güvenlik tedbirlerinin uygulandığını dikkate almakta, bankaya gelen sahte talimatın sanki gerçek kimlik doğrulama araçları kullanılmakla ve müşteri tarafından gerçekleştirildiği sonucunu doğurduğunu (yani müşterinin sözleşme ile bağlı olduğunu) kabul etmektedirler. Bu görüşün temelinde görünürdeki temsil yetkisi[408] (Anscheinsvollmacht, apparent authority) kavramı dayanmaktadır[409]. Buna göre, temsil olunan, temsilcinin kendi temsilcisi olduğu izlenimini yaratacak (genellikle, az çok tekrarlanmış)

---

[405] **Spindler, G./Recknagel, E.,** "Legal Aspects of Internet Banking in Germany", Handbook on Information Technology in Finance, Ed. **Seese, D./Weinhardt, C./Schlottmann, F.,** Springer, 2008, s. 737.

[406] Şüphesiz, bu ihtimalde dahi, müşterisinin talimatı ile hareket ettiğini isbat yükümlülüğü bankanın üzerindedir. Banka bu konuda her hangi delil takdim edemezse, giderlerinin karşılanmasını talep edemez.

[407] **Spindler/Recknagel**, s. 738'de anılan yazarlar.

[408] **Kocayusufpaşaoğlu**, "ihmal suretiyle yaratılan hukukî görünüşe dayalı temsil yetkisi" kavramını kullanmaktadır. Bkz., **Kocayusufpaşaoğlu**, s. 644 vd.

[409] **Spindler/Recknagel**, s. 738.

davranışlarından haberdar olmamasına rağmen gerekli özeni gösterseydi bu durumu öğrenmek ve engellemek imkânına sahip bulunuyor idiyse, ihmal suretiyle yaratılan ve ona isnat edilebilen bu hukuki görünüşün sonuçlarına katlanmak zorundadır[410]. Başka bir anlatımla, görünürdeki temsil yetkisinden maksat, temsil olunanın gerçekte bilmemekle birlikte, gerekli özeni göstermiş olsaydı, başka bir kişinin temsilci sıfatıyla kendi adına hateket ettiğini ve üçüncü kişilerin dürüstlük kuralına göre bu hareketten söz konusu kişinin temsilci olabileceği sonucunu çıkartabileceklerini bilmesi gereken yetkidir[411].

Ancak Alman Hukukunda hakim görüş, görünürdeki temsil yetkisi kavramının söz konusu durumlarda uygulanmasına şu gerekçelerle karşı çıkmaktadır[412]. Şöyle ki, görünürdeki temsil yetkisinin uygulanması için temsilcinin belli bir süre zarfında ve az çok tekrarlanmakla temsil olunanın temsilcisi görünüşünü yaratması gerekmektedir. Yetkisiz kişiler tarafından yapılan işlemler ise, genellikle, bir kereye mahsus gerçekleştirilmektedir.

Diğer yandan, elektronik bankacılık açısından banka, temsilcinin değil, müşterinin kendisinin kimlik doğrulama araçlarını kullandığını, yani işlemin gerçekleştirilmesine ilişkin talimatın müşteri tarafından verildiğini farz etmektedir[413]. Bundan başka, görünüşteki temsil yetkisinden sö etmek için temsilcinin, genellikle temsil olunana ait alanda hareket etmesi gerekmektedir, zira bu ihtimalde, temsil olunanın gerekli özeni gösterseydi bu durumu öğrenmek ve engellemek imkânına sahip bulunduğunu söylemek mümkün olabilir.

Görüldüğü gibi, görünüşteki temsil yetkisi kavramının elektronik bankacılık işlemleri açısından uygulanması mümkün görünmemektedir. Alman Hukuk öğretisinin görünüşteki temsil yetkisinin elektronik bankacılık işlemleri açısından uygulanmasını istisna eden hakim görüşün gerekçeleri Türk Hukuku[414] açısından da

---

[410] **Kocayusufpaşaoğlu**, s. 644 vd.; **Eren**, Genel Hükümler, s. 437; **Spindler/Recknagel**, s. 738.
[411] **Eren**, s. 437; **Oğuzman/Öz**, C. 1, s. 222.
[412] **Spindler/Recknagel**, s. 738'de anılan yazarlar.
[413] **Spindler/Recknagel**, s. 738.
[414] Alman Hukukundan (BGB, §167) farklı olarak TBK'da temsil yetkisinin üçüncü kişilere bildirilmek suretiyle verilmesine ilişkin açık hüküm bulunmamaktadır. Türk Hukuk öğretisindeki büyük çoğunluk temsil yetkisinin sadece temsilciye yapılacak bir beyanla verilebileceğini kabul, üçüncü kişiye yapılacak bir beyanla temsilci tayin etmek imkânını istisna etmektedir. Ancak temsil olunan temsilci olarak yetkilendirilecek kişiye karşı bir beyanda bulunmayıp, yalnız üçüncü kişiye yapılan bir bildirim ile yetinilmişse, üçüncü kişinin bu beyana olan güveni TBK'nın 41. maddesinin 1.

geçerlidir. Bu açıdan baktığımızda, bankanın TBK'nın 510. maddesinin 1. fıkrasına dayanarak giderlerin karşılanmasını talep hakkına sahip olduğunu demek mümkün değildir.

b. Tazminat Talebi

Müşteri elektronk bankacılık sözleşmesinden ileri gelen yükümlülüklerini ihlâl etmesi bankanın ona karşı tazminat talebinin doğmasına sebebiyet verir (TBK, m. 112). Müşterinin akdî sorumluluğunun doğması için onun yükümlülüyünün ihlâli ile birlikte diğer şartların (zarar, kusur, borca aykırı davranışla zarar arasında uygun illiyet bağı) da mevcut olması gerekmektedir. Buradaki zarardan maksat müspet zarardır. Zira buradaki müspet zarar bankanın malvarlığının aktifinin azalmasında (fiili zarar olarak) kendisini göstermektedir.

IV. Sorumsuzluk Anlaşmaları

A. Genel Olarak

Borcunu kasden veya ihmal suretiyle hiç veya gereği gibi ifa etmeyen borçlu, akdi bir kusur işlediğinden zararı gidermekle sorumlu bulunmaktadır. Bu anlamda, borçlunun, tarafı olduğu sözleşmeyi hiç veya gereği gibi ifa etmediği hâllerde, sorumluluğunun önceden kaldırılmasının mümkün olup olmadığı sorunu ortaya çıkmaktadır. Sorumsuzluk anlaşması, akdîn ihlâlinden kaynaklanan zararın ortaya çıkmasından önce alacaklı ve borçlu arasında açık veya örtülü olarak, bağımsız veya asıl sözleşmeye ek olarak yapılır. Amaç ilerde alacaklı lehine meydana çıkma ihtimali bulunan tazminat talebinin doğmasına tamamen veya kısmen engel olmaktır[415]. Hukuki niteliği yönünden sorumsuzluk anlaşması öne alınmış bir tasarruf işlemidir; gelecekteki olası tazminat borcunun önceden (peşinen) ibra edilmesidir[416]. Diğer bir ifadeyle, sorumsuzluk anlaşması, alacaklı yönünden bir tasarruf işlemi, borçlu yönünden ise bir kazandırıcı işlemdir. Bu sözleşme ile ilerde

---

fıkrası gereğince korunmuşur. Bkz. **Kocayusufpaşaoğlu**, s. 640-641; **Eren**, s. 436; **Oğuzman/Öz**, s. 222-223..

415 **Eren**, Genel Hükümler, s. 1085-1086; **Oğuzman/Öz**, s. 409-410; **Tandoğan**, Mesuliyet Hukuku, s. 453-454.

416 **Serozan,** İfa Engelleri, s. 279.

gerçekleşmesi muhtemel bir tazminat hakkı üzerinde tasarruf edilmektedir[417]. Borçlunun kendi kusurundan sorumlu tutulmayacağına ilişkin sorumsuzluk anlaşmaları TBK'nın 115. maddesinde, yardımcı kişilerin fiillerinden sorumsuzluğuna ilişkin sorumsuzluk anlaşmaları ise TBK'nın 116. maddesinde hükme bağlanmıştır. TBK'nın "*Sorumsuzluk anlaşması"* başlıklı 115. maddesine göre*; "borçlunun ağır kusurundan sorumlu olmayacağına ilişkin önceden yapılan anlaşma kesin olarak hükümsüzdür. Borçlunun alacaklı ile hizmet sözleşmesinden kaynaklanan herhangi bir borç sebebiyle sorumlu olmayacağına ilişkin olarak önceden yaptığı her türlü anlaşma kesin olarak hükümsüzdür. Uzmanlığı gerektiren bir hizmet, meslek veya sanat, ancak kanun ya da yetkili makamlar tarafından verilen izinle yürütülebiliyorsa, borçlunun hafif kusurundan sorumlu olmayacağına ilişkin önceden yapılan anlaşma kesin olarak hükümsüzdü*r."

Görüldüğü üzere, kanun koyucu, borçlunun ağır kusurundan veya hizmet sözleşmesinden kaynaklanan herhangi bir borç nedeniyle sorumlu olunmayacağına ilişkin yapılan sorumsuzluk anlaşmalarının kesin hükümsüz olduğuna ilişkin düzenleme getirmiştir. Ayrıca kanun ya da yetkili makamlar tarafından verilen izinle yürütülen ve uzmanlığı gerektiren bir meslek, sanat veya hizmete ilişkin faaliyetlere yönelik sorumsuzluk anlaşmalarına cevaz verilmemiş ve bu anlaşmalar da kesin hükümsüzlük yaptırımına bağlanmıştır.

B. Elektronik Bankacılık Sözleşmesi Açısından

Müşteri ve banka arasında kurulan elektronik bankacılık hizmetlerine ilişkin sözleşmelerde bazı durumlarda bankanın sorumlu olmayacağına dair şartlar bulunmaktadır. Söz konusu şartlar genel işlem koşulları çerçevesinde bankalar tarafından müşterilere dayatılmaktadır. Bankacılık uygulamalarında şöyle bir hükme rastlamak mümkündür: "*Müşteri, Banka'nın sunduğu elektronik bankacılık hizmetlerinin verilmesi esnasında veya herhangi bir zamanda oluşabilecek arıza, telefon hatlarından veya internet servis sağlayıcılarından kaynaklanan aksaklıklar vb. teknik sebepler ile bu hizmetlerin verilmesine ara veya son verilmesi yahut*

[417] Eren, **Genel Hükümler**, s. 1087.

hizmetin kesintiye uğramasından, elektronik bankacılık sistemleri ile gelen bilgi ve talimatların yanlış ya da yetersiz olmasından, yanlış ya da eksik iletilmiş olmasından Bankanın sorumlu tutulamayacağını kabul ve beyan eder"[418].

Bize göre; burada ikili bir ayırıma gitmekte fayda vardır: Şöyle ki, müşterinin banka hesabına kötü niyetli kişiler tarafından erişilmesi veya ATM'den yetkisiz kişiler tarafından para çekilmesi gibi durumlarda, işbu doktora tezinde savunduğumuz görüş uyarınca, ortaya çıkan zarar bankaya ait olduğundan, yani müşterinin bankaya karşı alacak hakkı devam ettiğinden sorumsuzluk anlaşmasına başvurulması söz konusu olmayacaktır. Zira TBK'nın 115. ve 116. maddeleri ancak başkasının malvarlığında doğan bir zarar nedeniyle var olan sorumluluğu kaldırma imkânını ve bunun sınırlarını ele alır, yoksa kendi malvarlığında doğmuş olan bir zarar için kişinin kendi kendine sorumsuzluk anlaşması yapması düşünülemez[419].

Ancak ikinci bir ihtimalde, yani müşterinin zarara uğraması (meselâ, bankanın sistemindeki aksaklıklar nedeniyle havale işleminin zamanında gerçekleşitilmemesi ve müşterinin havale alıcısı karşısında tazminat borcunun doğması, internette döviz alım-satımı işlemini gerçekleştirememesi vs.) ihtimalinde, cevaplandırılması gereken soru şudur: Müşterinin yapmak istediği elektronik bankacılık işlemi gerçekleştirilmezse (meselâ, havale talimatı verilmesine rağmen işlem hiç yapılmazsa), banka bu hükümden yararlanarak sorumluluktan kurtulacak mıdır? TBK'nın 115. maddesinin 3. fıkrasının açık hükmü karşısında, bu sorunun müspet cevaplandırılması imkânsızdır. Çünkü anılan hüküm, EBK'nın 99. maddesinin 2. fıkrasından farklı olarak[420], uzmanlığı gerektiren bir işin kanun ya da yetkili makamlar tarafından verilen izinle yürütülebiliyor olması durumunda, borçlunun hafif kusurundan sorumlu olmayacağına ilişkin önceden yapılan

---

418 Benzer bir şart şöyledir: "Müşteri, online yapılacak havalelerde veya ileri tarihli havalelerde aksine bir talimat verilmez ise teknik bir arızanın ortaya çıkması nedeniyle bekletilen havalenin arızanın giderilmesinden sonra yapılacağını kabul ve beyan eder".

419 **Atamer**, Kredi Kartı, s. 1028-1029.

420 EBK'nın 99. maddesinin 2. fıkrası, borçlunun hafif kusurdan sorumlu olmayacağına ilişkin sözleşme şartlarının, sorumluluğun hükümet tarafından imtiyaz suretiyle verilen bir işin icra edilmesinden kaynaklanması durumunda. hakim tarafından takdir yetkisi kullanılarak batıl sayılabileceği ile ilgili hükmü ihtiva etmekteydi. Ancak doktrinde, bankaların sorumsuzluk koşullarının somut olayın şartları, hakimin takdir yetkisi ile bağlı kalmaksızın, her zaman batıl sayılması yönünde Yargıtay uygulamasının yerleşmiş olduğu, bu şekilde hakime kanunla tanınan takdir yetkisinin elinden alınmış olduğu belirtilmiştir. Bu konuda bkz. **Battal**, s. 8.

anlaşmaların kesin olarak hükümsüz olduğunu kabul etmekdedir. Bankacılık faaliyetinin yetkili makamlar tarafından verilecek izinler çerçevesinde sürdürülebilecek bir faaliyet olmasında tereddüt yoktur. Dolayısıyla, bankaların müşterilerle yapacakları elektronik bankacılık sözleşmelerinde yer alan hafif kusurdan sorumlu olmayacaklarına ilişkin şartlar kesin hükümsüzdür.

Belirtmek gerekir ki, söz konusu sorumsuzluk koşullarının geçersiz sayılması için TBK'nın 25. maddesi veya tüketici sözleşmeleri bakımından TKHK'nın 5. maddesine başvurulması gerekmez. Zira anılan hükümler, emredici kurallara aykırı olmayan, yedek hukuk kuralı niteliğindeki yasa hükümlerinin bankaca tek yanlı olarak değiştirilip müşteriye dayatıldığı sözleşme şartlarının, müşteri bakımından adil olup olmadığı açısından sorgulanması ve adil olmadığının tespit edildiği durumlarda bunların geçersizliğine karar verilmesine hukuki dayanak teşkil eder. TBK'nın 115. maddesinin 3. fıkrası emredici niteliktedir ve söz konusu hükme aykırılık hâlinde TBK'nın 27. maddesinin 1. fıkrasında öngörülen kesin hükümsüzlük yaptırımı uygulama alanı bulur.

Eklemek gerekir ki, sorumsuzluk anlaşmasının geçersizliği, onun eklemlendiği ana sözleşmenin geçersizliğine yol açmaz; zira geçersizliği öngören kuralın amacı ve güven ilişkisi, yararlı olanın yararsızdan olumsuz biçimde etkilenmesini engeller[421].

§ 3. Bankanın Sorumluluğunun Ağırlaşması: Yardımcı Kişilerin Fiillerinden Bankanın Sorumluluğu

I. Genel Olarak

TBK'nın 116. maddesi yardımcı kişilerin fiilllerinden dolayı borçlunun sorumluluğunu düzenlemektedir. Anılan hüküm gereğince, "*borçlu, borcun ifasını veya bir borç ilişkisinden doğan hakkın kullanılmasını, birlikte yaşadığı kişiler ya da yanında çalışanlar gibi yardımcılarına kanuna uygun surette bırakmış olsa bile, onların işi yürüttükleri sırada diğer tarafa verdikleri zararı gidermekle yükümlüdür*".

[421] **Serozan**, İfa Engelleri, s. 283.

Borçlunun TBK'nın 116. maddesine göre sorumlu olabilmesi için herşeyden önce borçlu ile alacaklı arasında bir borç ilişkisinin bulunması gerekir[422]. Ancak buradaki borç ilişkisinin türü önemli değildir. Zira taraflar arasındaki borç ilişkinin kaynağı sözleşme, haksız fiil veya sebepsiz zenginleşme olabilir[423]. Önemli olan ifa yardımcısı tarafından alacaklıya zarar verilmesi anında, borçlu ile alacaklı arasında, bir borcun kaynağını teşkil eden borç ilişkisinin varlığıdır. Sözleşme görüşmelerinde de yardımcı kişi kullanmak mümkündür; bu durumda yardımcı kişi kullanan taraf karşı tarafın zararını TBK'nın 116. maddesi gereği karşılamak zorundadır[424].

