Araştırma Makale | Research Article

KHM, Cilt:6 Sayı:1, 2026, s. 111-137.
Geliş Tarihi | Received: 18.06.2025
Kabul Tarihi | Accepted: 11.12.2025
Yayın Tarihi | Published: 30.04.2026
doi: 10.59909/khm.06.01.004

İntihal | Plagiarism: Bu makale, en az iki hakem tarafından incelendi ve intihal içermediği teyit edildi.
| This article has been reviewed by at least two referees and scanned via a plagiarism software.

BANKA HESAP KAYITLARINDA BİLİŞİM SİSTEMLERİ VASITASIYLA YETKİSİZ DEĞİŞİKLİK YAPMAK

Unauthorized Alteration of Bank Accounting Records through Information Systems

Dr. Öğr. Üyesi Burak Boz*

Öz

Yargıtay, Bilişim sistemleri vasıtasıyla bir başkasının banka hesabındaki mevduat bakiyesinin bir başka hesaba aktarılmak suretiyle azaltılmasını, bu şekilde hesaba geçirilen bakiyenin kullanılıp kullanılmadığına bakmaksızın, nitelikli hırsızlık olarak değerlendirilmektedir. Yargıtay'ın yerleşik içtihadında, bu fiil ile çalınan şeyin "kaydî para" olduğunu ileri sürülmektedir. Oysa kaydî para, ne maddi bir cisimdir ne de taşınır bir (eşya) maldır. Bu nedenle kaydî para üzerinde 'alma' fiili işlenemez; yani kaydî para hırsızlık suçunun maddî konusunu oluşturamaz. Banka bilişim sistemlerine hukuka aykırı olarak girme, dijital muhasebe kayıtlarını değiştirme ve gerçek olmayan mevduat bakiyesini kullanma fiillerinin, mer'i mevzuata göre nitelendirilmesi gerekmektedir. Söz konusu fiillerin gerçekleştirilebileceği çeşitli ihtimâller yapılacak incelemede göz önünde bulundurulmalıdır. Kanaatimiz ve bilişim sistemleri vasıtasıyla bir başkasının banka hesabı bakiyesinin değiştirilmesi ve bu şekilde hesaba geçirilen bakiyenin kullanılması; bilişim sistemlerine girme (TCK m. 243/1), verileri değiştirerek menfaat sağlama (TCK m. 244/2, 3 ve 4), nitelikli hırsızlık (TCK m. 142/2-e) ve nitelikli dolandırıcılık (TCK m. 158/1-f) suçları bağlamında ele alınmalıdır. Ayrıca bilişim sistemi üzerinde tutulan banka muhasebe kayıtlarının değiştirilmesi, çevrimiçi bankacılık kanalıyla banka müşterisinin iradesine aykırı işlemlerin yapılması gibi fiilleri özel bir suç tipi hâline getiren ve bu yollarla elde edilen mevduat bakiyesinin kullanılmasını da cezayı ağırlaştıran nitelikli hâl olarak düzenleyen bir kanun hükmünün ihdası önerilmiştir. Bu değişiklik önerisi, kanunun açık ve anlaşılır olmasını sağlama ve mahkemelerin iş yükünün azaltılmasına katkı sunma amacı taşımaktadır.

Anahtar Kelimeler: kaydî para, çevrimiçi bankacılık, internet bankacılığı, mobil bankacılık, hırsızlık, dolandırıcılık, bilişim sistemleri.

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Ana Bilim Dalı.
0000- 0002-8282-3523 burak.boz@asbu.edu.tr

ABSTRACT

The act of grasping the balance in an individual's bank account, irrespective of the utilisation of the seized amount, is classified as qualified theft according to the established rulings of the Turkish Court of Cassation. The Turkish Court of Cassation has claimed that ' registered money' constitutes a stolen item. However, 'registered money' is not a movable prosperity (a good) because it does not have a physical form, thus it cannot be taken and cannot be considered 'the material object' in the context of theft. Once this issue is recognised, it is essential to examine those actions in terms of the law in force: illicit entry to a bank's information technology system, alteration of digital bank accounts, and utilisation of altered amounts within a bank account. Additionally, various options for executing these acts must also be considered. As a result, illicit access to banking information technology systems, manipulation of financial data within these systems, and misuse of the altered amounts must be considered in accordance with crimes of 'illicit entry into information technology systems (TPC art. 243/1)', obtaining unlawful gain by altering data (TPC art. 244/2, 3 and 4) 'qualified theft (TPC art. 142/2-e)', and 'qualified fraud (TPC art. 158/1-f)'. Additionally, an amendment is recommended that targets a criminal act of illicit access and manipulation of banking information technology systems, including a specific qualified variant of this crime that mandates a stringent penalty if the altered amount in the account is exploited. This recommendation seeks to reduce the workload on the courts while ensuring that legislation is clear and comprehensible.

Keywords: registered money, online banking, internet banking, mobile banking, theft, fraud, IT systems.

GİRİŞ

İnternet kullanımı, uzakları 'yakın' ve zamanı 'kısa' kılmıştır.[1] Bu etki hem olumlu hem de olumsuz sonuçlar doğurmakta, sunduğu kolaylıkların yanında risklerin de artmasına sebep olmaktadır. Özellikle halka açık internet bağlantı noktaları veya ortak kullanıma sunulan cihazlar üzerinden işlenen suçlarda, failin tespitinin görece zor olması,[2] bilişim alanını, becerikli suçlular[3] için cazip kılmaktadır.[4]

Bilişim alanındaki ihlâllerden korunma için bilişim sistemlerinin teknik yönden geliştirilmesi, saldırganların güvenlik duvarlarını aşmasını engellemek ilk seçenek olarak ortaya çıkmaktadır. Ancak teknolojideki ilerlemenin bilgi ve veri güvenliği alanında olduğu kadar saldırganların da lehine işlemesi, bu sistemlerin güvenliğinin yazılımcıları tarafından sağlanmasının yeterli olmayacağını göstermiş, ayrıca hukukî korumaya duyulan kaçınılmaz ihtiyacı ortaya koymuştur.[5] Bu noktada ceza hukukunun gösterdiği refleks; bu yeni alanı konu alan suç tipleri ihdas etmek ve mevcut suçların bilişim sistemleri aracılığıyla işlenmesini konu alan yeni düzenlemelere başvurmak olmuştur[6]. Zira suç fiillerinin gerçek dünyadan sanal mecraya taşınması, klâsik önlemleri ortadan kaldırmamakla birlikte bunlara ek veya tamamlayıcı tedbirleri gerektirmiştir.[7] Böylece bilişim ceza hukuku normları ceza kanunlarına dâhil olmuştur.[8]

Bilişim suçlarının işlenmesindeki artış, bankacılık sektörünü yakından ilgilendirmektedir. Çevrimiçi bankacılık ve mobil bankacılık parolalarının ele geçirilmesiyle işlenen suçlar giderek yaygınlaşmaktadır.[9] Doğrudan bankaya ait bilişim sisteminin saldırının hedefinde olması

---

1 Selman Dursun, "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni* 23, sayı 1-2 (Prof. Dr. Gülören TEKİNALP'e Armağan) (2003): 251.; *Örneğin* İspanya uyruklu bir kimsenin, Fransa'daki bilgisayarından, Almanya'daki bir bankanın ana bilgisayarına girerek kendisine para havalesi yapması durumunda, fail, fiilini Fransa'da gerçekleştirmiş ancak suçun neticesi Almanya'da cereyan etmiştir. Örnek olay ve hukukî değerlendirme için *bkz.* Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 4, sayı 1 (2002): 127.

2 Ortak bağlantı noktaları, aynı zamanda, internet bankacılığı gibi hassas kullanımlar bakımından mağdurları da açık hedef hâline getirebilmektedir. *Bkz.* Serdar Tutak, "Mobil bankacılık işlemlerinde 'halka açık Wi-Fi kullanmayın' uyarısı", Anadolu Ajansı, https://www.aa.com.tr/tr/ekonomi/mobil-bankacilik-islemlerinde-halka-acik-wi-fi-kullanmayin-uyarisi/3348749, Erişim 12 Ekim 2024.

3 Genellikle çıkar amaçlı olarak işlense de bilişim suçları, ücretli bir yazılımın kırılarak (*crack*) ücretsiz biçimde dağıtılmasında olduğu gibi, bir tür amme hizmeti yapıldığı inancıyla ve hatta entelektüel bir meydan okuma ve kendini ispat yöntemi olarak da işlenebilmektedir. *Bkz.* Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *Ankara Üniversitesi SBF Dergisi* 49, sayı 3 (1994): 157 ff.

4 Yaşar Karagöl, "Bilişim Suçları ve Önlemler", *Eskişehir Barosu Dergisi*, sayı 1 (2003): 65.

5 Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", 156.

6 Dursun, "İnternetten Kaynaklanan", 252.

7 Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", 156 ff.

8 Ancak bu, bilişim ceza hukukunun gelişiminin tamamlandığı anlamına gelmez. Bilişim ceza hukuku mevzuatı, bilişim yoluyla işlenen ihlâllerin nitelik ve niceliğine cevap verecek bir devinim içerisinde olmalıdır. Nitekim bilişim suçlarına dair düzenlemeler, ortaya çıktığı 1980'li yıllardan bu yana sıklıkla değişikliğe uğramıştır. *Bkz.* Berrin Bozdoğan Akbulut, "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, sayı 1-2 (Milenyum Armağanı) (2000): 548, 555.

9 Ayrıca, bilişim ve teknoloji altyapısı ile Türk bankacılık ve finans sektörü, mili güvenlik ve menfaatler açısından kritik altyapı olarak nitelendirilmekte olup bu alana gerçekleştirilen siber saldırılar, milli güvenlik tehdidi olarak değerlendirilmektedir. Kritik altyapı kavramı ve Türkiye Cumhuriyeti açısından kritik altyapılar hakkında detaylı bilgi için *bkz.* Muhammet Karaca ve Ensar Gül, "Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları", *Bilişim Hukuku Dergisi* 1, sayı 3 (2021): 4–6.

mümkün olduğu gibi banka ile işlem yapan kimselerin çevrimiçi işlem yapmalarına yarayan parola gibi verileri vasıtasıyla da suç işlenebilmektedir.[10] Ancak tüm bu riske[11] ve bankaların bilişim sistemlerini koruma ve teknik altyapılarını güçlendirme maliyetlerine rağmen, çevrimiçi bankacılık hacmi ve bankaların finansal başarısı arasında ciddi bir orantı bulunmaktadır.[12] Dolayısıyla bilişim ve iletişim teknolojilerinin bankacılık sektöründe kullanımından vazgeçme eğilimi söz konusu değildir; bilâkis çevrimiçi bankacılık hacminde artış gözlemlenmektedir.[13]

Bilişim sistemlerinin her türlü saldırıdan korunmasına dair teknik, sosyal ve hukukî tedbirlerin alınması, bankacılık sektörü bakımından kritik bir önem kazanmıştır. Ancak kimi zaman yeterli tedbir alınmamasına, kimi zaman ise alınan tedbirlere rağmen teknik yahut beşerî açıkların suistimâline dönük yeni yöntemler geliştirilmesine bağlı olarak bu tür suçlar işlenegelmektedir. Hatta bankacılık yazılımlarındaki kimi açıklar, nadiren de olsa, herhangi bir teknik bilgiye sahip olmayan kimselerin dahi banka hesapları üzerinde oynamasına fırsat verebilmektedir. Örneğin medyada dünyanın en büyük banka soygunu olduğu belirtilen ve *La Casa del Samsun* olarak adlandırılan olayda; akaryakıt istasyonunda pompacı olarak çalışan bir kimse, kardeşi ile beraber kullanmış oldukları mobil bankacılık uygulamasında bir hata keşfetmişler ve sahip olmadıkları fonları paraya çevirerek hesaplarında 16.000.000.000 (on altı milyar) Türk lirası varmış gibi göstermişlerdir.[14]

Bilişim sistemleri vasıtasıyla bir başkasının banka hesabı bakiyesinin değiştirilmesi ve bu şekilde hesaba geçirilen bakiyenin kullanılması fiilleri bakımından mevcut içtihadın eleştirisi ve sorunun çözümü, çalışmanın ana konusunu oluşturmaktadır. Banka çalışanlarının bankacılık zimmeti oluşturabilecek fiilleri, farklı bir olay grubu niteliğinde olduğundan, çalışmanın kapsamı dışında bırakılmıştır. Çalışmanın odağında, bir kimsenin banka hesabındaki bakiyenin; bu hesaplarla oynanmak suretiyle failin hesabına aktarılması bulunmaktadır. Bunun yanında failin hesabına haksız olarak aktarılan bakiye üzerinden yapılması muhtemel olan ATM'lerden ya da banka şubelerinden para çekilmesi veya bakiyenin başka hesaba havalesi işlemleri de değerlendirilecektir.

Çalışmamızda öncelikle bilişim sistemleri vasıtasıyla bir başkasının banka hesabı bakiyesinin değiştirilmesi ve bu şekilde hesaba geçirilen bakiyenin kullanılmasından ne anlaşıldığı

---

[10] Örnek olaylar için *bkz.*: Ali Aksoyer, "Banka hesap şifrelerini kıran 'hacker' iş üstünde yakalandı", https://www.hurriyet.com.tr/gundem/banka-hesap-sifrelerini-kiran-hacker-is-ustunde-yakalandi-5022308, Erişim 12 Ekim 2024; "Londra'da siber saldırıya gözaltı: 5 bin kullanıcının banka bilgileri tehlikede! - Son Dakika Teknoloji Haberleri | NTV Haber", https://www.ntv.com.tr/teknoloji/londrada-siber-saldiriya-gozalti-5-bin-kullanicinin-banka-bilgileri-tehlikede1gZx1Y6c2keFLGd0gihWbw, Erişim 13 Kasım 2024.

[11] Ankara ilinde yapılan ve sonuçları 2019 yılında yayımlanan bir araştırmada, internet bankacılığı kullanmama sebepleri arasında, internet bankacılığının güvenli olmadığı ve dolandırılma korkusu ikinci sırada yer almıştır. Araştırma sonuçları için *bkz.* Serhan Keskin, "Banka Müşterilerinin İnternet Bankacılığı Kullanmama Nedenlerinin Analizi", *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi* 9, sayı 1 (2019): 105.

[12] Uğur Uzun ve Murat Berberoğlu, "İnternet Bankacılığı Hizmetlerinin Banka Performansı Üzerine Etkisi", *Uluslararası İktisadi ve İdari İncelemeler Dergisi*, sayı 20 (2018): 59.

[13] Çevrimiçi bankacılık hacminde yüksek bir ivmeyle yaşanan artışı gösterir veriler için *bkz.* Türkiye Bankalar Birliği, "Dijital, Internet ve Mobil Bankacılık İstatistikleri (Rapor Kodu: DT22)", 2023, 1.

[14] "16 milyar liralık vurgun nasıl yapıldı? İşte Türkiye'nin konuştuğu Samsunlu Gezek kardeşler...", Hürriyet, https://www.hurriyet.com.tr/gundem/16-milyar-liralik-vurgun-nasil-yapildi-iste-turkiyenin-konustugu-samsunlu-gezek-kardesler-42028241 Erişim 12 Ekim 2024.

ortaya konulacaktır. Ardından meselenin Yargıtay tarafından nasıl nitelendirildiği tespit edilecektir. Konuya dair içtihat, mer'i mevzuat bağlamında değerlendirilecektir. Söz konusu içtihada dair literatürdeki görüşlere de yer verilecektir. Nihayet Yargıtay'ın içtihadına dair eleştirilerimiz ve meselenin yine mer'i mevzuata göre çözümüne dair kanaatimiz sunulacaktır.

Belirtmemiz gerekir ki literatürde, Yargıtay'ın konuya dair içtihadını ele alan pek çok önemli eser bulunmaktadır. Banka muhasebe kayıtlarında değişiklik yapılarak sahte mevduat bakiyesinin oluşturulması ve bu bakiyenin çeşitli biçimlerde kullanılması davranışlarının adım adım irdelenmesi suretiyle bunların hangi suçların tipikliğini karşıladığı ve birbirleriyle olan içtima durumları hususlarındaki değerlendirmelerimizin, bu çalışma ile literatüre sağlamayı amaçladığımız özgün katkıyı ihtiva ettiği umulmaktadır. Sonuç bölümünde, varılan neticenin kısa bir özetinin yanında, olması gereken hukuk (*de lege feranda*) bağlamında güncel ihtiyaçlara uygun ve sürdürülebilir bir çözüm[15] olduğunu düşündüğümüz bir kanun değişikliği önerisi de yer alacaktır.

Çalışma, inceleme konusu fiillerin hangi suçların tipikliğini karşıladığı sorunuyla sınırlıdır. Konu bütünlüğünün sağlanması ve bağlamın korunması maksadıyla, okuyucunun zaten aşina olduğu, zikredilecek suç tiplerine dair genel açıklamalara yer verilmeyecektir.

I. BANKA HESABI VE PARA HAVALESİ KAVRAMLARI

Bankacılık faaliyeti, hesap tutma temeline dayanır. Böylece bankaların işlemlerinin denetlenebilir ve izlenebilir olması sağlanır. Bu hem bankalar ile çalışan kişiler hem de resmî makamlar bakımından hayatî önemdedir.[16] Öyle ki 5411 sayılı Bankacılık Kanunu'nun[17] 37 ilâ 42. maddelerini kapsayan dördüncü bölümü, finansal raporlama hususuna hasredilmiştir. Ayrıca banka muhasebesi, muhasebe biliminin gereklerinin yanı sıra oldukça geniş kapsamlı bir ikincil mevzuata tabidir.[18]

A. BANKA KAYITLARININ İŞLEVİ

Banka mevduat sözleşmesi, niteliği bakımından kendine özgü bir sözleşme olmakla birlikte[19], usulsüz vedîa ve tüketim ödüncü (karz) sözleşmesinin niteliklerini haizdir.[20] Bu itibarla

[15] Bilişim alanındaki suçların güncel ihtiyaçları gözeterek yeniden ele alınması ve işin niteliğine uygun, sürdürülebilir düzenlemeler yapılması gerekmektedir. *Bkz.* Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları", *Denetişim*, sayı 8 (2011): 84.