TBK'nın 116. maddesi anlamında ifa yardımcısı kavramının kapsamına, borcun ifasında borçluya yardım edenler girdiği gibi, borçlunun borcun ifasını tamamen kendilerine bıraktığı ve "ikame edilen şahıs" adı verilen kimseler de girer[425]. Bu anlamda, üçüncü bir kişinin ifa yardımcısı olabilmesi için önce borçlunun oluruyla, onun "edim eylemini" (bilgisi ve ilgisi dâhilinde) yaşama geçirmesi gerekir[426]. Bunun yanısıra yardımcı kişinin bu sıfatı kazanabilmesi için ifa faaliyetine kendi fiiliyle bizzat katılmalıdır; ifa faaliyetine fiilen katılmayan, borcu ifa etmeyen kişi yardımcı kişi sıfatını kazanamaz[427]. İfa yardımcıları borcun ifasını tamamen yerine getirebilecekleri gibi ifa fiillerini bir kısmını da yerine getirebilirler[428].

---

422 **Eren**, Genel Hükümler, s. 1072.

423 **Tandoğan**, Mesuliyet Hukuku, s. 435.

424 **Eren**, Genel Hükümler, s. 1073; **Oğuzman/Öz**, a.g.e., s. 424.

425 **Oğuzman/Öz**, a.g.e., s. 416-417; .

426 **Serozan**, İfa Engelleri, s. 288; Borçlunun onayı olmaksızın ifaya karışan kişiye borçlu zarara yol açan davranışından sonra "fiilini onayladığını" bildirse de, TBK'nın 116. maddesine göre kusursuz sorumlu olmaz. Yardımcı kişiye onay en geç zarar doğuran fiilinden önce verilmiş olmalıdır (**Oğuzman/Öz**, a.g.e., s. 419).

427 **Eren**, Genel Hükümler, s. 1074; Serozan'a göre; yardımcının alacaklıya zarar veren eyleminin sadece ifa "vesilesiyle" değil de düpedüz "dolayısıyla", ifa "sırasında" gerçekleşmiş olması gerekmektedir; yani zarar verici eylemle borcun ifası arasında bir işlevsel bağlantının bulunması zaruridir. Başka bir deyişle, borçlunun bilgisi ve ilgisi olmaksızın devreye giren "borçluya yabancı" sözde yardımcılar ve "borca yabancı" (borca ilgisiz) atipik rizikolar TBK. 116 kuralının çerçevesi dışında kalır (**Serozan**, İfa Engelleri, s. 291).

428 **Eren**, Genel Hükümler, s. 1075.

II. Elektronik Bankacılık Açısından

Elektronik bankacılık hizmetleri sağlayan bankalar borclarını ifa ederken farklı ifa yardımcıları kullanmaktadırlar. Meselâ, işlem güvenliğinin sağlanması maksadıyla işlem doğrulama kodunun (OTP/One Time Password) müşteriye ulaştırılması için GSM operatorlarının veya sistem sürekliliğini ve bilgi güvenliğini sağlayacak teknik tedbirleri temin etmek için destek hizmet kuruluşlarının hizmetlerinden yararlanmada olduğu gibi.

A. GSM Operatörlerinin Davranışlarından Dolayı Bankanın Sorumluluğu

1. Genel Olarak

Elektronik bankacılıkta işlem doğrulama kodunun (OTP) SMS ile (SMS doğrulama hizmeti) müşteriye ulaştırılması kimlik doğrulama işlemlerine yönelmiş olta (phishing) ve diğer saldırılara karşı bir güvenlik tedbiri olarak uygulamaya konulmuştur. Bu durumda, müşterinin hizmetlerinden yararlandığı bankanın internet şubesine giriş işlemi sırasında, kullanıcı kodu ve statik şifresine ilave olarak veya internet şubesine giriş yapmış müşterinin gerçekleştirmek istediği işlemi onaylamak için işlem doğrulama kodu istenmektedir[429].

İnternet bankacılık hizmetlerinin sunulurken güvenliğin sağlanmasında işlem doğrulama kodunun kullanılmasının dayandığı temel düşünce şöyledir: Sistemdeki her bir hesap cep telefonuna bağlıdır ve söz konusu cep telefonu hesap sahibinin zilyetliğindedir. Böylece, hesap sahibi, hesabın bağlı olduğu cep telefonu numarasına SMS ile gönderilmiş işlem doğrulama kodunu kabul edebilecek tek kişidir. Bu durum, cep telefonunu şifre üreten cihaza (token) dönüştürmektedir. Bu anlamda, müşterinin internet ortamındaki belirli banka hesabına bağlı cihaza (cep telefonuna) fiziksel olarak sahip olmak ve SMS ile kabul ettiği işlem doğrulama kodunu kullanmakla internet bankacılık işlemlerini güvenli bir şekilde gerçekleştirmesi amaçlanmaktadır.

---

[429] **Andrews**, **N.,** "*Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers For SIM-Swap Attacks and Wireless Provider Liability*", Nw. J. Tech. & Intell. Prop., Vol. 16, Is. 2, 2018, s. 83.

SMS doğrulama sisteminde, genel olarak, üç tarafın katıldığı bir ilişki söz konusudur. Şöyle ki, bunlardan ilki, hiç şüphesiz, kimlik doğrulama işleminin güvenli şekilde gerçekleşmesine çalışan bankadır. İkinci taraf, SMS mesajının cep telefonuna ulaşmasını sağlayan GSM operatörüdür. Nihayet, SMS mesajın gönderildiği cep telefonu sahibi üçüncü taraftır. Ancak doktrinde söz konusu ilişkide GSM operatörünün yerine ilişkin iki farklı görüş ifade edilmektedir. Bir görüşe[430] göre; GSM operatörleri kısa mesajlarını banka ile arasındaki abonelik sözleşmesi veya banka ile bu çerçevede kurulan bir hukuki ilişki sebebiyle değil; ilgili telefon hattının kullanıcısı konumundaki abone ile arasındaki abonelik ilişkisi bağlamında iletmiş olmaktadır. Başka bir deyişle, hukuki ilişki (abonelik söleşmesi ilişkisi) banka ile GSM operatörü arasında değil; GSM operatörü ile banka nezdindeki mevduat hesabının sahibi konumundaki kişi arasında bulunmaktadır. Buna karşılık, diğer bir görüşe[431] göre; mevduat sahiplerinin internet bankacılığından yararlanırkan kullanacakları şifreleri cep telefonları üzerinden temin etmek hususunda akdettikleri ayrı bir sözleşme bulunmamaktadır. GSM operaratörü kısa mesaj yoluyla şifre iletiminde rol alsa da, mevduat sahibi abonelik sözleşmesi dışında, tarafı olmadığı bir başka sözleşmeye dayanarak, şirkete sorumluluk atfedemeyecektir. Yargıtay'ın da uygulaması bu yöndedir[432].

Bize göre; GSM operatörünün kısa mesajları hesap sahibine iletme yükümlülüğü banka ile yaptığı sözleşmeden doğmaktadır. Nitekim uygulamada banka ve GSM operatörü arasında yapılan sözleşmelerde genelde, banka tek kullanımlık şifreyi göndermek ve hesap sahibine iletilecek kısa mesajların ücretini ödemek yükümlülüğünü taşımaktadır. Banka, müşteri ile akdettiği elektronik bankacılık hizmetleri sözleşmesi çerçevesinde kısa mesaj ücretlerini müşteriye yansıtabilir. GSM operatörünün asli edim yükümlülüğü, işlem doğrulama kodunu içeren kısa mesajların hesap sahibine en kısa zamanda ulaşmasını sağlamaktır. Bu anlamda, hesap sahibi, taraf olmadığı (banka ile GSM operatörü arasında kurulmuş) sözleşmeye dayanarak GSM operatörüne karşı talepte bulunamaz; banka ile GSM

---

430 **Akkanat**, s. 66-67.
431 **Karaman Coşgun**, s. 175 vd.
432 **Yarg. 11. HD.**, E. 2010/10, K. 2011/16909, T. 13.12.2011; **Yarg. 11. HD.**, E. 2014/13736, K. 2014/19841, T. 16.12.2014.

operatörü arasında kurulmuş sözleşme tam üçüncü kişi yararına bir sözleşme niteliğini haiz değildir[433].

2. SMS Doğrulama Sistemine Yönelik Saldırılar

Dikkat edilirse, SMS doğrulama hizmetinin kullanılmış olması, gerçekleştirilen internet bankacılık işlemlerinde güvenliğin tam sağlandığı anlamına gelmemektedir. Şöyle ki, SMS doğrulama sisteminin kendisinin güvenliği SMS mesajlarının gizliliğine dayanmaktadır; SMS mesajlarının gizliliği ise, büyük ölçüde, GSM operatörünün kullandığı hücresel ağın güvenliğine bağlıdır. GSM ve hatta 3G ağlarına yapılan saldırılar SMS mesajlarının gizliliğinin yeterince sağlanamadığını ortaya çıkarmıştır[434]. Bundan başka, kötü niyetli kişiler cep telefonları için özel trojan virüsleri oluşturmakla işlem doğrulama kodunun sağladığı güvenliği aşabilmektedirler[435]. Meselâ, Kaspersky uzmanları, 2015 yılında Phishing olarak adlandırılan banka kartı bilgilerinin ve banka hesaplarından para çalmak amacıyla tasarlanan kötü amaçlı mobil yazılımların sayısının neredeyse 20 kat arttığını bildirmişlerdir. Ayrıca, 2015 yılı boyunca bankacılık trojan programlarının, kullanıcılar için en tehlikeli kötü amaçlı mobil yazılım türü olduğunu ve yılın başlarında bilinen bankacılık trojan programlarının sayısının 1.527'e yükseldiğini vurgulamışlardır[436].

Kötü niyetli kişilerin amacı işlem doğrulama kodunu içeren SMS mesajı ele geçirmektir. Bu amaçla kötü niyetli kişiler farklı yollara başvurmaktadır.

---

433 **Karaman Coşgun**, s. 177.

434 **Mulliner, C./Ravishankar, B./Stewin, P. vd.**, "*SMS-based One-Time Passwords: Attacks and Defense*", Detection of Intrusions and Malware, and Vulnerability Assessment, 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings, Ed. **Rieck, K./Patrick, S./Seifert, J-P.,** Springer-Verlag, Berlin, 2013, s. 150.

435 **Mulliner/Borgaonkar/Stewin**, s. 151.

436 **Aktürk, C./Talan**, **T.,** "*Mobil Bilişim Suçları*", Enformatik, Toplum ve Hukuk, Ed. **Gürsul, F.,** Legal Yayıncılık, İstanbul, 2016, s. 158.

a. Cep Telefonuna Fiziksel Erişim

Kötü niyetli kişi, cep telefonuna fiziksel olarak erişmekle kolay bir şekilde işlem doğrulama koduna ulaşabilir. Şüphesiz, cep telefonuna fiziksel erişim zor ve zaman alıcıdır. Müşteri tarafından da bu durumun tespiti kolaydır. Uygulamada bu yola başvurulması nadirdir. Zira cep telefonuna fiziksel olarak erişmeden de SMS mesajına ulaşmaya imkân tanıyan araçlar mevcuttur[437].

b. Usulsüz Sim Kart Değişikliği (SIM Swap Attack)

Kötü niyetli kişilerin işlem doğrulama kodunun sağladığı güvenliği aşmak için kullandıkları diğer bir yol, müşterinin elde edilen kişisel bilgileri doğrultusunda sahte belgeler ile SIM kart çıkartmaktır. Böylelikle, banka tarafından müşteriye gönderilen işlem doğrulama kodlarını içeren SMS mesajların yeni çıkarılan SIM karta gelmesi sağlanmakta, müşteri tarafından okunması gereken tüm SMS mesajları kötü niyetli kişilerce ele geçirilmektedir.

c. Kablosuz Araya Girme

Yukarıda belirtildiği üzere, SMS doğrulama sistemi tamamen hücresel ağın sağladığı güvenliğe dayanmaktadır. GSM operatörleri mobil iletişim (mesela, SMS mesaj ulaştırma) hizmetlerini sağlarken GSM, 3G ve CDMA teknolojilerini kullanmaktadırlar. Ancak GSM teknolojisi, karşılıklı kimlik doğrulamasının eksikliği ve şifreleme algoritmasısının zayıflığı sebebiyle güvenli değildir[438]. Özellikle, cep telefonlarıyla GSM baz istasyonları arasında karşılıklı kimlik doğrulama olmadığı için sahte baz istasyonu saldırılarının yapılması muhtemeldir. Sahte baz istasyonu oluşturma yönteminde, GSM opertaörünün frekansından daha fazla güç vererek cihazların sahte baz istasyonuna bağlanması sağlanır. GSM bağlantılarında kimlik doğrulama sadece GSM operatörü tarafında gerçekleştirildiğinden kullanıcı yalnış bir ağa bağlandığından haberdar olmaz ve bütün veri aktarımı sahte baz istasyonu üzerinden yapılmış olur[439].

---

437 **Andrews,** s. 83**; Mulliner/Borgaonkar/Stewin,** s. 152.
438 **Mulliner/Borgaonkar/Stewin,** s. 153.
439 **Aktürk/Talan**, s. 147.

Bundan başka, GSM alanındaki araştırmalar gösteriyor ki, burada uçtan uca (end-to-end) güvenlik yoktur. Bu anlamda, ucuz maliyetli cihazlar kullanarak GSM trafiğinin ele geçirilmesi ve zayıf algoritmalar sebebiyle trafiğin şifresinin çözülmesi mümkündür[440].

d. Kötü Amaçlı Mobil Yazılımlar

Genel olarak kötücül yazılımlar spam nitelikli emaillerle veya faydalı program uygulamaları içerisine eklenen gizli eklentiler ile mobil cihazlara sistemsal olarak erişmektedirler. Bu cür sistemsal erişim esasen mobil cihazlarda bulunan açıklıklar üzerinden yapılmaktadır. Kötücül yazılımları gruplaşdıracak olursak, bu listede trojan[441], solucan[442], virüs[443], toolkit[444], botnet[445], malvertising[446] gibi yazılımlar yer almaktadır. Bu tür mobil kötücül yazılımlar, SMS, MMS, enfekte uygulamalar, solucanlar[447] aracılığı ile yayılmaktadırlar. Bu yazılımların asıl amacı mobil cihazdaki kişisel bilgileri veya kullanıcının hesap bilgilerini ele geçirmektir.

---

[440] **Mulliner/Borgaonkar/Stewin,** s. 153.

[441] *"**Trojan** -yasal uygulamalar gibi davranan programlardır."* Bkz. **Sağıroğlu, Ş./Alkan, M.,** Siber Güvenlik ve Savunma (Farkındalık ve Caydırıcılık), Grafiker Yayınları, Ankara 2018, s. 315.

[442] *"**Solucan** - mobil şebekelerde havadan yayılabilen ve kendi kendini çoğaltabilen kötücül programlar.".* Bkz. **Sağıroğlu/Alkan**, s. 315.

[443] *"**Virüs** - yerleştiği bilgisayardaki veya mobil cihazdaki dosyalara zarar veren, kendini kopyalama yeteneğine sahip yazılımlardır."* Bkz. **Sağıroğlu/Alkan,** s. 315.

[444] *"**Toolkit** - network tabanlı yaygın saldırılar yapmak için kullanılan yazılımlardır."* Bkz. **Sağıroğlu/Alkan,** s. 315.

[445] *"**Botnet** - siber saldırganlar tarafından bilgisayarları kontrol etmek ve gerektiğinde farklı sistemlere saldırı düzenlemek amacıyla kullanılan yazılımlardır. Mobil cihazlardaki sosyal medya uygulamaları botnetler için yeni bir ortam sağlamaktadır."* Bkz. **Sağıroğlu/Alkan,** s. 315.

[446] *"Malversiting - sahte internet siteleri ile bağlantılı özgün görünen reklamlardır."* Bkz. **Sağıroğlu/Alkan,** s. 315.

[447] **"***Kaspersky Lab araştırmacıları tarafından litetatürde Cabir adı verilen ilk mobil kötücül yazılım 2004 yılında tespit edilmiştir. Cabir, dönemin en popüler Symbian işletim sistemine sahip cep telefonlarını hedef almıştır. Cabir bir kez telefona bulaştığında, "Caribe" kelimesi telefon her açıldığında telefon ekranında görüntülenmekteydi. Bu solucan bluetooth iletişimi açıklık olan diğer telefonlara kendini kopyalayabilme özelliğine sahipti. Aslında, Cabir kötücül bir yazılım değildi, ancak sonradan Cabir'in kullanmış olduğu yöntem siber saldırganlar tarafından siber saldırı amacıyla kullanıldığından mobil telefonlara yönelik ilk solucan olarak kabul edilmektedir. 2005 yılında, Cabir'in kullandığı yöntemi kullanan Commwarrior adında yeni bir kötücül yazılım ortaya çıkmıştır. Commwarrior, telefona bir kez bulaştığında adres defterindeki tüm kişilere SMS iletebilmekteydi, alıcı mesajı açtığında ise kendini hedef telefona kopyalamaktaydı. Commwarrior, geliştirenler açısından ekonomik bir fayda sağlamamakla birlikte kurbanlar üzerinde finansal etki yapan ilk mobil kötücül yazılımdır"* **Bkz.** Anonim, https://www.welivesecurity.com/2016/11/01/history-mobilemalware-cabir-sms-thief (Son erişim tarihi: 30.01.2021)

Meselâ, "SMS.AndroidOS.FakePlayer.b isimli uygulama trojan içermektedir. Bu uygulama kullanıcılar tarafından yetişkin içeriklerin izlenebilmesi için geliştirilmiştir ve manuel olarak kullanıcının bir web sitesinden telefonuna indirerek kurması gerekmektedir. Uygulamanın boyutu çok küçüktür ve kurulum sırasında kullanıcıdan SMS göndermeye ilişkin izin istenmektedir. Kullanıcı tarafından uygulama bir kez çalıştırıldığında kullanıcının bilgisi dışında, program tarafından Premium SMS göndermektedir. Bu mesajlar sonrasında kullanıcının parası, bilgisi dışında siber suçlulara transfer edilmektedir."