[16] Mesut Yıldırım, *Banka Muhasebesi*, 1. baskı (İstanbul: Türkiye Bankalar Birliği, 2008), 25.

[17] RG. 01.11.2005/25983.

[18] Yıldırım, *Banka Muhasebesi*, 26.

[19] Konuya ilişkin tartışmalar hakkında detaylı bilgi ve aynı yöndeki kanaat için bkz. Beyza Er, "Mevduat Sözleşmesinin Tanımı, Kurulması ve Türleri", *Türkiye Adalet Akademisi Dergisi* 13, sayı 49 (2022): 499–505.

[20] İsa Başbüyük, "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", *Ceza Hukuku Dergisi* 8, sayı 21 (2013): 197–214; Nuri Erdem, "Vadelerine Göre Mevduat Hesabı Türleri", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi* 1, sayı 2 (2004): 253–72.; *"…mevduat ödünç (karz) ile usulsüz vedia akitlerin karışımı kendine özgü niteliği bulunan bir sözleşme türü olmaktadır."* Yargıtay 11. Hukuk Dairesi, E. 1988/4712, K. 1988/4063, T. 17.6.1988; *"…mevduat, ödünç (karz) ile usulsüz vedia sözleşmelerinin niteliklerini taşıyan kendine özgü bir sözleşmedir."* Yargıtay 11. Hukuk Dairesi, E. 1989/7057, K. 1989/6640, T. 27.11.1989.

bankaya yatırılan para, bankanın mülkiyetine geçer, mudiin ise bankadan bir alacak hakkı doğar.

'Havale', mevduat alacağının, bankanın bir başka müşterisine temlikinden başka bir işlem değildir.[21] Havale işlemi, bankaya verilen havale talimatı çerçevesinde banka kayıtlarında, bir hesaba para çıkışı ve bir diğerine para girişi kaydının düşülmesiyle gerçekleşmektedir. Günümüzde bankalar, bu kayıtları dijital ortamda tutmakta ve banka müşterilerinin bilişim sistemleri yoluyla verecekleri havale emirleri doğrultusunda, banka kayıtları, sistem tarafından otomatik olarak değiştirilmektedir.

Alıcının bir başka bankanın mudii olması durumunda bankalar arasında borcun da devri gerekebilir. Bankalar arasındaki iletişim, Türkiye Cumhuriyeti Merkez Bankası tarafından sağlanan Elektronik Fon Transferi (EFT) ve Fonların Anlık Transferi (FAST)[22] veya Belçika merkezli Dünya Bankalararası Finansal Telekomünikasyon Derneği (*SWIFT*)[23] gibi kanallar aracılığı ile sağlanır.

B. Banka Muhasebe Kayıtları Üzerinde Oynanması

Banka kayıtları üzerinde oynama yapmak için bu kayıtların muhakkak dijital ortamda tutulması şart değildir. Ancak fizikî ortamdaki kayıtlar üzerinde oynama yapmak, hayatın olağan akışı içerisinde, bu kayıtları elinde bulunduran banka görevlileri tarafından, bankacılık zimmeti gibi suçların işlenmesi veya işlenen suçun delillerinin ortadan kaldırılması maksadıyla gerçekleşir.

Üçüncü bir kişinin fizikî kayıtlar üzerinde oynama yapma fırsatı yakalaması hayli düşük bir ihtimâldir. Fizikî ortamda tutulan kayıtlara müdahale edilebilmesi için ya bu defter ve belgelere bizzat erişebilecek biçimde, bankanın muhtemelen üçüncü kişilere açık olmayan kısımlarına bir şekilde girmeyi başarmak yahut yine fizikî olarak verilecek bir havale emrini sahte şekilde imzalayarak banka memurunu aldatmak ve dolaylı faillik suretiyle hesaplarda değişiklik yaptırtmak gerekir. Bu son ihtimâlde dolandırıcılık suçunun unsurları da değerlendirilmeye değerdir. Fail bir şekilde banka kayıtlarına erişmeyi başarabilirse, defterlerde kendisi tehine yaptığı tahrifatı, banka çalışanlarını aldatmak ve olmayan bir mevduat bakiyesini tahsil etmek için kullanabilir. Fiziken tutulan defter ve belgeler üzerindeki oynamaların belgede sahtecilik teşkil edeceği şüphesizdir. Böylece hesaba geçirilen parayı elde etmek için bankanın mevduat alacaklısı gibi şubeden tahsil gerekeceğinden, dolandırıcılık suçu da sübut bulmuş olacaktır.

Dijitalleşme, yalnız hesap kayıtlarında değil, ayrıca bu kayıtlarda yapılacak değişikliklere esas olacak havale emirlerinde de söz konusu olmuştur. Nitekim artık internet ve mobil bankacılık kanalları üzerinden verilen havale emirleri, banka bilişim sistemlerindeki otomasyonu

[21] Başbüyük, "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", 205.

[22] Türkiye Cumhuriyeti Merkez Bankası, Elektronik Fon Transfer Sistemi - Elektronik Menkul Kıymet Transfer Sistemi - Fonların Anlık ve Sürekli Transferi (FAST) Sistemi, https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Sistemleri/Turkiyedeki+Odeme+Sistemleri/Elektronik+Fon+Transfer+%28EFT%29+Sistemi, Erişim 22 Ekim 2025.

[23] Society for Worldwide Interbank Financial Telecommunication,https://www.swift.com/about-us/who-we-are, Erişim 22 Ekim 2025.

tetiklemekte ve banka kayıtları otomatik olarak değişmektedir. Bir anlamda banka kayıtları, artık doğrudan doğruya banka müşterileri tarafından değiştirilebilmektedir. Dolayısıyla banka kayıtlarında değişiklik yapmak isteyen failin, bankanın kapalı odalarına girmesine gerek kalmamıştır. Örneğin fail, bir şekilde, bankanın müşterisine sunduğu bilişim sistemine girebilirse, o müşteriye hasredilmiş banka hesaplarında kolaylıkla değişiklik yapabilecektir. Hatta fail, bir şekilde, bankanın bilişim sistemlerine daha kapsamlı bir müdahalede bulunabilecek teknik imkân yakalamış ise bankanın tüm kayıtları üzerinde oynama yapabilecektir. Bilişim sistemleri yoluyla banka kayıtlarının değiştirilmesi, çalışmamız bağlamında ele alınması gereken temel fiildir.

Banka hesap kayıtlarını hukuka aykırı biçimde değiştirdikten sonra failin hesabındaki bakiyeyi kullanabileceği birden fazla yol bulunmaktadır. Bunun ilki, parayı bir ATM'den çekmektir. İkincisi de failin şubeye giderek mevduatını tahsil etmesidir. Üçüncü yol ise çevrimiçi bankacılık hizmetleri yoluyla bir başkasına havale yapmak yahut banka şubesine giderek bir başkası lehine havale emri vermektir.

II. KAYDÎ PARA İÇTİHADI

Teknolojik ilerlemelerin görülmemiş bir hızla hayatımıza farklı açılardan dâhil olması ve günlük alışkanlıklarımızı hızla değiştirmesi karşısında, suç fiillerinin yaygınlaşması veya çeşitlenmesi şaşırtıcı da değildir. Elbette ki kanunkoyucudan teknolojinin getireceği her bir yeniliği ve bu yeniliklerin nasıl suistimâl edilebileceğini öngörmesi beklenemez. Ancak hukukun bu gelişmelere uyum sağlamada hızlı olması önem arz etmektedir. Hukukun, teknolojiyi takip etmesi iki türlü anlaşılabilir: İlki, yasama yoluyladır ki; günceli takip etmek ve hatta ileriyi görüp gerekli kanunları ihdas etmek işi, kanunkoyucuya düşmektedir. Diğeri ise içtihadın, teknoloji vasıtasıyla işlenen fiilleri mevcut kurallar bağlamında en doğru biçimde nitelendirmesiyle olur.

Hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesinin bir nitelikli hâl olarak mevzuata girişi, 5237 sayılı TCK ile olmuştur.[24] Bundan önce, klâsik bir suçun internet vasıtasıyla işlenmesi, doktrinde daha ziyade, internetin yayımcılık işlevi bakımından değerlendirilmekteydi.[25] Öte yandan TCK m. 244/4 hükmüne benzer bir düzenleme, 3756 sayılı Kanun[26] ile 765 sayılı TCK'ya iki fıkra hâlinde eklenen m. 525b hükmünde[27] yer almaktaydı.

[24] Selman Dursun, "Malvarlığına Karşı Suçlar", *Hukuki Perspektifler Dergisi*, sayı 2 (2004): 102.

[25] Bu yönde bir değerlendirme örneği için *bkz.* Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", 107 ff.

[26] RG. 14.06.1991/20901.

[27] (1) Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmiIyon liradan ellimilyon liraya kadar ağır para cezası verilir.
(2) Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir.

Türkiye'de ilk internet bankacılığı uygulaması ise 1997 yılında, İş Bankası ve Garanti Bankası öncülüğünde olmuştur.[28] Mobil bankacılık ve internet bankacılığı kanallarının, müşterilere, banka hesapları üzerinde doğrudan değişiklik yapmalarına imkân tanıması, inceleme konusu fiillerin ortaya çıkmasına da zemin hazırlamıştır.

Yargıtay, kaydî para içtihadını oluştururken, internet bankacılığını konu alan suçlar hayli yeni bir olguydu. TCK m. 244/4 ise daha önce var olan 765 sayılı TCK m. 525b'nin yeni kanundaki karşılığından[29] ibaret görülmekteydi. Bilişim araçları vasıtasıyla hırsızlık suçuna ilişkin düzenlemeleri doğrudan konu alan kapsamlı bir literatür ise henüz oluşmamıştı. Bu koşullar altında ortaya çıkan içtihadında, Yargıtay, dijital banka kayıtlarının bilişim sistemleri vasıtasıyla değiştirilmesini banka hesabında bakiye olan kişinin bu parasını almak yorumlamıştır. Paranın maddî varlığına dokunulmasa da kaydî bir paranın alındığı ileri sürülerek, işlenen fiil, bilişim araçları vasıtasıyla hırsızlık olarak nitelendirmiştir. Söz konusu içtihadın ardından bu fiillerin hangi suç tipi çerçevesinde değerlendirilmesi gerektiği konusunda önemli sayıda eser ortaya konulmuştur. Fakat Yargıtay'ın sonraki tarihli içtihadında meseleyi doktrindeki görüşler ışığında yeniden değerlendirdiği bir kararına rastlanılamamıştır.

A. İÇTİHADIN MUHTEVASI

Kaydî para içtihadı, Yargıtay Ceza Genel Kurulu'nun,

> "Yargıtay Ceza Genel Kurulu'nca çözümü gereken uyuşmazlık, sanığın 765 sayılı TCY'nin 525/b-2. maddesine uyan eyleminin, suç tarihinden sonra yürürlüğe giren 5237 sayılı TCY'nin 244/4. maddesine mi, yoksa 142/2-e maddesine mi, uyan suçu oluşturduğuna ilişkindir. (…) Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş bank Ankara K. .. Şubesindeki hesabından 10.750 YTL'yi Ş ... bank-İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır."[30]

şeklindeki kararı ile oluşmuştur. Yargıtay Ceza Genel Kurulu, banka hesapları arasında hukuka aykırı bir transfer şeklindeki banka kayıtlarının değiştirilmesi fiillerini, 'kaydî paranın'

[28] Tuba Özkan ve Osman Berna İpekten, "İnternet Bankacılığı Kullanımını Etkileyen Faktörler: Atatürk Üniversitesi Personeli Üzerine Bir Uygulama", *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 21, sayı 2 (2017): 651.

[29] TCK m. 244 hükmünün, TCK m. 525b'nin yeni kanuna tamamlayıcı bir norm olarak alındığı hakkında *bkz.* Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk Ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 14, sayı 2 (2010): 291.; Burada tamamlayıcı normdan maksat, bu suç tipinin bağımsız bir suç tipi olmaması anlamında değildir. Kastedilen, TCK m. 244'te yer alan *"…başka bir suç oluşturmaması halinde…"* ifadesinden hareketle, eğer fiil, bu hükmün yanında başkaca bir suç tipini oluşturuyorsa o hükmün uygulama alanı bulacak olması, TCK m. 244/4'ün uygulanmayacağıdır.

[30] Yargıtay Ceza Genel Kurulu, E. 2009/11-193, K. 2009/268, T. 17.11.2009.

çalınması olarak görmüştür. Ceza Genel Kurulu'nun kabulü, özel daire kararlarına yansımış[31] ve yerleşmiştir. Güncel içtihat, bilişim sistemlerinin kullanılması suretiyle hırsızlık (TCK m. 142/2-e) suçunun oluşacağı, paranın havalesiyle suçun tamamlandığı yani paranın çekilmesine dahi gerek bulunmadığı yönündedir.[32] Netice itibariyle Yargıtay, hırsızlık suçunun taşınır bir eşya olması gereken maddî konusunu, banka hesap kayıtlarındaki bakiyenin, yani 'kaydî paranın' oluşturabileceği kanaatindedir.

B. Kaydî Para İçtihadına Dair Literatür

Yargıtay'ın kaydî para içtihadına literatürdeki pek çok eserde değinilmektedir. Bu içtihadı destekleyen yazarlar olduğu gibi içtihadı eleştirilen yazarlar da söz konusudur.

Doktrinde *Aytekin,* kaydî para içtihadını desteklemektedir. Yazara göre, bu surette işlenen bilişim yoluyla hırsızlık suçunda, failin, hisse senedi, altın veya para gibi taşınırlara temas etmeden, bilişim sistemleri yoluyla bunları temsil eden verileri kendi hâkimiyeti altına alması söz konusudur.[33] *Dülger,* suça konu verinin alelade bir veri olmayıp parayı temsil ettiği hatta mudiin burada verisini değil, parasını kaybettiğini ileri sürmüştür. Yazar, yaptığı değerlendirmede, Yargıtay'ın kaydî para içtihadının, mevzuatın amacına uygun ve isabetli olduğu sonucuna varmıştır.[34] *Koca ve Üzülmez* de kaydî para içtihadını destekleyen yazarlardandır. Yazarlara göre, TCK m. 142/2-e ile TCK m. 244/4 arasında aslî norm - talî norm ilişkisi söz konusu olduğundan ve bir başkasının hesabından hukuka aykırı biçimde kendi hesabına para havalesi yapan kimsenin fiili, bilişim sistemleri yoluyla hırsızlık teşkil ettiğinden, TCK m. 244/4 değil, TCK m. 142/2-e'de düzenlenen nitelikli hırsızlık suçu oluşur.[35]

Hakimlik ve savcılık mesleğini icra eden yazarların da genel olarak söz konusu içtihadı desteklediği görülmektedir. Örneğin, Yargıtay 8. Ceza Dairesi Üyesi olan *Özsoy* tarafından kaleme alınan çalışmada, 'veri' kavramının, somut bir eşya niteliği olmadığı ve hırsızlık suçuna konu olamayacağı belirtilmiştir. Ancak TCK m. 142/2-e hükmünün bu kurala bir istisna

---

[31] *"…sanığın, katılanın banka hesabına internet bankacılığı aracılığıyla girilip mevduatında bulunan paranın isme havale edilmesi şeklindeki eyleminin, TCK.nın 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde, TCK.nın 244/4. maddesi uyarınca mahkumiyet hükmü kurulması,"* Yargıtay 8. Ceza Dairesi, E. 2021/11212, K. 2021/20923, T. 15.11.2021.

[32] "*Suç tarihinde katılanların Yapı Kredi Bankası Kurtköy Şubesi'nde bulunan ortak hesabındaki 20.000 YTL paranın, sanık ...'e ait Türkiye Ekonomi Bankası (tasfiye olan Fortisbank)'nın Küçükbakkalköy Şubesi'ndeki hesaba aktarıldığı ve şüpheli bir durum olduğunun fark edilmesi sebebiyle, ilgili banka görevlileri tarafından hesaba bloke konulmak suretiyle sanığın suça konu parayı çekmesinin engellendiği somut olayda; katılanların hesabından rızaları dışında havale yapılması ile paranın sanığın fiili hakimiyet alanına geçtiği ve suçun tamamlandığı, bu andan sonra sanığın parayı bankadan çekmemesinin suçun tamamlanmış olmasına etki etmeyeceğinin anlaşılması karşısında; eylemin teşebbüs aşamasında kaldığı belirtilerek sanık hakkında TCK'nın 35. maddesi uygulanmak suretiyle eksik ceza tayini aleyhe temyiz olmadığından bozma nedeni yapılmamış;"* Yargıtay 2. Ceza Dairesi, E. 2020/18556, K. 2021/10530, T. 26.5.2021.

[33] Murat Aytekin, *Bilişim Sistemleriyle İşlenen Hırsızlık ve Dolandırıcılık Suçları*, 1. baskı (Ankara: Seçkin Yayıncılık, 2024), 59.

[34] Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 10. baskı (Ankara: Seçkin Yayıncılık, 2023), 511, 512, 517 ff.