3. GSM Operatörünün Bankanın Sorumluluğuna Sebebiyet Verecek Davranışları

Yukarıda belirtildiği üzere doktrinde hakim görüş ve Yargıtay uygulaması banka hesabına yetkisiz erişim hâlinde ortaya çıkan zararın bankaya ait olduğu yönündedir. Bu anlamda, yetkisiz kişilerin banka hesabındaki parayı ele geçirmesi durumunda, GSM operatörünün kusuru mevcut ise, bu hususu ileri sürme hakkı zarar gören bankaya ait olur. Dolayısı ile, hesap sahibinin bankaya karşı alacak hakkı devam ettiğinden bankanın ifa yardımcısı konumundaki GSM operatörünün kusurlu davranışı sebebiyle sorumluluğu gündeme gelmez.

Doktrinde ileri sürülen bir görüş uyarınca, usulsüz sim kart değişikliği durumlarında GSM operatörünün kusurunun bulunmadığını belirtmektedir[448]. Şöyle ki, yazara göre; GSM operatörlerinin doğrudan sim kart pazarlama hak ve yetkileri bulunmamaktadır. Bu sebeple son kullanıcı konumundaki abone, kullandığı sim kartlarını genellikle satış faaliyetleri yürüten bayilerden almaktadır. Bayi ise GSM operatörü ile arasındaki bayilik sözleşmesi uyarınca faaliyet yürüten (çoğu zaman tüzel) kişidir.

Ancak bazı durumlarda bankanın sorumluluğu mevzubahistir. Meselâ, internet üzerinden işlem yapmak isteyen müşterinin GSM operatörünün kusurundan (kısa mesajı iletmemesinden) işlemi gerçekleştirememesi gibi.

---

[448] **Akkanat**, s. 72 vd.; Aksi görüşde: **Andrews**, 86 vd.

B. Destek Hizmet Kuruluşlarının Davranışlarından Dolayı Bankanın Sorumluluğu

Günümüzde elektronik bankacılık faaliyetini yürüten bankanın destek hizmeti kuruluşlarının hizmetlerinden yararlanması olağan bir durumdur. Bankalar bu yolla maliyetlerini düşürmek, gelirlerini artırmak, operasyonlarının hızını ve verimliliğini artırmak, sahip olmadıkları teknoloji ve uzmanlıktan yararlanmak istemektedirler. Bankalarca destek hizmeti alımına ilişkin usul ve esaslar BDDK'nın kabul ettiği Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik'te (BDHAY) öngörülmüştür. Şöyle ki, BDHAY ile bankaların hangi tür hizmetleri banka dışından alabilecekleri ve bu hizmetler için uymaları gereken kurallar düzenlenmektedir (m. 4, f. 1).

BDHAY'ın 4. maddesinin 5. fıkrası uyarınca, "*bankalarca, hatırlatma aramaları, teknik destek ve yardım masası, gecikmiş borç bildirimleri, müşteriye hesap bilgilerinin verilmesi, müşterilerin kişisel bilgilerinin güncellenmesi hizmetleri ile kredi kartı iptali, kapatılması, aktivasyonu, limit artış ya da azalışı ile bankacılık faaliyetlerine ilişkin müşteri taleplerinin bankaya aktarılması hususlarında çağrı merkezi hizmeti alınabilir*".

Görüldüğü üzere, banka, meselâ, destek hizmeti kuruluşu ile çağrı merkezi hizmetinin veya veri güvenliğinin sağlanması konusunda anlaşabilir. Bu durumda, destek hizmeti kuruluşu bankanın ifa yardımcısı konumunda bankanın müşterisi ile olan elektronik bankacılık hizmetleri sözleşmesinden doğan bocunun ifasına katılmaktadır. Söz konusu destek hizmeti kuruluşunun kusurlu davranışı sonucunda ortaya çıkan zarardan banka sorumlu olur. Meselâ, sistem arızası sebebiyle müşterinin internet bankacılık işlemini gerçekleştirememesi gibi.

Belirtmek gerekir ki, destek hzimeti kuruluşlarının hizmetlerinden yararlanan banka için temel sorun veri güvenliğinin sağlanmasıdır. Zira bu durumda banka müşterilerine ilişkin bilgileri destek hizmeti kuruluşu ile paylaşmaktadır. Bu anlamda, BDHAY'ın 5. maddesinin 8. fıkrasındaki hüküm özel önem arz etmektedir. Buna göre; "*destek hizmeti dâhil her türlü hizmet alımlarında bankalar tarafından, banka ve müşteri sırrının güvenliğinin sağlanması için gerekli tedbirlerin alınması zorunludur. Bilgi paylaşımı veya hizmet alınan kuruluşun bilgiye erişiminin*

söz konusu olduğu durumlarda verilecek sisteme erişim, veriye erişim veya veriyi görme yetkisi işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılır. Veri güvenliğinin sağlanması için alınan hizmetin niteliğine göre, müşteri isimlerinin ve önemli nitelikteki diğer kişisel bilgilerin kodlanması, maskelenmesi, şifrelenmesi, sisteme erişim yetkisi verilmeksizin veri girişinin sistem harici bir yerde yapılması ve bu verilerin daha sonra banka tarafından kendi sistemine aktarılması, veriye erişimin kısıtlanması, veriye erişimin işin gerektirdiği en az seviyede gerçekleştirilmesi, destek hizmeti kuruluşu nezdinde müşteri verisi saklanmasının engellenmesi veya benzeri başka yöntemler kullanılır. Destek hizmeti sağlayan kuruluşlarca bankaya ve müşterilerine ait sırların korunmasına yönelik gerekli tedbirlerin alınmasını sağlamak destek hizmeti alan ilgili bankanın sorumluluğundadır".

Görüldüğü üzere, bankanın BDHAY'ın 5. maddesinin 8. fıkrasındaki hükme aykırı davranışı söz konusu olduğu durumlarda, müşterinin TBK'nın 116. maddesine başvurmasına gerek kalmaz; müşteri, TBK'nın 112. maddesine dayanarak bankaya karşı talep ileri sürebilir.

C. Personelin Davranışlarından Dolayı Bankanın Sorumluluğu

Bilindiği üzere, TBK'nın 66. ve 116. maddelerinde, yardımcı kişilerin işin görülmesi sırasında başkalarına vermiş oldukları zarara göre adam çalıştıranın sorumluluğuna ilişkin, uygulama alanları farklı olan iki ayrı düzenlemeye yer verilmiştir. Her iki düzenlemenin ortak tarafı bir kimsenin başkasının fiilerinden, kendisinin kusuru olmasa dahi, sorumlu olduğunu öngörmesidir[449]. TBK'nın 66. maddesinin uygulanması için yardımcı kişi çalıştıran ile zarar gören üçüncü kişi arasında herhangi bir hukuki, özellikle de sözleşmeye dayalı ilişki bulunmamalıdır[450]. Buna mukabil, TBK'nın 116. maddesi gereğince sorumluluğun doması şartlarından biri alacaklı ile borclu (adam çalıştıran) arasında daha önce

[449] **Tandoğan**, Mesuliyet Hukuku, s. 449.
[450] **Tandoğan**, Mesuliyet Hukuku, s. 449-450; **Oğuzman/Öz**, C. II, s. 143; **Eren**, Genel Hükümler, s. 619.

kurulmuş bir hukuki ilişki, özellikle de sözeşme ilişkisinin varlığıdır[451]. Bu anlamda, elektronik bankacılık hizmetleri sözleşmesi çerçevesinde banka personelinin davranışlarından dolayı bankanın sorumluluğunun hukuki dayanağı TBK'nın 116. maddesi olacaktr.

Uygulamada banka çalışanlarının (personelin) kusurlu davranışı farklı şekillerde ortaya çıkabilir. Meselâ, müşterilere ait kişisel bilgilere erişimi olan banka çalışanları dikkatsiz davranmış veya kötü niyetli kişilerle ortak hareket etmiş olabilirler. Bu anlamda, banka personeli, kişisel verilerin korunmasında, en az teknolojik kaynaklar kadar öneme sahiptir. Nitekim banka çalışanları banka hesaplarına yetkisiz erişimden doğan banka zararlarının oluşmasında önemli bir paya sahiptirler[452].Mesela, 2011-2012 yıllarında İstanbul ili sınırları içerisinde bulunan Bakırköy, Kadıköy, Sultanahmet ve Pendik Adliyeleri olmak üzere 4 farklı yerdeki toplam 21 ceza mahkemesi ile İstanbul Emniyet Müdürlüğü'ndeki suç dosyalarındaki veriler dikkate alınmakla yapılmış bir araştırmada, kişisel bilgilerin ele geçirilmesinde örgüt üyelerinin banka görevlileri ile işbirliği yaptığı saptanmıştır[453].ABD'de Bank of America, Wachovia ve Commerce Bank'ın şube müdürleri ve çalışanları 500.000 müşteriye ait banka hesap bilgilerini üçüncü kişilere satmakla itham edilmişlerdi[454]. Bu anlamda, basit güvenlik tedbirleri (mesela, uygun eğitim), belirli davranışlardan kaynaklanabilecek riskleri başka türlü anlayamayacak çalışanlar açısından özellikle önemlidir.

Belirtmek gerekir ki, banka çalışanlarının yalnız kasıtlı davranışları değil, ihmali de bankanın sorumluluğuna yol açabilir. Zira dürüst ve iyi niyetle hareket eden banka çalışanları bile zaman zaman bankanın sorumluluğuna yol açacak davranışlarda bulunabilmektedirler. Bir araştırmaya göre, kişisel veri kaybına neden

---

451 **Eren**, Genel Hükümler, s. 619-620.

452 **Honeywill**, **C. S.**, "*Data Security and Data Breach Notification for Financial Institutions*", N. C. Banking Inst, C. 10, S. 1, 2006, s. 278.

453 **Yiğitbaşı, İ./Gürsul, F.,** "*Online Bankacılık Suçlarının İncelenmesi: İstanbul Örneği*", Enformatik, Toplum ve Hukuk, Ed. **Gürsul, F.,** Legal Yayıncılık,İstanbul, 2016, s. 198.

454 **Honeywill,** s. 278-279.

olan olayların yüzde doksan beş oranında çalışanların kasıtsız davranışı ve çoğunlukla, özensizlik ve eğitilmemiş[455] olmalarından kaynaklanmıştır[456].

Diğer yandan, bazı banka çalışanları normal iş akışında müşterilere ilişkin kişisel verileri işlemektedirler. Bu anlamda, banka, çalışanlarının kişisel verileri kötüyü kullanmasını önlemek amacıyla bazı tedbirler almakla mükelleftir. Mesela, müşterilerin kişisel bilgilerine erişmi olan banka çalşanlarının eylemlerinin, bankanın iç kontrol sistemi tarafından denetlenmesi gerekir.

III. Yardımcı Kişilerin Fiillerinden Bankanın Sorumluluğuna İlişkin Sorumsuzluk Anlaşmalarının Geçersizliği

Borçlunun yardımcı kişilerin fiilleri için sorumsuzluk anlaşması yapma imkânı, TBK'nın 116. maddesinin 2. fıkrasında öngörülmüştür. Buna göre, TBK'nın 115. maddesinin 1. fıkrasından farklı olarak, borçlu, alacaklı ile önceden yaptığı sorumsuzluk sözleşmesinde, yardımcı kişilerinin kasıtlı veya ağır kusurlu davranışlarıyla borca aykırılıktan doğan zararlardan tamamen ya da kısmen sorumsuz olacağını kararlaştırabilir. Ancak TBK'nın 116. maddesinin 3. fıkrası ile borçluya tanınmış yardımcı kişiden dolayı sorumluluğu kaldırma veya sınırlandırma imkânı daraltılmıştır. Buna göre, uzmanlığı gerektiren bir hizmet, meslek veya sanat, ancak kanun veya yetkili makamlar tarafından verilen izinle yürütülebiliyorsa, borçlunun yardımcı kişilerin fiillerinden sorumlu olmayacağına ilişkin anlaşma kesin olarak hükümsüzdür. Sorumsuzluk anlaşmalarını ifa yardımcısının yalnız ağır kusuru bakımından hükümsüz sayan eBK'nın 100. maddesinin 3. fıkrasından farklı olarak, TBK'nın 116. Maddesinin 3. fıkrası, ifa yardımcısının kusurunun ağır veya hafif olması arasında bir fark gözetmemiştir[457]. Bu anlamda, elektronik bankacılık hizmetlerinin sağlanmasına ilişkin borcunun ifasında kullandığı ifa yardımcısının

---

[455] BBSEBHY'Nin 19. maddesinin 2. fıkrası gereğince, "*bankanın BT kaynaklarına ve sistemlerine erişimi olan yeni ve mevcut personelin ve ilgili olduğu alanlar doğrultusunda BT kaynaklarına ve sistemlerine erişimi olan dış hizmet sağlayıcıların bu eğitimlerden geçmesi veya eğitimi aldıklarını belgelendirmeleri ve eğitim programı güncellendikçe ilgili kişilerin güncellenen kısımlarla ilgili tekrar eğitim alması sağlanır*."

[456] **Honeywill,** s. 279.

[457] **Akıncı**, Borçlar Hukuku, s. 253, dn. 102.

hafif kusurundan bankanın sorumlu olmadığına ilişkin kayıtlar TBK'nın 116. maddesinin 3. fıkrası uyarınca kesin hükümsüzdür.

§ 4.Özen Yükümlülüğünün İhlalinde İspat Külfeti ve Zamanaşımı

I. İspat Külfeti

A. Genel Olarak

Bilindiği üzere, TMK'nın 6. maddesi, "*Kanunda aksine bir hüküm bulunmadıkça, taraflardan her biri, hakkını dayandırdığı olguların varlığını ispatla yükümlüdür.*" hükmünü içermektedir. Bu norm gereğince sözleşmeye dayanan sorumlulukta, sözleşmeye aykırılığı iddia eden tarafın bu iddiasını ispatlaması gerekir. Ancak maddedeki "kanunda aksine bir hüküm bulunmadıkça" ifadesi ile söz konusu ispat yükünün dağılımına ilişkin farklı düzenlemelerin gtirilmesine imkân tanımıştır. Bu anlamda, TBK'nın 112. maddesi dikkate alınmalıdır. Bu hükme göre, "Borç hiç veya gereği gibi ifa edilmezse borçlu, kendisine hiçbir kusurun yüklenemeyeceğini ispat etmedikçe, alacaklının bundan doğan zararını gidermekle yükümlüdür.". Görüldüğü üzere, TBK'nın anılan hükmü, TMK'nın 6. maddesindeki temel ispat kuralına istisna getirmiş ve kusursuzluğun ispatını borçluya yüklemiştir. Başka bir deyişle, sözleşmenin ihlâli, zarar ve illiyet bağı gibi hususları ispat yükümlülüğü alacaklı üzerindeyken, borçlu kusursuzluğunu ispatla yükümlüdür[458].

Vekalet sözleşmesinde vekilin asli borcunu, özen borcuna aykırı davrandığı için ihlâl ettiğini ispat külfeti, vekalet verene aittir. Vekalet veren, özen borcunun yerine getirilmemesinden dolayı hedeflenen neticenin ortaya çıkmadığını ispat etmeli; vekil de, sorumluluktan kurtulmak için borcun yerine getirilmemesinde bir kusuru olmadığını ispatlamalıdır[459]. Vekalet veren, özen borcunun yerine getirilmediğini ve başarılı sonucun gerçekleşmediğini ispatlayarak bu külfetini tam yerine getiremez. Ayrıca vekilin benzer alanda iş üstlenen basiretli bir vekilin

---

[458] Serozan'ın belirttiği gibi, " ... *kusur sorumluluğu ilkesi aslında borçludan yanadır. Ama bu ilke de borçlunun özensizliği kavramının nesnelleştirilmesi ve ksurusuzluğu ispat yükünü borçluya yüklemesi yüzünden borçlu yanlısı karakterini geniş ölçüde yitirmiş sayılabilir*". Bkz.: **Serozan**, İfa Engelleri, s. 134.

[459] **Başpınar**, s. 276.

davranışından uzaklaştığını ve bu uzaklaşmanın, işlerin normal akışına göre sonucun meydana gelmemesinde etken olduğunu ispatlamak zorundadır. Bu ispat yükünü yerine getiren vekalet verene karşı, vekil, kusursuz olduğunu ispatlayarak sorumluluktan kurtulabilir[460].