[35] Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, 8. baskı (Ankara: Adalet Yayınevi, 2022), 721 ff.

getirdiğini ileri sürmüştür.[36] Benzer şekilde *Eker*, bir başkasının hesabından kendi hesabına para transfer eden kimsenin, o parayı mal edinme kastı bulunduğunu, paranın hesaba aktarılmasının da 'alma' fiili teşkil ettiğini savunmaktadır[37]. Yazara göre burada, çalınan, veri olmayıp verinin temsil ettiği paradır ve somut bir varlıktır ve dolayısıyla suçun maddî konusu mevcuttur.[38]

Doktrinde söz konusu fiilin hırsızlık suçunu ilgilendirdiğini kabul etmekle birlikte meseleye temkinli yaklaşan ve kimi durumlarda TCK m. 244/4 hükmünün de gözetilmesi gerektiğini düşünen yazarlar da bulunmaktadır. *Mahmutoğlu,* verinin hırsızlık suçunun konusunu oluşturamayacağı ancak bir kimsenin internet bankacılığına girip kendi hesabına para havale eden failin amacı parayı elde etmekse, söz konusu havalenin paraya giden bir anahtar olduğu ve TCK m. 142/2-e hükmünün uygulama alanı bulması gerektiği[39], bu bakımdan Yargıtay'ın kaydî para içtihadının kendi görüşlerini doğrular nitelikte olduğu kanaatindedir.[40] Diğer taraftan Yazar, failin amacı, parayı elde etmek değil de yalnızca başkasının hesabındaki parayı kendi hesabına geçirmek yani veriyi taşımaksa, bu durumda, TCK m. 244/4 hükmünün uygulanacağını belirtmektedir.[41]

Hırsızlık suçunda alınması gereken, suçun maddi unsuruna karşılık gelen, taşınır bir mal (eşya) olup *Aşkın ve Yeğrim'*e göre, bilişim sistemleri yoluyla bir taşınır eşyayı almak fiilen oldukça zordur. Yazarlara göre, bilişim sistemleri yoluyla ya da bir bilişim sistemindeki veriye müdahale ederek menfaat elde edilmesi durumunda ise, somut olayın koşullarına göre, dolandırıcılık veya TCK m. 244/4 bağlamında değerlendirme yapılmalıdır. Dolayısıyla hırsızlık suçunun bilişim sistemleri kullanılarak işlenmesine dair TCK m. 142/2-e hükmünün uygulama alanı bir hayli dardır.[42]

Başbüyük, kaydî paranın taşınır eşya niteliği bulunmadığı için hırsızlık suçunun konusunu oluşturamayacağını açıkça belirtmektedir. Yazara göre, hırsızlık suçu yalnızca mülkiyeti değil zilyetliği de konu almasına karşın; banka kayıtlarının değiştirilmesinde zilyetliğe yönelik bir fiil bulunmamaktadır.[43] *Özbek, Doğan ve Bacaksız*, otomatik yükleme sistemine sahip bir cihaz vasıtasıyla işlenen hırsızlık fiilinin, bilişim yoluyla hırsızlık olarak nitelendirilebileceğini; ancak maddî bir varlığı olmayan verinin, hırsızlığa konu olamayacağını dile getirmektedir. Yazarlara göre, Yargıtay'ın kaydî para içtihadında isabet bulunmamakta olup söz konusu fiil,

[36] Nevzat Özsoy, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK. 243 ve 244)", *Yaşar Hukuk Dergisi* 1, sayı 2 (2019): 331ff.
[37] Hüseyin Eker, *Açıklamalı-İçtihatlı Hırsızlık Suçları*, 1. baskı (Ankara: HUKAB Yayınları, 2013), 142.
[38] Eker, 143.
[39] Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 71, sayı 1 (2013): 881.
[40] Mahmutoğlu, 882.
[41] Mahmutoğlu, 881 ff.
[42] Uğur Aşkın ve Korhan Yeğrim, "Hırsızlık Suçunda Malın Bulunduğu Yerden Alınması", *Trabzon Üniversitesi Hukuk Fakültesi Dergisi* 1, sayı 1 (2023): 57.
[43] Başbüyük, "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", 167.

TCK m. 244/4 hükmünde düzenlenen bilişim suçunu oluşturur.[44] *Tezcan, Erdem ve Önok*, Yargıtay'ın kaydî para içtihadını, kripto varlıklar üzerinden sınamışlardır. *Yazarlar*, kripto-paraların veriden ibaret olması, başka bir ifadeyle, temsil ettikleri maddî bir varlığın söz konusu olmaması üzerinde durarak; Yargıtay'ın kaydî para içtihadının bu veriler bakımından da geçerli olup olmadığının önemli bir sorun teşkil ettiğini ifade etmektedirler.[45] *Yıldız*, burada maddî varlığa sahip bir verinin çalınmasının söz konusu olmadığı kanaatindedir. Yazara göre, failin kastının aslında para elde etmek olduğu noktasından hareketle verilen kaydî para içtihadı kanunilik prensibine aykırı niteliktedir.[46] Esasen failin kastına uygun çözüm de failin TCK m. 244/4 hükmünden sorumlu tutulmasıdır.[47]

Yargıtay, yukarıda zikredilen kararlarında, fiil neticesinde hesabındaki bakiye azalan mudiin malvarlığı değerinin azaldığını ve failin malvarlığının arttığını savunmaktadır. Ancak *Ketizmen*, Yargıtay'ın kaydî para görüşünün benimsenmesi hâlinde, hırsızlık suçunun mağdurunun kim olduğunu ele alan çalışmasında, mudiin malvarlığı değerinde doğrudan bir azalma olmadığını ortaya koymuştur: Yazar, esasen bulunduğu yerden alınan bir mal söz konusu olmadığından bu fiilin, hırsızlık değil, bilişim suçu yoluyla menfaat sağlama olduğunu belirtmiştir.[48] Ancak Yargıtay'ın kaydî para görüşünün benimsenmesi hâlinde de 'çalınan' paranın hem mülkiyetinin hem de zilyetliğinin bankaya ait olması nedeniyle hırsızlık suçunun mağdurunun, hesabındaki bakiyesi azalan mudi değil, banka olduğu sonucuna varmıştır.[49] Buna göre mudiin, bankadan mevduat alacağı devam etmektedir; ancak bankanın gördüğü zarar bakımından kusuru varsa, kusuru oranında bu alacağından indirim yapılacaktır.[50]

C. Değerlendirme

Kaydî parayı taşınır bir eşya olarak nitelendirmek ve banka dijital hesaplarında hukuka aykırı değişiklikler yapılması durumunda hırsızlık suçunun işlendiğini kabul etmek kanaatimizce isabetli değildir. Zira burada paranın ne zilyetliği ne de mülkiyeti değişmektedir. Banka, fiilden önce de sonra da paranın maliki ve zilyedidir. Her ne şekilde olursa olsun hesabına haksız biçimde para geçirmiş fail, bankadan bu parayı çekmedikçe, bankanın ne bir malvarlığı zararından ne de kaybettiği bir zilyetlikten söz edilebilir. Amerika Birleşik Devletleri'nde görülen *Shaw v. United States*[51] davasında benzer bir yorum yapılmış, bir başka mudiin hesap numaralarını kullanarak para transferi yapmak için hile yapan kimsenin, bu mudie karşı değil, bankaya karşı suç işlediği ve banka dolandırıcılığı (18 U.S.C. § 1334) suçunun oluştuğuna

[44] Veli Özer Özbek, Koray Doğan, ve Pınar Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, 18. baskı (Ankara: Seçkin Yayıncılık, 2023), 641.
[45] Tezcan Durmuş, Mustafa Ruhan Erdem, ve R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 21. baskı (Ankara: Seçkin Yayıncılık, 2023), 668 ff.
[46] M. Emre Yıldız, "İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi", *Ceza Hukuku Dergisi* 5, sayı 14 (2010): 148.
[47] Yıldız, 149.
[48] Muammer Ketizmen, "İnternet Bankacılığı Aracılığıyla Başkalarının Hesaplarında Usulsüz İşlemler Yapılması Suretiyle Yarar Sağlanmasında Suçun Mağduru", *Kırıkkale Hukuk Mecmuası* 4, sayı 2 (2024): 1003, 10. dn.
[49] Ketizmen, 1013.
[50] Ketizmen, 1013.
[51] Shaw v. United States 137 S. Ct. 462 (2016).

karar verilmiştir. Zira mudi, bankanın yalnızca alacaklısıdır, paranın mülkiyeti ise bankaya aittir.

Gerçekten, suçun mudiin zilyetliğine karşı işlendiğinin ileri sürülmesi durumunda, hırsızlık bağlamında 'alma' kavramının, medenî hukuk anlamında zilyetliğin hükmen devrini kapsamadığı, örneğin zilyetliğin havalesinin, 'almak' anlamına gelmeyeceği[52] gözden kaçırılmaktadır. Bu noktada, mudiin, çevrimiçi bankacılık yoluyla mevduatı üzerinde zilyetliğe sahip olmadığını ve alma fiilinin bu zilyetliğe yönelmesinin mümkün olmadığını ifade etmek gerekir. Zira kolay bir biçimde para havalesi yapabiliyor olmak, başka bir ifadeyle, alacağın temlikinin banka kayıtlarına işlendiğini bilişim yoluyla kolayca doğrulayabilmek, para üzerinde zilyede has bir hâkimiyet kurmak için yeterli değildir. Bu ancak alacağın temlikinin, bankacılık sistemi içerisinde kolay bir biçimde muhasebeleştirilebildiğini gösterir. Kaldı ki mudi, mobil ve internet bankacılığı parolalarına sahip olmayabilir veya belirli gün ve saatlerde bu hizmetlerin verilmesi kesintiye uğrayabilir.

Suçun maddi konusu bakımından da hırsızlık suçu oluşmamıştır. Hırsızlık suçunun işlenebilmesi için suça konu olacak bir taşınır eşyanın veya bir tarlanın üzerindeki verimli toprağın alınarak başka yere götürülmesi ya da bir binanın çatısındaki kiremitlerin, merdivenlerindeki trabzanların sökülüp götürülmesi gibi bir taşınmazdan sökülüp alınabilen bir şeyin, bir malın yani bir eşyanın varlığı gerekir.[53] 'Kaydî para' ise taşınır olmak bir yana eşya dahi değildir. Kaydî para, bankadaki somut para yerine geçen bir değer olarak da değerlendirilemez. Öyle ki uç bir örnekte, bankanın o sırada elinde mevcut olandan daha fazla bir meblağın havalesi mümkündür. Örneğin, yukarıda zikredilen *La Casa del Samsun* olayında da bankanın ilgili şubesinin ve belki de banka tüzel kişiliğinin hâlihazırda hukuka aykırı olarak hesaba geçirilen meblağda Türk lirası cinsinden mevduatının olup olmadığı tereddüt konusudur.

Netice itibariyle "alma" fiilinin gerçekleşmemesi ve "taşınır bir mal (eşya)" bulunmaması nedeniyle maddi konunun yokluğu, söz konusu fiillerin hırsızlık suçunun tipikliğini karşılamasına engeldir. Nitekim Yargıtay Ceza Genel Kurulu'nun yukarıda zikredilen kararında karşı oy kullanan beş üye, benzer gerekçelere vurgu yapmışlardır.[54] Meselenin dolandırıcılık ve hırsızlık gibi klâsik suç tiplerine sığdırılmaya çalışılmasında isabet bulunmamaktadır. Kaldı ki;

---

[52] Sulhi Dönmezer, *Kişilere ve Malvarlığına Karşı Cürümler*, 16. baskı (İstanbul, 2001), 349 ff.

[53] Faruk Erem, *Türk Ceza Kanunu Şerhi: Özel Hükümler*, 1. baskı, c. 3 (Ankara: Seçkin Yayıncılık, 1993), 2350 ff.; Dönmezer, *Kişilere ve Malvarlığına Karşı Cürümler*, 356.

[54] "*Somut olayda sanıklar bir bilişim sistemine girdikten sonra, yakınanın banka üzerindeki hesabında bulunan ve parayı temsil eden verileri önceden açtırdıkları hesaba göndermişlerdir. Kanımızca bu eylem, 5237 sayılı TCKnin 244/4. maddesinde tanımlanan, var olan verileri başka bir yere göndermek suretiyle haksız çıkar sağlanması suçunu oluşturur. TCK'da verinin taşınır mal olarak tanımlanmaması nedeniyle bu fiil hırsızlık suçuna ait norm, öncelikle uygulanması gereken asli norm niteliğini taşımaz.*
5237 sayılı TCK" veriyi taşınır bir mal olarak tanımlamadığına göre, veriyi temel almak suretiyle bilişim sistemleri kullanılarak elde edilen haksız edinimleri hırsızlık suçu olarak nitelendirmek TCK'daki" Suçta ve Cezada Kanunilik" ve "Kıyas Yasağı" ilkeleri karşısında olanaklı değildir. Bu nedenlerle somut eylemde, hırsızlık suçunun yasal unsurlarının gerçekleşmesi nedeniyle TCK'nin 142/2-e maddesinin uygulanmasının uygun olduğu yönündeki sayın çoğunluk görüşüne katılmıyorum" görüşüyle,
Diğer beş Kurul Üyesi de, benzer gerekçelerle eylemin 5237 sayılı TCY'nin 244/4. maddesine uyan suçu oluşturduğu düşüncesiyle karşı oy kullanmışlardır.", Yargıtay Ceza Genel Kurulu, E. 2009/11-193, K. 2009/268, T. 17.11.2009.

maddî varlığı bulunan eşyanın suçun konusunu oluşturduğu fiiller yüzyıllardır cezalandırılıyorken günümüzde TCK m. 244/4 gibi hükümlerin ihdası, veriler gibi maddî varlığı olmayan, soyut hususları konu alan fiillerin cezalandırılması ihtiyacından ileri gelmekte, bir bakımdan da klâsik suç tiplerinin meseleyi çözmekte yeterli olmadığını gözler önüne sermektedir.[55]

III. CEZAÎ SORUMLULUĞUN TESPİTİ

Yargıtay, yukarıda zikrettiğimiz kaydî para içtihadında, banka hesaplarına müdahale ederek kendi hesabında olmayan bir para bakiyesi oluşturan kimsenin fiilini hırsızlık olarak nitelendirmektedir. Hırsızlık konusu şeyin kaydî para olduğunu varsaymaktadır. Bu bakımdan paranın daha sonra ATM'den çekilip çekilmemesinin yahut şubeden tahsil edilip edilmemesinin bir önemi bulunmadığı gibi bir miktar mevduatın havale edilip edilmemesi de suçun oluşumu bakımından etkisiz olduğu kabul edilmektedir.

Yukarıda, suçun maddi unsurları bağlamında alma fiilinin gerçekleşmediği ve kaydî paranın, hırsızlık suçunun maddî konusunu oluşturabilecek bir taşınır eşya olmadığı yönündeki kanaatimiz izah edilmişti. Dolayısıyla söz konusu fiillerin, herhangi bir suç oluşturup oluşturmadığı ve oluşturuyorsa hangi suç tipleri kapsamında değerlendirilmesi gerektiği açıklığa kavuşturulmalıdır.

A. BANKANIN DİJİTAL MUHASEBE KAYITLARININ DEĞİŞTİRİLMESİ

Bir kimse, banka hesaplarına hukuka aykırı biçimde müdahale ederek kendi banka hesabındaki bakiyeyi olduğundan fazla göstermesi; bankadan bir mevduat alacağının bulunduğu veya bakiye alacağın miktarının gerçekten daha yüksek olduğu konusunda yanlış bir muhasebe kaydının sisteme girilmesi anlamına gelir. Söz konusu hukuka aykırı müdahale, doğrudan banka kayıtları hedeflenerek gerçekleştirilebileceği gibi bankanın müşterilerine ve çalışanlarına tahsis ettiği parolalar çalınarak da yapılabilir. Bir üçüncü yol da banka müşterileri veya çalışanlarını aldatarak hesaplarda değişiklik yaptırtmaktır.

Doğrudan banka kayıtlarını hedef alan bir müdahale, yani bankanın bilişim sistemlerine siber saldırı yoluyla girilmesi ve değişiklik, yapılması fiilleri bakımından sırasıyla; bilişim sistemlerine girilmesine dair TCK m. 243/1 hükmündeki

> "(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir." ve bilişim sistemlerinde değişiklik yapmak suretiyle menfaat sağlanmasına dair TCK m. 244/2, 3 ve 4 hükümlerindeki "(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.", "(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır." ve "(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

[55] Ramazan Doğan, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*, 1. baskı (Ankara: Adalet Yayınevi, 2014), 152.

düzenlemeleri uygulama alanı bulur. Zira bankanın bilişim sistemine hukuka aykırı biçimde girilmekte, hukuka aykırı giriş veya hukuka aykırı biçimde sistemde kalmak neticesinde verilerin değişmesi (TCK m. 243/2)[56] durumunu aşar biçimde, TCK m. 244 kapsamındaki bir fiille sahte bir havale emrini sistem kayıtlarına ekleyerek veri değiştirilmektedir. Böylece fail; kendisini veya üçüncü kişiyi, bankaya karşı mevduat alacaklısı konumuna getirmekte veya alacak bakiyesini yükseltmekte yani menfaat sağlamaktadır. Hukuka aykırı olarak girilen bilişim sisteminin sahibi bankadır.[57] Doktrinde TCK m. 243/1 çerçevesinde bilişim sistemlerine girilmesinde, bankanın yanında bilgileri görüntülenen hesap sahibinin de mağdur olduğu fikri de savunulmaktadır.[58] Aynı görüş, banka hesabındaki bakiyesi azaltılan mudi bakımından TCK m. 244 bağlamında da ileri sürülebilir. Kanaatimizce bu kimseleri, girilen sistemin ve değiştirilen verilerin sahipleri olmadıklarından mağdur olarak değil, suçtan zarar gören olarak değerlendirmek gerekir.