B. Elektronik Bankacılık İşlemleri Açısından İspat Yükünün Dağılımı

1. Genel Olarak

İhtilaflı elektronik bankacılık işlemleri bahis mevzu olduğu zaman ortaya çıkan zararlardan kimin sorumlu olduğu üzerinde banka ve müşteri arasında uyuşmazlık çıkmaktadır. Bunun yaygın örneğini, bankanın, işlemin gerçekleştirilmesi zamanı müşteri tarafından banka kartı ve şifresinin kullanıldığı yönündeki inanca sahip olması oluştrmaktadır. Bankaya göre, müşteri banka işlemini şahsen gerçekleştirmiş (ve bankaya karşı dolandırıcılık yapmış) olabileceği gibi, banka kartını veya şifresini veya hem banka kartını hem de şifresini özenle saklamak yükümlülüğünü ihlâl etmiş ve banka hesabına yetkisiz erişimin sağlanmasına ağır ihmaliye sebebiyet vermiş de olabilir. Yargıtay uygulamasına[461] baktığımızda müşterilerin banka hesaplarına yetkisiz erişimin sağlandığını ve yetkisiz kişiler tarafından banka hesaplarındaki paraların gerek ATM üzerinden gerekse de havale yolu ile diğer (yetkisiz kişilerin) banka hesabına aktarılması ile tahsil edildiğini, kredi kartları ile tanımadığı kişiler tarafından harcama yapıldığını ileri sürmektedirler. Buna mukabil, bankaların yaptığı itirazlarının temelindeki gerekçeler şunlardır: Müşterinin kişisel bilgisayarıyla ilgili önlem almadığı[462], ihtilaflı bankacılık işlemlerinin tamamının kredi kartı şifresi girilmek suretiyle gerçekleştirildiği[463], bankanın internet sisteminin yeterli güvenlik koşullarına sahip olduğu, davacının kişisel bilgilerini ve şifresini gizleme konusunda basiretli

---

460 **Yavuz/Acar/Özen**, s. 1161.

461 **Yarg. 11 HD.**, E. 2016/8699, K. 2017/5896, T. 31.10.2017; Yarg. 19. HD, E. 2016/9783, K. 2017/6467, T. 2.10.2017; **Yarg. 11. HD.**, E. 2016/7337, K. 2017/5353, T. 16.10.2017; Yarg. 19. HD., E. 2016/10698, K. 2017/6160, T. 21.9.2017.

462 **Yarg. 11. HD.**, E. 2016/2409, K. 2017/5249, T. 11.10.2017.

463 **Yarg. 19. HD.**, E. 2016/9814, K. 2017/5953, T. 18.9.2017.

davranmadığı[464], müşterinin şifre ve parolasının üçüncü kişilerin eline geçmesine sebebiyet verdiği, bankanın sağladığı ek güvenlik önlemlerinden yararlanmadığı[465] vs.

Banka hesabına yetkisiz erişim durumunda cevaplandırılması gereken soru şudur: Müşterinin banka hesabındaki paranın çekilmesi veya başka hesaba aktarılması hâlinde söz konusu işlemin müşterinin talimatı üzerine gerçekleştirilip gerçekleştirilmediğini isbat külfeti kime aittir?

Doktrinde, kural olarak, banka hesabındaki işlemin müşterinin talimatı üzerine gerçekleştirdiğini ispat yükümünün bankanın üzerinde olduğu ifade edilmektedir[466]. Şöyle ki, geleneksel bankacılık işlemleri açısından müşterinin imzasına dayanarak bankacılık işlemini gerçekleştirdiğini ileri süren bankanın, elektronik bankacılık hizmetleri açısından da müşterinin elektronik imzasının varlığını isbat etmesi gerekir.

BanKK'nın 32. maddesinin 2. fıkrası uyarınca, "*kart çıkaran kuruluş ile kart hamili arasında oluşabilecek herhangi bir uyuşmazlık hâlinde, işlemin hatasız bir şekilde kaydedildiği, hesaba intikal ettirildiği ve herhangi bir teknik yetersizlik veya arıza hâlinin bulunmadığını ispat etme yükümlülüğü kart çıkaran kuruluşa aittir*".

BBSEBHY'nin 35. maddesinin 1. fıkrasına göre, "*banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır.Kullanılan tekniğin oluşturduğu iz kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte olması sağlanır.*" Kullanılacak teknikler ve tesis edilecek kontroller gerek banka gerekse müşteri için, finansal sonuç doğuran her türlü işlemde hem işlemi başlatan hem de işlemi sonuçlandıran tarafın gerçekleştirdiği işlemleri inkâr edememesini sağlamalıdır.

Aynı zamanda, BBSEBHY'nin 38. maddesinin 3. fıkrası gereğince, *"Finansal sonuç doğuran işlemler için doğrulama kodlarının, işlemi gerçekleştirirken*

---

464 ***Yarg.11. HD.**, E. 2007/9336 K. 2009/4347 T. 09.04.2009.*

465 ***Yarg. 11. HD.**, E. 2008/3759 K. 2009/7585 T. 22.06.2009.*

466 **Geva**, **B.,** "Consumer Liability in Unauthorized Electronic Funds Transfers", CBLJ, Vol. 38, Y. 2003, s. 232; 2; **Mason**, **S.** "Electronic Banking and how courts approach the evidence", CLSR, Vol. 29, Y. 2013, 145.

müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik hâlinde bu bilgilere göre oluşturulmuş ilgili doğrulama kodunun da geçersiz hâle gelmesi temin edilir." Görüldüğü üzere, banka, tüm internet bankacılığı faaliyetleri için yeterli ve etkin bir denetim izi tutma mekanizması tesis eder. Banka asgari olarak, hesap açılışı, kapanışı ve hesapta değişiklik faaliyetlerine, finansal sonuç doğuran işlemlere, müşteri için verilen limit aşım onaylarına, internet bankacılığı sistemine erişimi düzenleyen hak, ayrıcalık ve kısıtlamalarda yapılan her türlü değişikliğe ilişkin denetim izlerini tutar. Denetim izlerinin, gerçekleşen işlemlerin başlangıcından sonuna kadar akışını ve kaynağını gösterecek detayda bilgi içermesi gerekir. Banka, internet bankacılığı faaliyetlerine ilişkin işlem ve kayıt tutma süreçlerinin ve alt yapısının, delil üretecek ve bu delillerin bozulmasını önleyecek, yanıltıcı delilleri ayırt edebilecek ve taraflara sorumluluk yüklemede kullanılabilecek bilgileri sunacak şekilde yapılanmasını temin eder. BBSEBHY'nin 3. maddesinin (ü) fıkrası gereğince, *"kimlik doğrulama, bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizmayı"* ifade eder.

Görüldüğü gibi, elektronik bankacılık işlemleri bankanın kurmakla yükümlü olduğu kimlik doğrulama mekanizmasının kontrolü altında gerçekleştirilmektedir. Elektronik bankacılık hizmetleri sunan bankanın uyguladığı kimlik doğrulama mekanizmasının müşterilerin ve personelin bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar olan tüm süreci kapsaması gerekir. Banka, kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler almalıdır. Şu durumda, müşterinin banka hesabındaki paranın yetkisiz kişiler tarafından tahsil edildiği iddiasında bulunduğu hâlde, bankanın söz konusu işlemin müşterinin kendisi yahut müşterinin ağır ihmali sebebiyle yetkisiz üçüncü kişiler tarafından gerçekleştirildiğini ispat etmesi gerekmektedir. Yargıtay'ın uygulaması da bu yöndedir. Şöyle ki, Yüksek Mahkeme'ye göre, elektronik bankacılık işlemleri sırasında kullanılan şifre ve parola gibi kişisel bilgilerin müşterinin kusuru ile ele geçirildiğinin kanıtlanamamış olması karşısında, müşterinin şifresini koruyamadığından bahisle yazılı şekilde kusur paylaşımı yapılması, yani zarara kısmen müşterinin katlanması gerektiğinin kabulü

doğru değildir[467]. Yargıtay, müşterinin ihmal ve kusuru ile şifre ve parolasını kötüniyetli üçüncü kişilere verdiği veya onların almalarına neden olduğuna dair dosyada kanıt olmaması gerekçesiyle müşterinin müterafik kusurlu olmasına ilişkin ilk derece mahkemesinin kararını isabetli bulmamıştır[468].

Belirtmek gerekir ki, uygulamada Yüksek Mahkeme'nin çoğu kez bankanın "müşteriye vermiş olduğu şifre ve parolanın müşterinin kusuru ile ele geçirildiği"ni, "müşterinin kasti veya kötü niyetli hareketlerinin zarara sebebiyet verdiği"ni, "müşterinin üçüncü kişilerle el ve iş birliği yaparak ya da başka şekilde kusurlu davrandığı"nı kanıtlayamadığı gerekçesiyle sorumlu olduğu sonucuna ulaştığını görmekteyiz[469]. Ancak şu sorunun cevaplandırılması gerekmektedir: Banka müşterinin kusurunu veya üçüncü kişilerle işbirliği yaptığını nasıl kanıtlayabilir? Bu soru, usulsüz işlemlerin internet üzerinden yapıldığı hâlde özel bir önem arzeder. Meselâ, müşterinin Türkiye'de A bankasında olan internet banka hesabının ABD'deki hacker tarafından boşaltılmasında olduğu gibi. Gerçekten de, söz konusu durumlarda bankanın müşterinin kusurunu, özellikle de üçüncü kişilerle işbirliği yaptığını ispat etmesi, deyim yerindeyse, imkânsızdır. Şu durumda, banka, aslında, uyguladığı güvenlik sisteminin kırılmaz olduğunu, yapılmış usulsüz işlemlerin bankanın güvenlik zaafiyetinden kaynaklanmadığını, bankanın aldığı güvenlik tedbirlerinin müşterinin ağır ihmali sonucu bertaraf edildiğini ispat etmek zorundadır. Başka bir deyişle, bu gibi hâllerde, banka, sorumluluktan kurtulmak için müşterinin kusurunun varlığını değil, kendi kusursuzluğunu ispat etmelidir[470].

Uygulamada bankalar, çoğu kez, ihtilaflı işlemlerin hangi saatte ve hangi IP adresinden yapıldığına ilişkin bilgileri mahkemeye sunmakta, mahkemeler de, sadece

---

[467] Yarg. 11. HD., E. 2009/14495, K. 2011/6729, T. 02.06.2011; Yarg. 11. HD., E. 2009/12002, K. 2011/5171, T. 28.04.2011; Yarg. 11. HD., E. 2008/12915, K. 2010/3753, T. 05.04.2010; Yarg. 11. HD., E. 2009/12767, K. 2011/5607, T. 09.05.2011.

[468] Yarg. 11. HD., E. 2010/10088, K. 2012/1827, T. 13.02.2012; Yarg. 11. HD., E. 2009/9420, K. 2011/2538, T. 10.03.2011; Yarg. 11. HD., E. 2009/8125, K. 2011/1159, T. 03.02.2011.

[469] **Yarg. 11. HD.**, E. 2009/13324, K. 2011/6181, T. 23.05.2011; **Yarg. 11. HD.**, E. 2011/14788, K. 2012/6188, T. 17.04.2012; **Yarg. 11. HD.**, E. 2015/13404, K. 2017/1319, T. 7.3.2017.

[470] **Reisoğlu'na** göre, bankanın teknolojinin gerektirdiği tüm tedbirleri aldığının belirlenmesi halinde şifresini kötü niyetli kişiye vermediğini, kaybetmediğini, bankanın istediği önlemleri aldığını ispat yükü müşteriye ait olur. Bkz.: Reisoğlu, C. 1, s. 1262.

bankanın sunmuş olduğu IP bilgisinden yola çıkmaktadırlar[471]. Bu sebepledir ki, doktrinde[472] bankalarca kayıt (log)[473] dosyalarının mahkemeye takdim edilmesi gerektiği savunulmuştur; zira bu durumda, bankanın web sitesinde gerçekleşmiş olan tüm olayların (bankanın sisteminin saldırıya uğrayıp-uğramadığı, müşterinin hatasının olup-olmadığı vs.) incelenmesi mümkün olmaktadır. Ancak belirtmek gerekir ki, kayıt (log) dosyaları üreten sistemler karmaşık yapıya sahiptirler ve daha iyi anlaşılabilemleri için onların çıktılarının daha fazla işlenmesi gerekmektedir. Bu nedenle log dosyalarının tahlili ve daha iyi anlaşılması amacıyla raporlama sistemlerinin kullanılması yaygındır. Kayıtlama veya raporlama sistemlerindeki herhangi bir hata, işlemin yalnış yorumlanmasına sebebiyet verebilir; meselâ, işletmeci bunun Chip ve PIN işlemi olduğunu düşünebilir, ancak gerçekte fallback[474] işlemi söz konusudur[475]. Diğer taraftan, kayıt (log) veya raporlama sistemine sızan kötü niyetli kişiler, sistem kayıtlarını değiştirebilir veya silebilirler. Zira bu sistemler, genel olarak, kimlik doğrulama sistemlerine nazaran daha az korunaklıdır[476].

---

471 **Özdilek**, Hukuk Kurultayı, s. 96; Konuyu Ceza Hukuku yönünden ele alan Erdoğan'ın da belirttiği gibi, "*Birçok yargılamada, IP bilgilerinin kaynağının güvenilir olup olmadığının araştırılması gerekirken, araştırma yapılmadığı gözlemlenmektedir. Çoğu zaman verilen IP ile ilgili sağlanan bilgilerin doğru kabul edilmesi sonucu yanlış mahkumiyet kararı verilebildiği gibi, bir çok sanık da internet bağlantılarının şifresiz olduğu ya da IP bilgisinin değiştirilmiş olabileceği savunmaları ile (başkaca delil yoksa) beraat ettikleri görülmüştür. Peki, gerçek sanıkların bıraktığı izler nerededir, ne yazık ki soruşturma makamları, bu sorunun cevabını haâlen verebilecek nitelikte değildir. Sayı üretmek zor olmadığından soruşturmanın yönünün ya da davanın seyrinin yetkisiz kimseler tarafından tutulan ve güvenli olmayan bilgiler doğrultusunda yönlendirmek verilen hükmün güvenilirliğini de tartışma konusu hâline getirir"* (**Erdoğan**, **B.,** "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?.", http://www.digisophia.com/Article/Details/61, Erişim tarihi Ocak 03, 2021).

472 **Özdilek**, Hukuk Kurultayı, s. 96; **Murdoch**, **J. S.,** "Reliability of Chip and PIN Evidence In Banking Disputes", Digital Evidence & Elec. Signature Law Rev., Vol. 6, Y. 2009, s. 108.

473 Windows, Linux gibi modern işletim sistemlerinde yapılan tüm işlemler kayıt (log) dosyaları aracılığıyla kayıt altına alınmaktadır. Bu, uygulamaların başlangıcı ve farklı sınıf hata iletilerinin de dâhil olduğu sistem hadiselerini ihtiva etmektedir. Kayıt (log) dosyalarındaki bilgiler, örneğin, yetkisiz şahısların kişisel verileri ele geçirmek amacıyla sisteme nasıl ulaşdığının belirlenmesine yardımcı olmaktadır (Bu konuda bkz.: **Stephen Mason and Daniel Seng**, Electronic Evidence, Fouth Edition, Institute of Advanced Legal Studies, London, 2017, s. 8); **Murdoch**, s. 108.

474 Chip'li bir kartın Chip'i kullanarak işlem yapılamaması durumunda manyetik şerit kullanılarak yapılan işleme fallback işlem denmektedir.

475 **Murdoch**, s. 108.

476 **Murdoch**, s. 108.

2. Bankanın İspat Yükünü Kolaylaştırıcı Araç Olarak İlk Görünüş Kanıtı (*Prima Facie Evidence*)

a. Kavram

İlk görünüş kanıtı fiili karine olmakla yasaya değil de genel yaşam deneyimlerine dayanır[477]. Fiili karine, ispat edilen bir olgudan başka bir olgunun varlığı veya yokluğu sonucunun çıkarılmasıdır[478]. Buna göre, hâkim ispat edilen bir olgunun, ispat edilecek husus için fiilî karine olup olmadığını delilleri takdir yetkisi çerçevesinde dikkate alır ve karinenin varlığı sonucuna ulaşırsa, karinenin ortaya koyduğu hususun ispatı ayrıca aranmaz[479].

İhtilaflı elektronik bankacılık işleminin, özellikle de bu işlemlerin bankanın kimlik doğrulama mekanizmasından geçmekle gerçekleştirildiği durumlarda, bankanın olguların isbatıyla ilgili ciddi zorluk yaşayacağı açıktır. Şu durumda, bankanın ispat yükümünün hafifleşmesi açısından ilk görünüş delilinden yararlanması mümkün müdür?

İlk görünüş kanıtının ihtilaflı elektronik bankacılık işlemlerine uygulanmasının sonucunu şöyle özetleyebiliriz: Kimlik doğrulama mekanizmasından geçmekle yapılan bankacılık işlemlerinin müşterinin kendisi veya yetkilendirilmiş üçüncü şahıs veya müşterinin önceki seçenekleri (yani işlemi kendisinin veya yetkilendirdiyi üçüncü şahıs tarfından yapılmasını) inkar etmesi durumunda müşterinin ağır ihmali ile yetkisiz üçüncü şahıslar tarafından yapıldığının kabulü gerekir.

Yargıtay uygulamasına baktığımızda, bankaların açıkça ifade etmemelerine rağmen, bankanın kullandığı kimlik doğrulama mekanizmasının üst düzey standartlara uygun olduğunu ileri sürmekle aslında ilk görünüş kanıtından yararlanmak istediklerini görmekteyiz[480].

---

477 **Serozan**, Medeni Hukuk, s. 21.
478 **Oğuzman/Barlas**, s. 345.
479 **Oğuzman/Barlas**, s. 346.
480 **Yarg. 19. HD.**, E. 2007/2343, K. 2007/7377, T. 12.07.2007 kararına konu olan olayda, davalı bankanın itirazının gerekcesi "*internet bankacılığı işlemlerinde müşteri numarası şifre ve parolanın doğru girilmesi durumunda hesaba ulaşıldığı, dava konusu havale işlemlerinde davanın bu kişisel bilgileri kullanılarak havale işleminin gerçekleştirildiği, bankanın sisteminden davacının bu kişisel bilgilerinin ele geçirilmesinin mümkün olmadığı*" şeklinde ifade edilmişti;

b. Yabancı Mahkeme Kararlarında İlk Görünüş Kanıtı (*Prima Facie Evidence*)

Yabancı mahkeme kararlarına baktığımızda özellikle ATM'den banka kartlarının kullanılması ile gerçekleştirilen işlemler açısından ispatı kolaylaştırıcı bir araç olan ilk görünüş kanıtından yararlanıldığını görmekteyiz. Şöyle ki, kural olarak, şifreyi bilmeden elektronik bankacılık işleminin gerçekleştirilmesi imkânsızdır. Bu nedenle Alman Federal Mahkemesi (BGH) bazı kararlarında[481] söz konusu durumlarda kart sahibinin özen yükümlülüğünü ihlâl ettiği sonucuna varmıştır.

Alman Federal Mahkemesi (BGH) 5 Ekim 2004 tarihli XI ZR 210/03 sayılı kararında[482] ispat yükü ve ilk görünüş ispatına ilişkin değerlendirmeye yer vermiştir. Karara konu olan olayda, 23 Eylül tarihinde saat 15:00-17:00 arası davacının banka kartı yöresel festivalde çalınmış, aynı gün iki farklı bankaya ait ATM'den iki kez (her biri 500 Alman markı olmakla), ertesi gün ise bir defa (1000 Alman markı miktarında) para çekme işlemleri gerçekleştirilmiştir. Davacı şifresini banka kartının üzerine yazmadığını, cep telefonunda not ettiğini, cep telefonun ise çalınmadığını bildirmiştir. Alman Federal Mahkemesi alt derece mahkemesinin davanın reddine ilişkin kararını onamıştır. Mahkemeye göre; banka kartlarından sui-istimal hâllerinde bankalar ilk görünüş kanıtına dayanabilirler. Şöyle ki, ATM'den para çekme işleminin çalınmış banka kartı ve doğru PIN şifresi kullanılmakla, kartın çalınmasından kısa bir zaman sonra, gerçekleştirildiği durumda, ilk görünüş kanıtı karinesinin uygulanması ve kart sahibinin şifresini banka kartının üzerinde yazması veya banka kartı ile birlikte saklaması sonucuna varılmalıdır. Mahkeme, davacının PIN şifresinin üçüncü kişiler tarafından elde edilmesinin teorik ve pratik bakımdan mümkün olduğuna dair itirazını, üçüncü kişi tarafından banka kartının orjinalinin ve

---

Yarg. 11. HD., E. 2014/7100, K. 2014/14305, T. 23.09.2014 kararına konu olan olayda davalı banka "*güncel teknolojik güvenlik tedbirlerini aldığını, davacının gerekli güvenlik önlemlerini almadığını savunarak*" davanın reddini istemiştir.

481 BGHZ 145, 337 = NJW 2001, 286, 287 BGHZ 160, 308 = NJW 2004, 3623, 3624, **Karolin, L.,** Grazhdansko-Pravovaya Otvetstvennost Bankov v Raschetnıx Pravootnosheniyax Po Zakonadatelstvu Germanii i Rossiyskoy Federachii, Sravnitelno-Pravovoy Aspekt, Prospekt Yayımevi, Moskva, 2017, s. 148, dn. 235'ten naklen.

482 Kararın ingilizce metni için bkz.: Digital Evidence & Elec. Signature Law Rev., Vol. 6, Y. 2009, s. 248-254.

doğru PIN şifresinin kullanılmakla para çekme işleminin yapılmasının kart sahibinin ağır ihmali dışında izahının olmaması gerekçesiyle kabul etmemiştir[483].

Ancak Avrupa Birliği Ödeme Hizmetleri Direktifi'nin Alman Hukuku'na aktarılmasından sonra BGB'ye ödeme talimatının kimlik doğrulamasına ilişkin ispat yükünü öngören § 675/w ilave edilmiştir. Anılan hükme göre, ödeme işleminin kimlik doğrulaması çekişmeli ise, kimlik doğrulaması olgusunu, ödeme işleminin kayıt altına alınmasını, hesap kayıtlarını ve ödeme işleminin teknik açıdan başarıyla gerçekleştirildiğini ispat yükü bankaya aittir.

Maddenin 3. fıkrası özel bir önem taşımaktadır. Buna göre; ödeme işlemi kimlik doğrulama yöntemi ile başlatılmışsa, kimlik doğrulama yönteminin kayıt altına alınmış olması tek başına aşağıdaki hususları onaylamak için yeterli değildir: Müşteri ödeme işlemini yetkilendirmiştir; hileli davranmıştır, § 675/l'de öngörülmüş yükümlülüklerinden birini veya bir kaçını ihlâl etmiştir; kişisel bilgilerinin verilmesi ve kullanılması şartlarından birinin veya bir kaçını kasten veya ağır ihmali ile ihlâl etmiştir.

BGH, 26 Ocak 2016 tarihli bir kararında[484], BGB § 675/w'nin 3. fıkrasının ilk görünüş kanıtını dışlamadığını, ancak ilk görünüş kanıtını özel kriterlere tabi tuttuğunu ifade etmiştir. Mahkemeye göre, özel kriterlere şu hususlar dâhildir:

Banka;

1. Genellikle, pratik olarak kırılmaz güvenlik sistemine sahip olduğunu;

2 İhtilaflı işlemin gerçekleştirildiği anda sistemin düzgün kullanıldığını ve hatasız çalıştığını, ispatla mükelleftir.

BGH, daha sonra, internet bankacılığında kimlik dorğulama mekanizmasının kırılmaz olmasına açıklık getirmiştir; Mahkemeye göre, kimlik doğrulama mekanizmasının kırılmaz olması için;

---

[483] German Civil Code, Bürgerliches Gesetzbuch (BGB), Volume I, Books 1-3: Paragraph 1-1296, Article-by-Article Commentary, edited by Gerhard Danneman Reiner Schulze, Nomos, 2020, s.1324.

[484] BGH, XI ZR 91/14, kararın ingilizce özet metni için bkz.: Digital Evidence & Elec. Signature Law Rev., Vol. 15, Y. 2018, s. 95-97.

1) Kullanılmış cihazların güvenilirliğinin bozulmasından etkilenmemiş olması;

2) Yetkisiz kişilerin iletişim ağlarına erişimi engellenmiş olması;

3) TAN (işlem doğrulama kodu) özel işleme bağlanmış olması gerekmektedir.

Sistemin kırılmaz olduğunu kanıtlamak yükü bankaya aittir. BGH'ye göre, söz konusu talepler incelenmiş ve karşılanmış olmadıkça, PIN ve TAN kullanıldığına ilişkin belgelerin mevcudiyeti, elektronik bankacılık işleminin yetkili kişi tarafından gerçekleştirildiğini tasdikleyen ilk görünüş kanıtı (prima facie evidence) olarak kabul edilemez.

Doktrinde[485] belirtildiği üzere adı geçen fıkranın BGB'ye eklenmesinden sonra yukarıda değinilen BGH uygulaması büyük ölçüde güncelliğini kaybetmiştir. Ancak PIN şifresi dâhil edilmekle yapılmış işlemler bakımından ilk görünüş kanıtının uygulanması devam etmektedir[486].

Avusturya Yüksek Mahkemesi 29 Haziran 2000 tarihli bir kararında[487] işlemin orjinal banka kartı ve PIN şifresi kullanılmakla yapılmasının bankacılık işleminin müşterinin kendisi tarafından şahsen veya müşterinin kusuru ile üçüncü kişi tarafından gerçekleştirildiğinin kabülü için kuvvetli belirti olarak değerlendirmiştir. Ancak Mahkeme anılan davada, işlemin orjinal banka kartı kullanılmakla gerçekleştirildiğini ispat edememesi sebebiyle bankanın itirazını reddetmiştir.

Norveç Trondheim Bölge Mahkemesi 20 Eylül 2004 tarihli bir kararına[488] (Jorgensen davası) konu olayda, Jorgensen'e ait iki aded sırt çantası 4 Ağustos 2001

---

485 **Karolin**, s. 149.

486 BGH NJW 2012, 1277, Urteil vom 29.11.2011-XI ZR 370/10; BGH, Urteil vom 26/01/2016, Az. XI ZR 91/14, **Karolin**, s. 149, dn. 236'dan naklen.

487 OGH Urteil vom 29.6.2000, 2 Ob 133/99v, Kararın ingilizce özet metni için bkz.: Digital Evidence & Elec. Signature Law Rev., Vol. 5, Y. 2008, s. 141.

488 Kararın ingilizce metni için bkz.: Digital Evidence & Elec. Signature Law Rev., Vol. 9, Y. 2012, s. 117-123. Karar doktrinde Nuth tarafından eleştirilmiştir. Yazara göre; tüketiciler ağır ihmallerinin bulunmadığını ispat etmek için sınırlı imkânlara sahiptirler. Müşteriler, bankanın kullandığı güvenlik sistemi hakkında herhangi bir bilgiye sahip değiller. Buna mukabil, banka olguların araştırılması veya isbatına ilişkin gereken imkânları hazidir. Aynı zamanda, Banka, banka kartlarında uygulanan güvenlik derecesini belirlemiştir. Karara konu olan olay gibi şüpheli

tarihinde İspanya'da çalınmıştı. Çantalarda Jorgensen'e ait kişisel eşya ile birlikte banka kartlarının da bulunduğu cüzdan vardı. Çantalar saat 15:00-15:20 arası çalınmış, nakit para çekme işlemleri 16:13, 16:14, 16:15 ve 16:19'da gerçekleştirilmişti. Mahkeme'ye göre; davacının itirazına rağmen zaman faktörü davaya konu olan olay açısından önem arz etmektedir. Şöyle ki, yetkisiz kişiler tarafından yapılan işlemler kartların çalınmasından bir saat sonra gerçekleştirilmiştir. Dava dosyasında bulunan yetkilendirmeye ilişkin deliller doğru PIN'in ilk girişimde dâhil edildiğini kanıtlamaktadır. Bu, şifrenin kolayca erişilen olduğuna ve kartla birlikte saklandığına delil teşkil eder. Mahkeme'nin görüşüne göre; PIN'in kırılması ihtimali teorik açıdan her zaman mümkündür. Ancak davaya konu olan olayın şartları açısından şifrenin kısa bir sürede kırılması imkânsızdır. Bu sebeple, Mahkeme şifrenin banka kartıyla birlikte muhafaza edildiği, yani Jorgensen'i ağır ihmalinin olduğu sonucuna ulaşmıştır.

Letonya Yüksek Mahkemesi'nin 20 Şubat 2002 tarihli bir kararına[489] konu olayda, müşteriye ait banka hesabından Polonya'da farklı ATM'lerden nakit para çekimi işlemi gerçekleştirilmişti. Müşteri söz konusu işlemlerin usulsüz olduğunu ileri sürmüş ve çekilmiş paranın banka tarafından iadesini talep etmiştir. Mahkemeye göre; kart hamili bankanın elektronik ödeme sistemini belirlemek veya sistem üzerinde etkide bulunmak imkânına sahip değildir. Bu nedenle, sistem güvenlik mekanizmasının etkisiz hâle getirilmesinde veya ödeme talimatının oluşumu için gereken şartların suistimalinde müşterinin kusurunun varlığını ispat yükümlülüğü bankaya aittir. İspat yükünün müşteriye doğru yer değiştirmesi şu hâlde mümkündür ki, bankanın güvenlik mekanizmasının salt müşterinin bilgisi veya müşterinin kusuru sonucunda etkisizleştirildiği saptanmış olsun. Sonuç olarak; müşterinin kusursuzluğunu ispat edememesi durumunda, bankanın sorumluluğu tam veya müşterinin kusur derecesine bağlı olarak kısmen istisna edilecektir.

---

durumlarda, müşteriye değil, bankaya doğru eğilim gösteren mahkeme, bununla zayıt taraf olan müşteriyi değil, güçlü bankayı korumuştur. Bkz.: **Nuth**, **M. S.,** "Unauthorised Use of Bank Cards With or Without The PIN: A Lost Case For The Customer?", Digital Evidence & Elec. Signature Law Rev., Vol. 9, Y. 2012, s. 98.

489 Kararın ingilizce özet metni için bkz.: Digital Evidence & Elec. Signature Law Rev., Vol. 5, Y. 2008, s. 143-145.

c. Yargıtay'ın Görüşü

Yargıtay'ın kredi kartı şifresi kullanılmakla nakit para çekiminin gerçekleştirildiği işlemler bakımından bankanın sorumlu olmadığı yönünde kararları vardır. Meselâ, 05.07.2017 tarihli bir kararında Yüksek Mahkeme, ortaya çıkan zarardan tarafların eşit oranda kusurlu oldukları sonucuna varmış alt derece mahkemesinin kararını "*Davacının kredi kartının, şifre kullanılarak nakit çekim için kullanıldığı anlaşılmaktadır. Somut olayda davalı bankaya atfedilebilecek bir kusur olmadığından yazılı şekilde karar verilmesi doğru olmamıştır*" gerekçesiyle bozmuştur[490].

Yargıtay 11.12.2013 tarihli diğer kararında[491] kart sahibine ait şifrenin kullanılmakla yapılmış olan işleme göre bankanın sorumlu olmadığına ilişkin görüşünü şöyle gerekcelendirmiştir: *"... dava konusu olayda da, para çekme işlemlerinin davacı kart sahibine ait şifrenin kullanılması suretiyle yapılmış olması nedeniyle, gerek açıklanan yasa hükümleri, gerekse imzalanan sözleşme gereğince, kartın üçüncü kişilerce kullanımından davacı kart sahibinin sorumlu olduğunun kabulü gerekir. Davacının kartının şifresine ulaşılmış olması, şifrenin güvenli bir şekilde seçilmediğini ya da muhafaza edilmediğini göstermektedir. Kaldı ki, dosya kapsamındaki delillerden dava konusu kartın çalındığı ya da kopyalandığı yönünde bir bulguya da rastlanmadığı anlaşılmaktadır*".

Yargıtay, " *... kredi kartı sahibi yasa ve sözleşme hükümleri gereğince, Bankayla sözleşme imzaladığı ve kartın zilyetliğine geçtiği andan itibaren kendisine tevdi edilen kredi kartını ve bu kartın kullanımıyla ilgili bilgileri koruma ve saklamayla yükümlü olup, davaya konu olayda da kartın fiziken kullanılmadığı, söz konusu işlemlerin, bilgisayarla intrnet ortamı üzerinden ve davacı kart sahibine ait şifrenin kullanılması suretiyle yapılmış olması sebebiyle davacının sorumluluğu bulunmaktadır*" gerekçesiyle alt derceli mahkemenin kararını bozmuştur[492].

---

490 **Yarg. 19. HD.,** 2016/10693, K. 2017/5620, T. 05.07.2017.

491 **Yarg. 13. HD.,** E. 2013/22035, K. 2013/31177, T. 11.12.2013

492 **Yarg. 13. HD.,** E. 2012/9364, K. 2012/12757, T. 17.05.2012; Yargıtay diğer bir kararında, "... Davacının kartının şifresine ulaşılmış olması, şifrenin güvenli bir şekilde seçilmediği ya da muhafaza edilmediğini göstermektedir. Kaldı ki, dosya kapmasındaki delillerden dava konusu kartın çalındığı veya kopyalandığı yönünde bir bulguya rastlanmadığı anlaşılmaktadır. ... Bu durumda, kartın hukuka aykırı kullanımında ağır kusuru olan davacının, bankaca kendisine

Belirtmek gerekir ki, Yargıtay'ın doğru şifre kullanılmakla internet üzerinden gerçekleştirilmiş işlemlerde davacının/hesap sahibinin kusurunun varlığının banka tarafından ispat edilmesi gerektiği, yani salt doğru şifrenin kullanılmasının ilk görünüş kanıtı oluşturmadığı yönünde kararları da vardır. Meselâ, Yüksek Mahkeme 11 Eylül 2017 tarihli bir kararında[493] alt derce mahkemesinin kararını şu gerekçe ile bozmuştur: *"... dava konusu havale işleminin, dvacının internette bankacılık işlemlerini gerçekleştirmekte kullandığı şifre ile yapıldığı, bu şekilde gerçekleştirilen havalelerde bankanın ayrıca davacıdan teyit almasının gerekmediği, davalı bankanın bir kusurunun bulunmadığı gerekcesiyle davalı banka yönünden davanın reddine karar verilmiş isede, davacıya ait mevduat, davalı bankaya karşı gerçekleştirilen sahtecilik işlemi ile hesaplardan çekilerek başka hesaplara havale edilmiş olup, bu durum davalı bankayı aldığı mevduatı iade etme yükümlülüğünden kurtarmayacağı gibi, ispat yükü kendisinde olan davalı banka, davacıya vermiş olduğu şifre ve parolaların davacının kusuru ile üçüncü kişilerce ele geçirildiğini de kanıtlayamamıştır*".