Parolanın ele geçiriliş biçiminin ayrıca bir suç teşkil etme ihtimâli bir yana bırakıldığında, bir şekilde ele geçirilen parolalar yahut cihazlar vasıtasıyla banka müşterilerinin veya çalışanlarının çevrimiçi bankacılık hesapları üzerinden bilişim sistemlerine girilmesi ve bu hesaplarda değişiklik yapılması hâlinde de TCK m. 243/1 ve TCK m. 244/2, 3 ve 4 hükümlerinin uygulanacağı kanaatindeyiz. Giriş için kullanılan kullanıcı adı ve parola, her ne kadar müşteri veya çalışan adına tanımlanmış olsa da bu tanımlama yalnızca söz konusu kimselerin bilişim sistemine girebilmesi konusunda bankanın gösterdiği rızayı ifade etme işlevi taşımaktadır. Yani bilişim sisteminin kullanıcına ait bir değer değildir. Bu itibarla girilen bilişim sisteminin sahibi hâlâ banka olup bu sisteme hukuka aykırı biçimde girilmesi (TCK m. 243/1) ve bankanın bilişim sistemindeki verilerin değiştirilmek suretiyle menfaat elde edilmesi (TCK m. 244/2, 3 ve 4) fiillerinin mağduru yine bankadır. Doktrinde ise burada, verinin, parola kullanılmak suretiyle değiştirildiği, yani sistemin olağan işleyişi dışında bir müdahalede bulunulmadığı ve dolayısıyla TCK m. 244/4 hükmünün uygulanamayacağı ileri sürülmektedir. Bu görüşe göre, hukuka aykırı havale, herhangi bir suç tipini karşılamaz; ancak parola ile sisteme girilmesi ve sistemde kalınması, TCK m. 243/1'in uygulanmasını gerekli kılar.[59] Kanaatimizce ise TCK m. 244/2, 3 ve 4 hükümlerinin uygulanabilmesi için veri değişikliğinin hukuka aykırı olması yeterlidir, sistemin işleyişinin aksine gerçekleştirilmesi gerekmez. TCK m. 243/3 ve TCK m. 244/2 arasındaki ayrım, bilişim sistemlerindeki verinin değişmesinin bilişim sistemine hukuka aykırı girişin bir sonucu olarak gerçekleşmesi ile sisteme girmenin ötesinde veride değişiklik yapmaya yönelik bir davranışın varlığına dayanır. Yargıtay da failin parolayı haricen öğrenerek

[56] TCK m. 243/2 hükmünün, 243/1 hükmünde düzenlenen fiillerin neticesi sebebiyle ağırlaşmış hâli olduğu konusunda *bkz.* Dülger, *Bilişim Suçları*, 279 ff.; Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", 282.

[57] Kanaatimizce, suçun mağdurunun bir tüzel kişi olmasının önünde bir engel bulunmamaktadır; zira tüzel kişiler de gerçek kişiler gibi hak süjesidir. Tüzel kişilerin suçun mağduru olabileceği yönündeki görüş için *bkz.* Meral Ekici Şahin, *Dolandırıcılık Suçu*, 1. baskı (Ankara: Adalet Yayınevi, 2019), 167.

[58] Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, sayı Özel sayı (2010): 1364.

[59] Başbüyük, "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", 209, 211.

sisteme girmesi ve verileri değiştirmesi hâlinde TCK m. 244/2 hükümlerinin uygulanabileceğini kabul etmektedir.[60]

Ele alınması gereken bir diğer sorun, bilişim sistemlerine girme (TCK m. 243/1) ve banka bilişim sistemlerinde değişiklik yaparak menfaat sağlama (TCK m. 244/2, 3 ve 4) hükümleri arasındaki ilişkidir. Bilişim sisteminde değişiklik yapma, mutlaka bilişim sistemine girmeyi gerektirmez. Sisteme dışarıdan müdahale ya da zararlı yazılımı üçüncü cihazlara bulaştırılacak türden yazılımlar, *rabbits*[61], yoluyla da bu suç işlenebilir. Bu itibarla her iki suç tipi de bilişim sistemlerinin güvenliğini konu almaktaysa da aradaki ilişkinin geçitli suç ilişkisi olduğu söylenemez. Bu nedenle içtima bakımından her bir durum özelinde inceleme yapılması gerekir.[62] Örneğin bir şekilde ele geçirilen parolayla yahut başkaca bir biçimde bilişim sistemine girilip banka muhasebe kayıtlarının değiştirilmesi fiillerinin hukukî anlamda tek fiil teşkil ettiği açıktır. Bu itibarla farklı nev'iden fikri içtima hükümleri uygulama alanı bulmalı ve daha ağır cezayı gerektiren TCK m. 244/2, 3 ve 4 hükümlerinden ceza verilmelidir.[63]

Burada, çevrimiçi bankacılık kanalıyla sahte havale emri düzenlenmesinin özel belgede sahtecilik suçunu oluşturup oluşturmayacağı da incelemeye değerdir. Her şeyden önce, dijital ortamda tutulmak, belgenin müellifinin belli olması ve hukukî değer taşıması kaydıyla, sahtecilik suçu anlamında 'belge' niteliğini haiz olmasını engellemez, meğerki bu veri müellifinin eseri olduğunu ortaya koyan bir değerden yoksun olsun.[64] Her ne kadar SMS (*Short Message*

---

[60] *"Oluşa ve tüm dosya kapsamına göre; sanığın olay tarihinde katılan şirkette satış destek uzmanı olarak görev yaptığı, katılan şirketin şirket taşımayla ilgili operasyonel süreçlerin yönetilmesi amacıyla kullandığı KOPS isimli yazılım programına giriş için her personele ayrı şifre verildiği, sanığın da bu şifreleri hukuka aykırı olarak ele geçirip yetkisi olmadığı halde veriler üzerinde düzeltmeler ve eklemeler yaptığı iddia olunan somut olayda; sanığın katılan şirkete sunmuş olduğu 14.02.2014 tarihli dilekçesinde; 2007 yılında eğitim için şirket genel müdürlüğüne gittiğinde eğitim ekranına bir başka personel olan...'ın şifresiyle giriş yaptığını gördüğü sırada bu şifreyi kullanarak diğer personellerin şifresine ulaştığını, sisteme giriş yaptığını, düzeltme ve eklemeler gerçekleştirdiğini beyan etmesi, İzmir Cumhuriyet Başsavcılığı'nın 12.09.2014 tarihli yazısında sanığın diğer şirket çalışanlarının yetkilerini kullanarak işlem yaptığına dair bilgisayar kayıtlarının çıkartılmasını yönündeki talebi karşısında; katılan şirkete ait bilgisayar kayıtlarında bilirkişi incelemesi yaptırılıp sanığın KOPS isimli yazılım programına bilgisayar kayıtları incelenerek personellerin rızası dışında ve şifrelerini kullanarak giriş yapıp yapmadığı, giriş yapmış ise verileri değiştirip değiştirmediği, erişilmez kılıp kılmadığı, veri yerleştirip yerleştirmediği hususunda bilirkişi raporu alınarak ve tüm deliller birlikte değerlendirilerek katılanın kullandığı adı geçen programa erişilmez kılındığı takdirde TCK.nın 244/2, ancak; bu programa girişin engellenmemesi ve katılanın da programda kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı dikkate alınıp sanığın hukuki durumunun takdir ve tayini gerekirken"* Yargıtay 8. Ceza Dairesi, E. 2018/415, K. 2019/6567, T. 9.5.2019.

[61] Sisteme bir kez bulaştıktan sonra dışarıdan bir komuta ihtiyaç duymaksızın, niteliğine göre kendiliğinden sistemi yavaşlatan, bozan veya sistemde değişiklik yapan hatta bulaştıkları mesajlaşma uygulamaları üzerinden üçüncü kişilerle iletişim kurabilen zararlı yazılımlar. *Bkz.* Gürkan Özocak, "Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçu ve Uygulamadaki Saldırı Türleri", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi* 21, sayı 1 (2024): 285.

[62] Dülger, *Bilişim Suçları*, 362.; Aksi yöndeki görüş ve bilişim sistemlerine girmeden veri değiştirmenin mümkün olmadığı yönündeki yargı kararı örnekleri için *krş.* Ahmet Gül, *Doğrudan - Dolaylı Bilişim Suçları*, 3. baskı (Ankara: Seçkin Yayıncılık, 2021), 113.

[63] Fikrî içtima konusu suçların, Yargıtay'ın kaydî para içtihadına paralel olarak, TCK m. 142/2-e ve TCK m. 243 hükümlerinde düzenlenen nitelikli hırsızlık ve bilişim sistemlerine girme suçları olduğu görüşü ve bu yöndeki içtihat örnekleri için krş. Aytekin, *Bilişim Sistemleriyle*, 75.