II. Zamanaşımı

TBK'nın 146. maddesi gereğince, kanunda aksine bir hüküm bulunmadıkça, her alacak on yıllık zamanaşımına tabidir. TBK'nın 147. maddesinin 5. fıkrasına göre; vekalet, komisyon ve acentalık sözleşmelerinden, ticari simsarlık ücreti alacağı dışında, simsarlık sözleşmesinden doğan davalar beş yıllık zamanaşımına tabidir.

Elektronik bankacılık sözleşmesine vekalet sözleşmesine ilişkin hükümler uygulandığından, söz konusu sözleşmeden doğan talepler 5 yıllık zamanaşımına tabidir.

Elektronik bankacılık hizmetleri sözleşmesinin bir tarafının tüketici olması durumunda, TKHK'nın ilgili hükümlerinin uygulanması gerekir. TKHK'ya göre, "*hizmet, bir ücret veya menfaat karşılığında yapılan ya da yapılması taahhüt edilen*

---

bildirim yapıldığı tarihe kadar olan harcamalardan ve nakit çekimlerden sorumluluğu bulunmaktadır. " gerekcesiyle alt derece mahkemesinin kararını bozmuştur (**Yarg. 13. HD.**, E. 2013/22035, K. 2013/31177, T. 11.12.2013).

493 **Yarg. 11. HD.**, E. 2017/2386, K. 2017/4206, T, 11.09.2017.

mal sağlama dışındaki her türlü tüketici işleminin konusunu" ifade eder (m. 3/b.d). Bu anlamda, elektronik bankacılık hizmetlerinin anılan hüküm kapsamına dâhil olduğu açıktır.

Elektronik bankacılık hizmeti sunan bankanın özen yükümlülüğünü ihlâl etmesi durumunda ayıplı hizmet sağladığı gündeme gelebilir. TKHK'nın 16. maddesi ayıplı hizmetten doğan sorumluluğun tabi olduğu zamanaşımına ilişkin hükümleri içermektedir. Buna göre, "*kanunlarda veya taraflar arasındaki sözleşmede daha uzun bir süre belirlenmediği takdirde, ayıplı hizmetten sorumluluk, ayıp daha sonra ortaya çıkmış olsa bile, hizmetin ifası tarihinden itibaren iki yıllık zamanaşımına tabidir*". Ancak ayıp, ağır kusur ya da hile ile gizlenmişse zamanaşımı hükümleri uygulanmaz.

Görüldüğü gibi, tüketiciye ayıplı hizmet sağlanması durumunda, TKHK'nın 16. maddesinin 1. fıkrasında öngörülmüş zamanşımı süresi TBK'nın 147. maddesinin 5. fıkrasına nazaran daha kısadır. Bu hâlde, TBK'nın 147. maddesinin 5. fıkrasındaki 5 yıllık zamanaşımının uygulanması gerekir. Zira TKHK'nın 16. maddesinin 1. fıkrasındaki 2 yıllık zamanaşımının kanunlarda veya sözleşmede daha uzun bir süre belirlenmediği takdirde uygulanabileceği hükme bağlanmıştır.

SONUÇ

Mevzuat açısından baktığımızda elektron bankacılık ilk kez Bankacılık Düzenleme ve Denetleme Kurulu tarafından çıkarılan, 15.03.2020 tarihli, 31069 sayılı RG.'de yayımlanmış Bankalarda Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğinin (BBSEBHY) 3.maddesinin 1. fıkrasının (l) bendinde tanımlanmıştır. Söz konusu madde uyarınca, *"elektronik bankacılık hizmetleri: İnternet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını"* ifade ediyor. Fikrimizce, daha kısa ve net tanımlayacak olursak , elektronik bankacılık, bankacılık hizmetlerinin her türlü elektronik vasıtalar aracılığıyla verilmesi şeklinde tanımlanabilir.

Çalışmada varılan sonuçlardan biri de, banka dolandırıcılıklarının çok büyük bir kısmı *phising* ismiyle anılan bir online dolandırıcılık yöntemiyle gerçekleştiriliyor. Bu yöntemde dolandırıcılar bankanın web sitesini taklit ederek kullanıcıları kendilerinin yarattığı sahte siteye çekiyor, kişisel bilgileri elde etmiş oluyor ve aracı üçüncü kişileri kullanmakla banka müşterilerinin hesaplarındaki parayı çalabiliyorlar.

Bankaların ekonomik gücü ve elektronik bankacılığını başlatan ve idare eden taraf olmaları sebebiyle dikkat edilmesi gereken hususlar ve alınması gereken önlemler bankaca tespit edilmelidir. Teknolojik şartlardaki değişmelere paralel olarak bankalar da bu tedbirleri geliştirmeli ve değiştirmelidir. Kanımızca dijitalleşen günümüzde gerekli tedbir almanın boyutu değişmeli, şöyle ki, elektronik bankacılık hizmeti veren bankalardan müşterilerine ücretsiz bir anti-virüs programı tahsis etmesi, internet güvenliğini sağlaması ve bu esnada buna ilişkin teknik güncellemeleri ücretsiz erişime açması beklenmektedir. Diğer taraftan, müşterinin banka hesabına kötü niyetli kişiler tarafından erişilmesi veya ATM'den yetkisiz kişiler tarafından para çekilmesi gibi durumlarda, işbu doktora tezinde savunduğumuz görüş uyarınca, ortaya çıkan zarar bankaya ait olduğundan, yani

müşterinin bankaya karşı alacak hakkı devam ettiğinden sorumsuzluk anlaşmasına başvurulması söz konusu olmayacaktır.

Müşteri daha sonra internet bankacılığı hizmeti talebinde bulunursa, banka gerekli bilgilendirmeyi müşteri ile sözleşme kurulurken yaptığını ve sözleşmenin bir örneğinin de müşteride bulunduğunu gerekce göstererek müşteriyi bilgilendirmek zorunda olmadığını ifade edebilir mi? Bizce, bankanın böyle bir itirazda bulunması haklı sayılamaz. Zira, "BBSEBHY'in 37. maddesinin 1. fıkrası, banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnai durumlarda ilgili olarak açık bir şekilde bilgilendirilir" hükmünü içermektedir. Bize göre, anılan hüküm elektronik bankacılık hizmetlerinden yararlanmak isteyen müşterilerin bu taleplerini gerek banka ile sözleşme kurulduğu, gerekse de sözleşme kurulduktan sonraki bir aşamada ifade ettikleri hâlleri kapsamaktadır. Zira hükümde yer alan "elektronik bankacılık hizmetlerinden yararlanacak müşterilerin" ibaresini geniş yorumlamakla bu sonuca ulaşmamız mümkündür.

Taraflar arasında elektronik bankacılık hizmetlerinin kurulması ile birlikte, alternatif dağıtım kanallarının kullanılmasına ilişkin şartlar banka ve müşteri arasındakı diğer sözleşme (meselâ, mevduat sözleşmesi) ilişkisinden doğan hak ve yükümlülüklerle yan yana mevcut olmaya devam eder. Başka bir ifadeyle, banka, borç ilişkisi çerçevesinde sunduğu hizmetlerin geleneksel değil, alternatif dağıtım kanalları aracılığıyla sağlanması yükümlülüğü altına da girmiş olur. Sonuç itibariyle, kavramsal olarak farklı bir sözleşme olan elektronik bankacılık hizmetleri sözleşmesi, alternatif dağıtım kanallarının kullanılması şartlarını banka ve müşteri arasında kurulmuş daha kapsayıcı bir sözleşmeyle bütünleştirmiş olmaktadır.

Çalışmada aynı zamanda kart hamilinin ağır ihmalinin varlığı hâlinde, BKartK'nın 12. ve 16. maddeleri uygulaması ile ilgili fikirler yer alır. Söz konusu ağır ihmalin varlığı hâlinde BKartK'nın 12. ve 16. maddeleri uygunır ve haksız kullanım sonucunda ortaya çıkan zarara kart hamili katlanır. Şöyle ki, banka kartının kaybolması veya çalınması hâlinde, durumdan haberdar olan kart hamilinin bankaya derhal bildirimde bulunmaması, ağır ihmal olarak nitelendirilebilir. Bize göre, bu (yani müşterinin bildirimde bulunması gereken andan bildirimde bulunduğu ana kadar yirmidört saatlik sürenin bitmediği) ihtimalde dahi, yüzelli türk lirası

miktarındaki sınırlı sorumluluk uygulama alanı bulmaz, zarara müşterinin tek başına katlanması gerekir.

Uygulamada banka ve GSM operatörü arasında yapılan sözleşmelerde genelde, banka tek kullanımlık şifreyi göndermek ve hesap sahibine iletilecek kısa mesajların ücretini ödemek yükümlülüğünü taşımaktadır. Banka, müşteri ile akdettiği elektronik bankacılık hizmetleri sözleşmesi çerçevesinde kısa mesaj ücretlerini müşteriye yansıtabilir. GSM operatörünün asli edim yükümlülüğü, işlem doğrulama kodunu içeren kısa mesajların hesap sahibine en kısa zamanda ulaşmasını sağlamaktır. Bu anlamda, hesap sahibi, taraf olmadığı (banka ile GSM operatörü arasında kurulmuş) sözleşmeye dayanarak GSM operatörüne karşı talepte bulunamaz; banka ile GSM operatörü arasında kurulmuş sözleşme tam üçüncü kişi yararına bir sözleşme niteliğini haiz değildir. Varılan sonuç odur ki, GSM operatörünün kısa mesajları hesap sahibine iletme yükümlülüğü banka ile yaptığı sözleşmeden doğmaktadır.

Müşterinin banka hesabına kötü niyetli kişiler tarafından erişilmesi veya ATM'den yetkisiz kişiler tarafından para çekilmesi gibi durumlarda, işbu doktora tezinde savunduğumuz görüş uyarınca, ortaya çıkan zarar bankaya ait olduğundan, yani müşterinin bankaya karşı alacak hakkı devam ettiğinden sorumsuzluk anlaşmasına başvurulması söz konusu olmayacaktır. Zira TBK'nın 115. ve 116. maddeleri ancak başkasının malvarlığında doğan bir zarar nedeniyle var olan sorumluluğu kaldırma imkânını ve bunun sınırlarını ele alır, yoksa kendi malvarlığında doğmuş olan bir zarar için kişinin kendi kendine sorumsuzluk anlaşması yapması düşünülemez.

Fikrimizce, kredi kartı sözleşmesinin hizmet sözleşmesi olarak nitelendirmek isabetli olmaz. Şöyle ki, hizmet sözleşmesi acısından geçerli olan bağımlılık ilişkisi kredi kartı sözleşmesinde bulunmamaktadır. Zira bankanın, müşterinin denetimine bağlı olarak çalışması söz konusu değildir.

Sonuç itibairyle, elektronik bankacılık hizmetleri sunan bankanın teknoloji bazlı riskleri, özellikle de güvenlik risklerini belirlemesinde ve yönetiminde, basiretli tacir gibi davranması gerektiği söylenebilir. Nitekim Yargıtay da, bir çok kararında, elektronik bankacılıkta gerekli güvenlik tedbirlerinin alınmasına ilişkin sorunları değerlendirirken bankanın basiretli tacir gibi davranması gerektiğinden hareket

etmiştir. Bankanın sözleşme öncesi bilgilendirmenin sözleşmenin akdedilmesinden ne kadar süre önce yapılması gerektiğine ilişkin herhangi bir kural mevzuatta öngörülmemiştir. Ancak sözleşme öncesi bilgilendirmenin, adından görüldüğü üzere ve işlevi gereği, müşterinin sözleşmenin kurulmasına ilişkin iradesini açıklamasından önce yapılması gerektiği açıktır. Mevzuatta somut bir sürenin öngörülmemesinin sebebi, sözleşmenin kurulma anı ile aydınlatıcı bilgilerin verilmesi anları arasında bulunması gerekli zaman aralığının ne olacağı konusunda önceden belirli bir mutlak yasal ölçünün konulmasının çok güç olmasıdır. Bu anlamda, müşterinin bilgilendirilmesi yükümlülüğünün yerine getirildiğini söyleyebilmek için her somut olayın özelliklerinin göz önünde bulundurulması ve ona göre sonuca varılması uygun görünmektedir. Eğer müşteriye serbest şekilde, bilinçli olarak sözleşmenin kurulması hakkında karar vermek için gereken bütün bilgiler yeterli bir zaman dilimi içerisinde verilmişse, bankanın kurala uyduğu söylenebilir.

Böylece bankanın websitesi ya hiç çalışmamakta veya yavaş çalışmaktadır. Bu gibi durumlarda, bankanın edimini gereği gibi ifa ettiği söylenemez. Bu sebeple, müşteri bir zarara uğramışsa, zararını ispat etmesi hâlinde banka sözleşmenin ihlâli sebebiyle söz konusu zararları tazmin etmek zorundadır. Teknolojik gelişmelerin ve tehlikelerin devamlı inkişafı karşısında bu yükümlülüğün dinamik nitelik taşıdığı dikkate alınmalıdır. Başka bir deyişle, banka kendi güvenlik sistemini (bilgisayar yazılımlarını) değişen standartlara uygun hâle getirmek zorundadır, aksi durumda, bankanın özensiz davrandığı söylenebilir. BİSHY'nin 11. maddesinin 3. fıkrası gereğince, bilgi sistemlerinin güvenilirliğinin sağlanması ve düzenli olarak güncellenerek gerekli değişikliklerin yapılması zorunludur.

Belirtmek gerekir ki, bankaların bilgisayar sisteminin mükemmel olması itimalinde dahi müşterilerin internet bankacılığı hizmetlerinden yararlanmak için kullandıkları bilgisayarların belirli düzeyde güvenlik taleplerine cevap vermesi gerekmektedir. Söz konusu bilgisayarların bir bölümünün müşterilerin aile bireyleri tarafından farklı amaçlar doğrultusunda kullanılan ev bilgisayarı olması dikkate alındığında anılan yükümlülüğün önemi daha da artmaktadır.

Uygulamada bankalar internet bankacılık hizmetlerinden yararlanmak isteyen müşterilerin kendilerinin gerekli donanım ve yazılım programının (firewall, anti virüs programları, internet koruma programları gibi) bulunmasnı talep etmektedir.

Sözkonusu denetimin uygulanabilmesi için ilave donanım ve yazılım yapılanmasına ihtiyaç olduğu açıktır. Ancak müşterilerin, özellikle de tüketicilerin ileri seviyede güvenlik tedbirleri alma konusunda yeterince bilgi sahibi olduğu söylenemez. Bu anlamda, güvenlik açısından müşterinin bilgisayarında orta düzeyde bir bilgisayar kullanıcısının kullanabileceği nitelikte bir lisanlı antivirüs programı bulunması gerekir. Aksi takdirde, müşterilerin çok az kısmının bankanın talep ettiği seviyede güvenlik önlemi aldığı söylenebilir. Bu durum müşterilerin yetkisiz kişilerce yapılmış işlemlerden dolayı sorumlu tutulmasıyla sonuçlanırdı.

Yetkisiz kişiler tarafından yapılan elektronik bankacılık işlemleri açısından "müşterinin ortak kusuru" kavramının kullanılmasının isabetli olup-olmadığı zararın müşterinin mi, yoksa bankanın mı malvarlığında doğduğu ile ilgilidir. Zira zararın bankanın malvarlığında meydana geldiği görüşünün kabulü durumunda müşterinin ortak kusurundan bahsedilmesi mümkün görünmemektedir. Buna karşılık, zararın müşterinin malvarlığında doğduğu fikrinin kabulü durumunda, müşterinin ortak kusurunun dikkate alınacağı söylenebilmektedir. Bu açıdan baktığımızda, yetkisiz kişiler tarafından müşterinin kredi kartından para çekilmesi veya internet bankacılığı üzerinden havale yapılması gibi durumlarda ortaya çıkan zararın banka yahut müşterinin malvarlığında doğduğunun belirlenmesi önem arz etmektedir. Doktrinde hâkim görüş ve Yargıtay uygulaması bu gibi durumlarda zararın bankanın malvarlığında ortaya çıktığı yolundadır. Buna mukabil, doktrinde savunulan diğer bir görüş uyarınca, kişisel bilgilerin kullanıcının kusuru ile üçüncü kişinin eline geçip geçmediği dikkate alınarak bir ayrım yapılmalıdır. Şöyle ki, kişisel bilgilerin üçüncü kişilerin eline geçmesinde kullanıcının bir kusuru yoksa doktrinde hâkim olan görüşe katılmak gerekir. Ancak kullanıcının kusurunun varlığı durumunda, kimlik doğrulama verilerini müşteriden ele geçiren dolandırıcı, sahte değil, doğru ve gerçek bilgileri girmekte ve bankanın sistemi tarafından müşteri (veya yetkili temsilci) gibi algılanmaktadır; bu anlamda, rizikonun yine de bankaya ait olduğu ve zararın onun malvarlığında gerçekleştiği söylenemez. Diğer bir deyişle, müşteri sistemin kendi tarafındaki ucunu korumakla mükelleftir, söz konusu ödeve kusurlu aykırılığın sonuçlarına müşteri katlanmalıdır.

Yargıtay uygulamasına baktığımızda, Yüksek Mahkeme'nin bazı kararlarında "müşterinin ortak kusuru" kavramına yer verdiğini görüyoruz. Şöyle ki, Yargıtay

bazı kararlarında, "*davacının güvenliği sağlayıcı tedbirler almadığı*", "*davacının kimsenin bilmemesi gereken ve korumakla yükümlü olduğu şifresi gibi kişisel bilgilerini koruyamadığı*", "*davacının kart bilgilerini ve şifrelerini karşı tarafa kendisinin bildirdiği*", "*kartın cihaza sıkışmasından sonra arka sırada bekleyen tanımadığı bir kişiden yardım isteyen davacının anılan kötü niyetli kişinin talimatı üzerine şifresini iki defa girdiği*" gerekçesiyle yetkisiz kişiler tarafından yapılan işlemler sebebiyle meydana çıkan zararlardan müşterinin ortak kusuru oranında sorumlu olduğu sonucuna ulaşmıştır.

KAYNAKÇA

Açıkgöz, Osman: "İnternet Bankacılık Hizmetlerinin Sağlanmasına Yönelik Borcun İfasında Mobil Haberleşme (GSM) Şirketinin Hukuki Konumu ve Banka ile Mevduat Sahibine Karşı Sorumluluğu", Kadir Has Üniversitesi Hükuk Fakültesi Dergisi, C. 3, S. 2, Aralık 2015, s. 59-76.

Adams, Anne/ Sasse, Martina Angela: "Users Are Not The Enemy", Communications of the ACM, December 1999, Vol. 42, No. 12, s. 41-46.

Akarslan, Hüseyn: Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2015.

Akçaal Mehmet: Sözleşme Sonrası Sorumluluk (Sözleşme Sonrası Yükümlülüklerin İhlâlinden Doğan Sorumluluk), 1. bs., Konya, Sayram Yayınları, 2018

Akıncı, Şahin: Borçlar Hukuku Bilgisi, Genel Hükümler, 10. bs., Sayram Yayınları, Konya, 2017

Akıncı, Şahin: Vekalet Sözleşmesinin Sona Ermesi, Sayram Yayınevi, Konya, 2004 (Kısaltılmışı: Akıncı, Vekalet).

Akıncı, Şahin: Kötü İfa-Eksik İfa-Ayıplı İfa Ayrımı ve Bu Ayrımın Hukuki Sonuçları, 1926'dan Günümüze Türk-İsviçre Medeni Hukuku, C. 2, Yetkin Yayınları, Ankara, 2017, s. 1391-1421 (Kısaltılmışı: Akıncı, Kötü İfa).

Akipek, Şebnem: Alt Vekalet, Yetkin Yayınları, Ankara 2003 (Kısaltılmışı: Akipek, Alt Vekalet).

Akkanat, Halil: "İnternet Bankacılığı Sistemi Üzerinden Bankalara Verilen Zararlardan GSM Operatörleri Sorumlu Tutulabilir mi?", Telekomünikasyon Hukuku, Filiz Kitabevi, İstanbul 2017, s. 54-79.

Akkılıç, M. Emin: **"**Teknolojik Gelişmelerin Bankaların Dağıtım Kanallarının Yapısı Üzerine Etkileri", DAUM Dergisi, S. 2, Y. 2005, s. 110-114.

Akkurt, Sinan Sami: "Elektronik Ortamda Hizmet Sunumu Ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri", AÜHFD, C. 60, S. 1, Y. 2011, s. 19-46.

Aksoy, Ramazan: İnternet Ortamında Pazarlama, 2. bs., Ankara, Seçkin Yayıncılık, 2009.

Aksoy, Tüfvik Emre: İşadamlarının Elektronik??? Bankacılık Kullanma Durumları ve Karşılaşılan Problemler", Yayımlanmamış Yüksek Lisans

Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara 2007.

Aktürk, Kemal/ Talan, Tarık: "*Mobil Bilişim Suçları*", Enformatik, Toplum ve Hukuk, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016.

Alptürk, Ercan: Elektronik Ticaretin Hukuku Ve Vergilendirilmesi, , Kazancı Matbaacılık Sanayii, İstanbul 2005.

Altan, Mikail: Fonksiyonlar ve İşlemler Açısından Bankacılık, , Beta Basım Yayın, İstanbul 2001.

Altaş, Hüseyin: "Mevduat Hesabından Yetkisiz Para Çekilmesinde Bankanın Hukuki Sorumluluğu", ABD, 2001/3, s. 37-45.

Altınışık, Ülvi: Elektronik Sözleşmeler, , Seçkin Yayıncılık, Ankara 2003.

Altıparmak, Yağmur: "*Kredi Kartı Sözleşmesi*", 6502 sayılı Tüketicinin Korunması Hakkındaki Kanun Hükümlerine göre Tüketici Hukuku Uygulamalarında Tüketicinin Korunması, Ed. Sütçü S.S., Seçkin Yayınevi, Ankara, 2019, s. 207-224.

Andrews, Nathanael: "*Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers For SIM-Swap Attacks and Wireless Provider Liability*", Northwestern Journal of Technology and Intellectual Property, Vol. 16, Is. 2, 2018, s. 79-105.

Aral, Fahrettin: Türk Borçlar Hukukunda Kötü İfa, Ankara, Yetkin Yayınları, 2011.

Aral, Fahrettin/ Ayrancı, Hasan: Borçlar Hukuku Özel Borç İlişkileri, 11. bs., Yetkin Basımevi, Ankara 2015.

Arkan, Sabih: Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukukî Sorunlar, Ankara, TBB Yayınları, 1991 (Kısaltılmışı: Arkan, Elektronik Bankacılık).

Arkan, Sabih: Ticari İşletme Hukuku, Ankara, 23. bs., Banka ve Ticaret Hukuku Araştırma Enstitüsü, 2017 (Kısaltılmışı: Arkan, Ticari İşletme).

Atamer, M. Yeşim: "Kredi Kartının Üçüncü Kişi Tarafından Hukuka Aykırı Şekilde Kullanılması Hâlinde Doğan Zararları Kim Taşıyacaktır?", Bilgi Toplumunda Hukuk/Prof. Dr. Ünal Tekinalp'a Armağan, C. 1, İstanbul, Beta Basım Yayın, 2003, s. 993-1031 (Kısaltılmışı: Atamer, Kredi Kartı).

Avşar, Zakir/ Güngören, Gürsel: Bilişim Hukuku, Türkiye Bankalar Birliği Yayını No: 270, İstanbul, 2010.

Aysal, Hakan: "Güvenlik ve İnternet Erişim Politikaları Oluşturulması:

İstanbul Üniversitesi'nde Uygulama Süreci", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, 2007.

Bahtiyar, Mehmet: "Banka Kartları ve Kredi Kartları Kanunu'na göre Kartın Haksız Kullanımından Dolayı Hukuki Sorumluluk" İÜHFM, C. LXXI, 2013, s. 71-89.

Başpınar, Veysel: Vekilin (Avukatın, Hekimin, Mimarın, Bankanın) Özen Borcundan Doğan Sorumluluğu, 2. bs., Ankara, Yetkin Yayınları, 2004.

Battal, Ahmet: Güven Kurumu Nitelendirilmesi Işığında Bankaların Hukukî Sorumluluğu, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, 2001.

Bayrakdaroğlu, Ali: "Bireylerin İnternet Bankacılığı Kullanımını Etkileyen Faktörlerin Belirlenmesi Üzerine Bir Alan Araştırması", Business and Economics Research Journal, Vol. 3, No 4, Y. 2012.

Berber, Leyla Keser: Adli Bilişim, Ankara, Yetkin Yayınları, 2004.

Berber, Leyla Keser: İnternet Bankacılığında Banka ve Müşterilerin Sorumluluğu, beyazsapka. org (son erişim tarihi: 30.01.2021).

Bilgen, Mahmut: İnternet Bankacılığından Kaynaklanan Zararlarda Bankaların Sorumlulukları, Bankacılar Dergisi, Sayı 71, 2009, 78-96 (Kısaltılmışı: Bilgen, Sorumluluk).

Bilgen, Mahmut: Banka Hukukunda Sözleşmeler, Uyuşmazlıklar ve Hukuki Sorumluluk, Adalet Yayınevi, Ankara, 2011 (Kısaltılmışı: Bilgen, Sözleşmeler).

Bozbel, Savaş: "İnternet Üzerinden Yapılan Hukuki İşlemler ve Bu Konuda 97/7 Sayılı Tüketicinin Korunmasına Dair AT Yönergesi", Yargıtay Dergisi, C. 27, 2001, 749-788.

Burrow, K. Robert: "Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank", North Carolina Banking Institute, Vol. 17, Iss. 1, 381-400.

Cardoso, Jorge/ Fromm, Hansjörg/ Nickel, Stefan/ Satzger/ Gerhard/ Studer, Rudi/ Weinhar, Christof : Fundamentals of Service Systems, Springer, 2015.

Çeker, Mustafa: "İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden Bankaların Sorumluluğu (Yargıtay 11. Hukuk Dairesi'nin Bir Kararı Münasebetiyle)", Prof. Dr. Hüseyn Ülgen'e Armağan, C. 2, İstanbul, Vedat Kitapçılık, 2007, s. 1335-1352 (Kısaltılmışı: Çeker, İnternet Bankacılığı İşlemleri).

Çeker, Mustafa: "İnternet Ortamında Yapılan Usulsüzlüklerden Bankaların Hukuki Sorumluluğu (Yargıtay 11. Hukuk Dairesi'nin Bir Kararı Münasebetiyle)", Prof. Dr. Bilge Öztan'a Armağan, Ankara, Seçkin Yayıncılık, 2008, s. 248-261 (Kısaltılmışı: Çeker, Sorumluluk).

Çeker, Mustafa: Hukukî Yönüyle Banka Mevduatı, Ankara, Karahan Kitabevi, 2004 (Kısaltılmışı: Çeker, Banka Mevduatı).

Çentr İssledovaniy Platejnıx Sistem ve Rasçetov: Distançionnoe Bankovskoe Obslujivanie, Moskova, KNORUS Yayınevi, 2010.

Ceylan, Eyyup Ensar: "İnternet Bankacılığı ve Bankaların Hukukî Sorumlulukları", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2013.

Classens, Joris/ Dem, Valentin/ De Cock, Danny/ Preneel, Bart/ Vandewalle, Joos: "On the Security of Today's Online Electronic Banking Systems", Computers and Security, Vol. 21, Issue 3, Y. 2002, s. 253-265.

Coşgun, Karaman Özlem: "Bankaların, Telekomunikasyon Şirketlerinin ve Mevduat Sahiplerinin İnternet Bankacılığından Doğan Sorumlulukları", Hukuk Biliminin Güncel sorunları, III. Uluslararası Kongre Bildiri Kitabı, C. 2 (Özel Hukuk), s. 169-200.

Cox, Buket Öztuna: Avrupa Birliği Hukukunda Elektronik Ticaret ve Türkiye'deki Gelişmeler, İstanbul, Pusula Yayıncılık, 2002.

Demir, Mehmet: Mesafeli Sözleşmelerin İnternet Üzerinden Kurulması, Ankara, Turhan Kitabevi, 2004.

Donay, Süheyl: "Vekilin Talimata Uyma ve Dürüstlükle Hareket Etme Borcu", BATİDER, Aralık 1970, C. 5, S. 4, s. 728-749.

Douglas, L. John: "Cyberbanking: Legal and Regulatory Considerations for Banking Organizations", North Carolina Banking Institute Journal, 2000, Vol. 57, s. 57-127.

Dülger, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayıncılık, 2015.

Eralp, Özgür: İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Ankara 2012.

Erbek, Özge: Tüketici Satımlarında Satıcının Sözleşme Öncesi Aydınlatma Yükümlülüğü ve İhlalinin Hukuki Sonuçları, Yayımlanmamış Doktora Tezi, DEÜ SBE, 2010.

Erdoğan, Burcu: "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?", http://www.digisophia. com/Article/Details/61, (Erişim tarihi Ocak 03, 2020).

Eren, Fikret: Borçlar Hukuku Genel Hükümler, 18. bs., Ankara, Yetkin

Basımevi, 2015 (Kısaltılmışı: Eren, Genel Hükümler).

Eren, Fikret: Borçlar Hukuku Özel Hükümler, 4. bs., Ankara, Yetkin Basımevi, 2017 (Kısaltılmışı: Eren, Özel Hükümler).

Erol, İbrahim/ Çınar, Serkan/ Durmaz, Selim: "Bankaların Yeni Gelir Kaynağı: Elektronik Bankacılık İşlem Ücretleri, Türk Bankacılık Sektöründe Banka Karlılığı Üzerindeki Etkisi", AİBÜ SBED, C. 15, S. 2, Y. 2015, 1-21.

Craig, Brain: Cyberlaw: The Law of the Internet and Information Technology, Pearson Education, 2012.

Georges Ifrah: Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi IX, Çev. Kurtuluş Dinçer, Ankara, Tübitak Popüler Bilim Kitapları, 2002.

Gerhard Danneman Reiner Schulze German Civil Code, Bürgerliches Gesetzbuch (BGB), Volume I, Books 1-3: Paragraph 1-1296, Article-by-Article Commentary, Nomos, 2020, s.1356-1357.

Geva, Benjamin: "Consumer Liability in Unauthorized Electronic Funds Transfers", Canadian Business Law Journal, Vol. 38, Y. 2003, s.

Gkoutzinis, Apostolos: Internet Banking And The Law In Europe, Cambridge University Press, 2006.

Gül, Ahmet: Doğrudan/Dolayı Bilişim Suçları, Ankara, Seçkin Yayınları, 2016.

Gülerci, Altan Fahri: Sorumluluk Hukuku Bakımından Bankacılıkta Risk Kavramı, TBB Yayınları, İstanbul, 2015.

Gümüş, Mustafa Alper: Türk-İsviçre Borçlar Hukukunda Vekilin Özen Borcu, İstanbul, Beta Basım Yayın, 2001 (Kısaltılmışı: Gümüş. Özen Borcu).

Gümüş, Musatafa Alper: "6102 Sayılı Türk Ticaret Kanunu (TTK) m.18/II'de Yer Alan "Basiretli İş Adamı (Tacir) Davranışı" Ölçütünün İyiniyetin (TMK m.3) Varlığının Belirlenmesindeki İşlevi", MÜHF-HAD, Özel Sayı, Prof. Dr. Cevdet Yavuz'a Armağan, Y. 2016, C. 2, S. 3, 1221-1240 (Kısaltılmışı: Gümüş, Basiretli İş Adamı).

Güngör, Müberra/ Evren, Gökhan: İnternet Sektörü ve Türkiye İncelemeleri, T.C. Telekomünikasyon Kurumu Tarifeler Dairesi Başkanlığı, Ankara, 2002.

Güran, Sait/ Akünal, Teoman/ Bayraktar, Köksal ve Diğerleri: İnternet ve Hukuk, Superonline Workshop Metni, İstanbul, 2000.

Gürpınar, Damla: Sözleşme Dışı Yalnış Tavsiyede Bulunma, Öğüt veya Bilgi Vermeden Doğan Hukuki Sorumluluk, İzmir, Güncel Hukuk Yayınları, 2006.

Harrel, C. Alvin: "The Bank-Customer Relationship: Evolution of a Modern Form?", Oklahoma City University Law Review, 1986, Vol. XI, s. 641-682.

Haybäck , Gerwin: "Civil law liability for unauthorized withdrawals at ATMs in Germany", Digital Evidence and Electronic Signature Law Review, 57, (2009), s. 57-66.

Honeywill, C. Sean: "*Data Security and Data Breach Notification for Financial Institutions*", North Carolina Banking Institute, C. 10, S. 1, 2006, s. 269-304.

İşgüzar, Hasan: Banka Kredi Kartı Sözleşmeleri, Ankara, Yetkin Yayınları, 2003.

Işkın, Seyit Ahmet: Elektronik Bankacılık Hizmetleri ve Denetimi, İstanbul, İTO Yayınları, 2012.

İnal, Emrehan: E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması, İstanbul, Vedat Kitapçılık, 2005 (Kısaltılmışı: E-Ticaret).

İnal, Emrehan: "İnternet Dolandırıcılığı Eylemlerine Karşı Bankanın Yükümlülükleri ve Sorumluluğu", Banka ve Tüketici Hukuku Sorunları Sempozyumu, XII Levha Yayıncılık, 2010, 365-375 (Kısaltılmışı: Sempozyum)

İstanbul Ticaret Odası İnternet Üzerinde Güvenlik Sorunları ve Güvenli Ticaret Yapmanın Yolları, İstanbul, İTO Yayınları, 2007.

Kandıralıoğlu, Pınar Çağla: Türk Hukukunda Bankaların Sır Saklama Yükümlülüğü, İstanbul, XII Levha Yayıncılık, 2011.

Kaneko, Hiraneo: "How Bank Depositors are Protected in Japan", Digital Evidence and Electronic Signature Law Review, Vol. 8, Y. 2011, s. 92-106.

Kaneti, Selim: "Elektronik Banka İşlemlerinin Hukuksal Yapısı", Makalaler, On İki Levha Yayıncılık, İstanbul, 2011.

Kaplan, İbrahim: Banka Sözleşmeleri Hukuku, C. 1, Ankara, Dayınlarlı Yayıncılık, 1996 (Kısaltılmışı: Kaplan, Sözleşme).

Kaplan, İbrahim: "Bankanın Hukuki Sorumluluğu", Prof. Dr. Haluk Tandoğan'ın Hatırasına Armağan, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1990, s. 445-460 (Kısaltılmışı: Kaplan, Sorumluluk).

Kaplan, İbrahim: "Banka Hesap Türleri, Hesap Sahibinin ve Hesap Türünün Tayininde Uygulanacak Kurallar", AÜSBFD, C. 49, S. 1-2, s. 273-289 (Kısaltılmışı: Kaplan, Banka Hesabı).

Karloin, Laue: Grazhdansko-Pravovaya Otvetstvennost Bankov v Raschetnıx Pravootnosheniyax Po Zakonadatelstvu Germanii i Rossiyskoy Federachii, Sravnitelno-Pravovoy Aspekt, Prospekt Yayımevi, Moskva, 2017.

Kaya, Taner: "İnternet Bankacılığı", Bilişim ve Hukuk Dergisi (Ankara Barosu), S. 9, Y. 2008.

Kawawa, Noriko "The Japanese Law on Unauthorized On-line Credit Card and Banking Transactions: Are Current Legal Principles With Respect to Unauthorized Transactions Adequate to Protect Consumers Against Information Technology Crimes in Contemporary Society?", Digital Evidence and Electronic Signature Law Review, Vol. 10, Y. 2013, s. 71-80.

Kent, Stephen: "On the Trail of Intrusions Into Information Sy, s. stems", **IEEE Spectrum**, Vol. 37, Is. 12, Y. December 2000, s. 52-56.

Kılıçoğlu, M. Ahmet: Borçlar Hukuku Genel Hükümler, 21. bs., Ankara, Turhan Kitabevi, 2017.

Kocasakal, Özdemir Hatice: Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, Vedat Kitapçılık, İstanbul 2003.

Kocayusufpaşaoğlu, Necip: Borçlar Hukukuna Giriş – Hukuki İşlem – Sözleşme, C. 1, İstanbul, Filiz Kitabevi, 2017.

Kolodinsky, M. Jane/ Hogarth, M. Jeanne/ Hilgert, A. Marianne: The adoption of electronic banking technologies by US consumers", International Journal of Bank Marketing, Vol. 22, Issue 4, 2004, s. 238-259.

Kondabagil, Jayaram Risk Management in Electronic Banking: Consepts and Best Practices, John Wiley and Sons (Asia), 2007.

Küçükyılmazlar, Aysun: Elektron Ticaret Rehberi, İstanbul Ticaret Odası, Yayın No: 2006-3, Şubat 2006.

Lombardo, Tom: Information Technology and Artificial Intelligence, http://www.centerforfutureconsciousness.com/pdf_files/Readings/ReadingInfoTech.pdf.

Leiner, M. Berry: "A Brief History Of The Internet", Computer Communication Review, Vol. 39, No 5, October 2009, s. 22-31.

Mikhaylichenko, Karina: "Finansal Hizmetlerin Küreselleşmesine Katkı Açısından Elektronik Bankacılık", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, İstanbul, 2015.

Muktadir, Lale: "İnternet Bankacılığında Hukuki Sorumluluk", Terazi Hukuk Dergisi, S. 42, Şubat 2010. Sayfa???

Mulliner, Collin/ "*SMS-based One-Time Passwords: Attacks and Defense*",

Bargaonkar, Ravishankar/ Stewin, Patrick vd.: Detection of Intrusions and Malware, and Vulnerability Assessment, 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings, Ed. Konrad Rieck, Patrick Stewin, Jean-Pierre Seifert, Springer-Verlag, Berlin, 2013, s. 150-159.

Murdoch, J. Steven: "Reliability of Chip and PIN Evidence In Banking Disputes", Digital Evidence and Electronic Signature Law Review, Vol. 6, Y. 2009, s. 98-115.

Oğuz, Sefer: "Telif Hakkı İhlallerinden İnternet Servis Sağlayıcıların Sorumlulukları", **GÜHFD**, C. XII, S. 1-2, Y. 2008, s. 149-183.

Oğuzman, M. Kemal/ Barlas, Nami: Medenî Hukuk, İstanbul, Vedat Kitapçılık, 2016.

Oğuzman, M. Kemal/ Öz, M. Turgut: Borçlar Hukuku Genel Hükümler, C. 1, 14. bs., İstanbul, Vedat Kitapçılık, 2016.

Özboyacı, Alper: Kartlı Ödeme Sistemlerinde Kartın Kötüye Kullanılmasından Kaynaklanan Hukuki Sorumluluk, Seçkin Yayıncılık, Ankara, 2019

Özdamar, Naci: "İnternet Bankacılığı ve Banka Kartları", Bilişim ve Hukuk, Ankara Barosu Uluslararası Hukuk Kurultayı, C. 2, Y. 2008.

Özdilek, Ali Osman: Internet ve Hukuk, İstanbul, Papatya Yayıncılık, 2002 (Kısaltılmışı: Özdilek, İnternet).

Özdilek, Ali Osman: Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, Vedat Kitapçılık, İstanbul, 2006 (Kısaltılmışı: Örnek Olaylar).

Özdilek, Ali Osman: Ankara Barosu Uluslararası Hukuk Kurultayı 2008, 8 Ocak-11 Ocak 2008, C. 2, Ankara Barosu Yayınları, 2009.

Özel, Sibel: Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, Ankara, Seçkin Yayıncılık, 2004.

Özmen, Şule: Ağ Ekonomisinde Yeni Ticaret Yolu E-Ticaret, 4. bs., İstanbul Bilgi Üniversitesi Yayınları, 2012.

Özmestik, Fehmi Ünsal: "Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar", Yayımlanmamış Yüksek Lisans Tezi, İstanbul bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2015.

Mason, Stephen /Bohm, Nicolas: "Banking and Fraud", Computer Law and Security Review, The International Journal of Technology Law and Practice, Vol. 33, Iss. 2, April 2017, s. 237-241.

Mason, Stephen: "Electronic Banking and how courts approach the evidence", Computer Law and Security Review, Vol. 29, Y. 2013, s.

Mason, Stephen/ Seng, Daniel: Electronic Evidence, Fouth Edition, Institute of Advanced Legal Studies, London, 2017.

Mason, Stephen: Electronic Signatures in Law, SAS Humanities Digital Library, School of Advanced Study, University of London, 2016.

Memiş, Tekin: "Elektronik Bankacılıkta Bankanın Yükümlülük ve Sorumlulukları", Prof. Dr. Ergon A. Çetingil ve Prof. Dr. Rayegan Kender'e 50. Birlikte Çalışma Yılı Armağanı, İstanbul, Çizgi Basım Yayın, 2007 (Kısaltılmışı: Memiş, Sorumluluk), 875-885.

Memiş, Tekin: "Hukuki Açıdan Kitlelere E-Posta Gönderilmesi", AÜEHFD, C.5, S. 1-4, Y. 2001 (Kısaltılmışı: Memiş, E-Posta), s. 431-444.

Micklitz, Hans-W / Stuyck, Jules/ Terryn, Evelyne: Cases, Materials and Text on Consumer Law, Oxford and Portland, Oregon, Hart Publishing, 2010.

Nuth, Silahi Maryke: "Unauthorised Use of Bank Cards With or Without The PIN: A Lost Case For The Customer?", Digital Evidence and Electronic Signature Law Review, Vol. 9, Y. 2012, s. 95-101.

Pekşirin, Hülya: Modern İletişim Araçları ve Özel Hukuk (İnternette Sözleşme Akdi), Ankara Barosu Hukuk Kurultayı, Ankara 2000, C. 3, s. 324-326.

Reisoğlu, Seza: Bankacılık Kanunu Şerhi, C. 1, Gözden Geçirilmiş 2. bs., Yaklaşım Yayınları, Ankara, 2015.

Reisoğlu, Seza: Bankacılık Kanunu Şerhi, C. 2, Gözden Geçirilmiş 2. bs., Yaklaşım Yayınları, Ankara, 2015.

Reha, Poroy/ Yasaman, Hamdi: Ticari İşletme Hukuku, 14. bs., Vedat Kitapçılık, İstanbul, 2012.

Rowan Legal: "*Commentary: Slovak case law on the responsibility of a bank for unauthorised financial transactions*", Digital Evidence and Electronic Signature Law Review, 12 (2015), s. 101-102.

Saka, Tamer: Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi, TBB Yayınları, İstanbul, 2001.

Sağıroğlu, Şeref/ Alkan, Mustafa: Siber Güvenlik ve Savunma (Farkındalık ve Caydırıcılık), Grafiker Yayınları, Ankara, 2018.

Sağlam, İpek: Elektronik Sözleşmeler, Legal Kitabevi, İstanbul, 2007.

Sarıhan, Deniz Tan: Herkes İçin İnternet, Beta Yayınları, İstanbul, 1998.

Savaş, Abdurrahman: "İnternet Bankacılığı ve Tarafların Yükümlülükleri", SÜHFD, C. 19, S. 2, Y. 2011, 137-166.

Serhateri, Ayhan: "Elektronik Ticarette Güvenliğin Tüketicilerin İnternet

Üzerinden Alışveriş Yapma Tutumlarına Etkisi: Kocaeli Örneği", Karadeniz Uluslararası Bilimsel Dergi, C. 1, S. 27, Y. 2015, s. 227-249.

Serozan, Rona: Medeni Hukuk, Genel Bölüm/Kişiler Hukuku, Vedat Kitapçılık, İstanbul, 2011.

Serozan, Rona: Borcçlar Hukuku, Genel Bölüm, C. 3, İfa, İfa Engelleri, Haksız Zenginleşme, Filiz Kitabevi, İstanbul, 2016.

Serozan, Rona: «"Culpa İn Contrahendo", "Akdin Müsbet İhlâli" ve "Üçüncü Kişiyi Korucu Etkili Sözleşme" Kurumlarının Ortak Temeli: Edim Yükümlerinden Bağımsız Borç İlişkisi"», MHAD, 1968, Y. 2, S. 3, s. 108-129 (Kısaltılmışı: Serozan, Bağımsız Borç İlişkisi).

Shah, Mahmood/ Clarke, Steve: E-Banking Management: Issues, Solutions, and Strategies, Information Science Reference, New York, 2009.

Shinar-Plato, Ruth: "The Banking Contract As a Special Contract: The Israeli Approach", Touro Law Review, 2013, Vol. 29, s. 721-746 (Kısaltılmışı: Shinar-Plato, Contract).

Shinar-Plato, Ruth: "The Bank's Duty of Disclosure – Towards a New Model", Banking & Finance Law Review, Vol. 27, Y. March 2012, s. 427-444 (Kısaltılmışı: Shinar-Plato, Duty of Disclosure).

Sınar, Hasan: İnternet ve Ceza Hukuku, Beta Yayınları, İstanbul, 2001.

Sonat, K. Ali: "Nakit Dışı Ödeme Usulleri Çerçevesinde Para Borcunun Banka Havalesi Yoluyla Ödenmesi", (Yayımlanmamış Doktora Tezi), Galatasaray Universitesi Sosyal Bilimler Enstitüsü, Şubat 2010.

Soysal, Tamer: **"**İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", TBBD, S. 61, Y. 2005, s. 304-339 (Kısaltılmışı: Soysal, Servis Sağlayısıları).

Soysal, Tamer: **"**Elektronik Posta Yoluyla Kişilik Haklarına Müdaheleden Doğan Hukuki Sorumluluk", ABD, Y. 65, S. 1, Kış 2007, s. 144-167 (Kısaltılmışı: Soysal, Elektronik Posta).

Steennot, Reinhard: "Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping", Financial Law Institute, Working Paper Series, July, 2010 (Steennot , Allocating liability).

Steennot, Reinhard: "Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market", Computer Law and Security Report, 24 (2008), s. 555-561, (Steennot, Directive)

Stoufflet: "Bankacılıkta Sorumluluk", Mukayeseli Banka Hukuku İhtisas Dönemi, İstanbul 3-14 Aralık 1973, C. 3, TBB Yayınları, 1974.

Subramanian, Revaathi: Bank Fraud, Using Technology to Combat Losses, Wiley, 2014.

Şahin, Levent Yusuf: "Ağ Güvenliği", Bilgisayar Ağları ve İletişim, Ed. Abdullah Kuzu, Ankara, Nobel Yayınları, 2011.

Şeker, Muzaffer: Elektronik Ödeme Sistemleri, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl: 10, Sayı: 20, Güz 2011, s. 55-73.

Şeker, Muzaffer: 6098 Sayılı Yeni Türk Borçlar Kanununa göre Internet Üzerinden Sözleşmelerin Kurulması, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl: 11, Sayı: 20, Güz 2012/2, s. 127-155.

Tandoğan, Halûk: Türk Mes'uliyet Hukuku (Akit Dışı ve Akdi Mes'uliyet), Ajans-Türk Matbaası, Ankara, 1961 (Kısaltılmışı: Mes'uliyet Hukuku).

Tandoğan, Halûk: Borçlar Hukuku Özel Borç İlişkileri, C. 2, 3. bs., Banka ve Ticaret Hukuku Araştırma Enstitüsü, Ankara, 1987 (Kısaltılmışı: Özel Borç İlişkileri).

Tandoğan, Halûk: "Türk Hukukunda Bankacının Hukuki Sorumluluğu", Mukayeseli Banka Hukuku İhtisas Dönemi, İstanbul 3-14 Aralık 1973, C. 3, TBB Yayınları, 1974 (Kısaltılmışı: Bankacının Hukuki Sorumluluğu).

Tian, Yan/ Stewart, Concetta: "History of E-Commerce", Electronic Commerce: Concepts, Methodologies, Tools, and Applications, Ed. S. Ann Becker, Vol. 1, Information Science Reference, New York, 2008.

Topuz, Seçkin: "Türk Hukukunda Vekalet Sözleşmesinde Vekilin Özen Borcu", Yayımlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale 2001.

Türk, Ahmet: Hukukî Yönden Banka Havalesi, Yetkin Yayınları, Ankara, 2007.

Türkiye Bankalar Birliği: Dolandırıcılık Eylemleri ve Korunma Yöntemleri, TBB Yayınları, Aralık 2015.

Türkiye Bankalar Birliği: Dijital, Internet ve Mobil Bankacılık İstatistikleri Haziran 2018, Rapor Kodu: DT22, Temmuz 2018.

Ülgen, Hüseyin/ Mehmet, Helvacı/ Abuzer, Kendigelen/ Arslan, Kaya/ Nomer Ertan, Füsun: Ticari İşletme Hukuku, 24. bs., On İki Levha Yayıncılık, İstanbul, 2015.

Yasaman, Hamdi: Banka Hukuku İle İlgili Makaleler, Hukuki Mütalaalar, Bilirkişi Raporları, İstanbul, Vedat Kitapçılık, 2005.

Yaşar, Hakan/ Çakır, Hüseyn: "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, C. 3, S. 2, Y. 2015, s. 488-507.

Yavuz, Cevdet/ Faruk, Acar/ Özen, Burak: Türk Borçlar Hukuku Özel Hükümler, 9.bs., Beta Yayınevi, İstanbul, 2014.

Yıldırım, Kadir: "Avrupa Birliği ve Türkiye'de Elektronik Bankacılık Uygulamaları", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü İktisat Teorisi Ana Bilim Dalı, 2006.

Yılmaz, Davut: Hacking/Bilişim Korsanlığı ve Korunma Yöntemleri, Hayat Yayınları, İstanbul, 2004 (Kısaltılmışı: Yılmaz, D.).

Yılmaz, Süleyman: Hukukî Açıdan Internet Bankacılığı, Yetkin Yayınları, Ankara, 2010 (Kısaltılmışı: Yılmaz, S.).

Yiğitbaşı, İsmet /Gürsul, Fatih: "*Online Bankacılık Suçlarının İncelenmesi: İstanbul Örneği*", Enformatik, Toplum ve Hukuk, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s. ?????

Yurttadur, Mustafa/ Süzen, Ekrem: "Türkiye'de Banka Müşterilerinin İnternet Bankacılığına Yaklaşımlarının İncelenmesi Üzerine Bir Uygulama", Tüketici ve Tüketim Araştırmaları Dergisi, C. 8, S. 1, Y. Haziran 2016, s. 93-120.

Tekinalp, Ünal: Banka Hukukunun Esasları, Yeniden Yazılmış 2. bs.,Vedat Kitapçılık, İstanbul, 2009.

Yüksel-Mermod, Aslı: Finansal Küreselleşme Işığında Elektronik Bankacılık ve Riskler, İstanbul, Beta Yayınevi, 2011.

Vitalyeviç, Leonid Lyamin: Primenenie Tekhnologiy Elektronnoqo Bankinga. Risk-Orientirovannıy Podkhod, Moskova, KNORUS Yayınevi, 2011.

Wan, Hakman: Electronic Financial Services: Technology and Management, Chandos Publishing, 2006, s. 104

Wiegand, Wolfgang "Legal Aspects of the Bank-Customer Relationship in Electronic Banking", Legal Issues in Electronic Banking, Ed. Norbert Horn, Kluwer Law International, Netherlands, 2002, s. 163-186.

Zevkliler, Aydın/ Gökyayla, Emre: Borçlar Hukuku Özel Borç İlişkileri, 16.bs., Ankara, Turhan Kitabevi, 2016.

Zevkliler, Aydın/ Özel, Çağlar: Tüketicinin Korunması Hukuku, 1. bs., Seçkin Yayınevi, Ankara, 2016.