[64] *"…765 Sayılı Türk Ceza Kanunu'nun 339 ve devamı maddelerinde düzenlenen sahtecilik suçlarında suçun maddi konusu, üzerinde sahtecilik yapılan "varaka" ve "evrak" olarak tanımlanmış iken, 5237 Sayılı Türk Ceza Kanunu'nun 204 ve devamı maddelerinde "belge"den bahsedilmiş, ancak tanımı yapılmamıştır. (…) Buna karşılık, belge ile ilgili*

Service) doğrulaması ve benzeri güvenlik tedbirleri, üçüncü kişilerin kullanımını zorlaştırsa da internet bankacılığı üzerinden verilen havale emrinin, hesap sahibinin eseri olduğunu gösteren bir niteliği bulunmamaktadır. Cep telefonuna kod gönderen SMS'e doğrudan veya dolaylı olarak kimin eriştiğini bilmenin bir yolu bulunmadığı gibi; bu konuda bir karinenin mevcut olduğu da söylenemez. Çevrimiçi bankacılık yoluyla yapılan işlemlerde, asıl ispat fonksiyonu; sisteme parola ile girildiğinin, güvenlik protokolüne uygun ek doğrulamaların gerçekleştirildiğinin (üç boyutlu doğrulama, kişisel verilerin eşleşmesi, geçici parola vb.), giriş yapan cihaza ve cihazın internet bağlantısına dair bilgilerin, kullanıcının bilişim sisteminde verilen komutların, konuşma kayıtlarının ve ilgili diğer verilerin tutulduğu kütüklerin (*log*) bütün olarak değerlendirmesiyle dahi ancak sınırlı bir aşamaya kadar sağlanabilir. Kanaatimizce, bilişim sistemi içerisinde verilen banka havalesi komutları, bankadaki kayıtları otomatik olarak değiştiren verilerden ibaret olup müellifinin eseri olduğunu ortaya koyan özel bir işaret yahut veri içermediklerinden özel belgede sahtecilik suçuna konu olmazlar.

Üçüncü bir yol olarak banka muhasebe kayıtlarına müdahalenin fail tarafından gerçekleştirilmemesi, fakat yine fail tarafından bilişim sistemleri kullanılarak aldatılan banka müşterisi ya da çalışanı olan üçüncü kişilere yaptırılmasıdır. Çevrimiçi bankacılık kanalındaki sözde hatadan kaynaklı olarak sistemde görünen borcu silmek üzere arayan ve kendisini müşteri hizmetleri yetkilisi olarak tanıtan kimsenin tarif ettiği adımları izleyerek farkında olmadan para

---

başkaca yasal düzenlemelerin gerçekleşmesi, gelişen toplumsal yaşam ile özel ve kamudaki yazışmaların elektronik ortamda yapılıyor olması, sonuç olarak "belge" kavramının yeniden yorumlanmasını gerektirmiştir. Esasen Türk Ceza Kanunu'nun TBMM Adalet Komisyonu'nda görüşülmesi sırasında, belge kavramının tanımlanması tartışması yapılmıştır. Bu görüşmelerde, belgenin tanımlanmasının uygulamaya bir süre sonra dar gelebileceği vurgulanmış, bu tanımın uygulamacılar tarafından yapılmasının uygulamayı rahatlatacağı ve maddi gerçeğe ulaşmada kolaylık sağlayacağı belirtilmiştir.

Hâlihazırda kanun koyucu da birçok yasada, güvenli elektronik imza ile imzalanan bilişim sistemindeki verilerin belge hükmünde olduğunu kabul ederek, belgenin kapsamını genişletme eğilimindedir.

Genel olarak sahtecilik suçunun maddi konusu olan belgenin;

a-) Taşınır şey üzerine yazılması,

b-) Yazının belli bir kimseye ait olması (düzenleyenin belli olması),

c-) Hukuki değer taşıyan içeriğe sahip ve (hukuki bir vakayı veya bir hakkı ispata elverişli bulunması) hukuki sonuç doğurmaya elverişli olması gerekir. Yargıtay da belgeyi, "Hukuki hüküm ifade eden bir hakkın doğmasına ve bir olayın ispatına yarayan yazı" olarak tanımlamıştır.

(…)

Güvenli elektronik imza ile oluşturulan veya ilgili mevzuatında imza zorunluluğu olmayan ancak düzenleyeni belli olan (5258 Sayılı Kanun'un 5/3. maddesindeki düzenleme gibi veya işaret, mühür, etiket, amblem ya da hologramın yeterli olduğu belgeler) ve hukuki değer taşıyan içeriğe sahip olup hukuki sonuç doğurmaya elverişli elektronik verilerin, kanun hükmüyle "Belge" olarak nitelendirilmesi koşuluyla sahtecilik suçunun maddi konusu olarak kabulü, örneğin Türk Borçlar Kanunu'nun 15/1. maddesi, Türk Ticaret Kanunu'nun 1526. maddesi, İcra İflas Kanunu'nun 8/a. maddesi, 5271 Sayılı CMK'nin 38/A. maddesiyle 6100 Sayılı HMK'nin 199 ile 445. maddeleri kapsamında, UYAP sistemi ve diğer elektronik ortamlarda oluşturulan elektronik belgeleri ceza kanunu koruması altına alacaktır. Bu kabul kanunilik ilkesi ile çelişmeyeceği gibi, sahtecilik suçunun koruduğu hukuki yarar olan belgelerin gerçekliğine ilişkin kamu güveninin sarsılmasını da önleyecektir.

Nitekim Yargıtay Ceza Genel Kurulu'nun 24/01/2017 tarih ve 2016/21-1065 E.-2017/27 K. sayılı kararında; "… sanıkların gerçeğe aykırı şekilde oluşturdukları ödeme listelerini elektronik imzayla imzalamaksızın sanık K.U.'ya ait e-posta adresinden bankaya gönderdikleri olayda;… e-posta adresinden bankaya gönderilen ödeme listelerinin elektronik imza ile imzalanmamış olması nedeniyle resmi belge niteliğinde bulunmaması karşısında, sanıklara atılı kamu görevlisinin resmi belgede sahteciliği suçunun unsurlarının oluşmadığı…" görüşüyle elektronik imza ile imzalanmayan elektronik verilerin belge niteliğinde olmadığını ve sahtecilik suçunun maddi konusunu oluşturmadığını savunan Yargıtay Cumhuriyet Başsavcılığının itirazının kabulüne karar verilmiştir." Yargıtay 11. Ceza Dairesi, E. 2018/6165, K. 2021/2805, T. 18.3.2021.

transferi yapan kimse, dolandırılmış mıdır yoksa TCK m. 244/2, 3 ve 4 hükümlerinde tanımlanan, banka bilişim sistemlerinde veri değiştirmek suretiyle menfaat sağlama fiilini işleyen dolaylı failin uzayan eli (*longa manus*) mi olmuştur? Benzer bir örnek olarak, kendini polis olarak tanıtan kimseye, hakkındaki sözde soruşturmada kullanılmak üzere bir miktar para havalesi yapan kimsenin durumu da zikredilebilir. Burada hileli davranış, banka havalesinin sebebini oluşturmaktadır ve dolandırıcılık suçunun gündeme geleceği açıktır.

Kimi durumda, özellikle bankacılık hizmetlerini yalnızca ATM'den para çekmekle sınırlı olarak kullanan, çevrimiçi bankacılık kanalları konusunda tecrübe sahibi olmayan kimselerin, banka havalesi yaptıklarının bilincinde olmadan, kendilerine verilen adımları izlemesi mümkündür. Örneğin, kendisine havale yapılabilmesi için mobil bankacılığında işlem yapması gerektiği konusunda kandırılan kimseye, alacağını zannettiği tutardaki havaleyi yaptırtmak böyledir. Kanaatimizce burada da bilişim sistemlerine girmek veya banka bilişim sistemindeki verileri değiştirerek menfaat sağlamak değil, nitelikli dolandırıcılık suçu (TCK m. 158/1-f) söz konusudur. Zira burada mağdur, aldatılarak, aslında farklı bir işlem yaptığı zannıyla kendine ait mevduat alacağını devretmektedir ve bu hile, *"(b)ilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"* gerçekleştirilmektedir. Bu durumda menfaat unsuru[65], alacağın faile devriyle tamamlanacağından, paranın daha sonra nasıl kullanıldığına dair aşağıda yapacağımız açıklamaların suçun sübutu bakımından önemi bulunmamaktadır.

B. Hesaba Geçirilen Bakiyenin Kullanılması

Banka hesabındaki bakiye, çeşitli bankacılık işlemleri yoluyla mudii tarafından kullanılabilir. Banka muhasebe kayıtları üzerinde oynayarak hesabında olmayan bir bakiyeyi mevcut kılan kimsenin, bu bakiyeyi kullanmasının, ceza hukukundaki karşılığı inceleme konusu yapılmalıdır. Bu kullanımın çeşitli şekillerde gerçekleşmesi mümkün olup burada, yaygın olarak karşılaşılması mümkün olan alternatifler değerlendirilecektir.

Bir kimse hesabındaki bakiyeyi peyder pey kullanabilir. Bu kullanımın her biri, kural olarak ayrı fiil teşkil eder. Bu tekrar eden kullanımlardan, aynı suç, aynı mağdura karşı, tek bir suç işleme kararı altında gerçekleşmiş ise zincirleme suç hükümleri uygulama alanı bulur. Örneğin hesaba geçirilen paranın her ay bir bölümünün ATM'den çekilmesinde durum böyledir. Öte yandan ATM'den her biri 200 Türk lirası olan beş banknottan oluşan 1.000 Türk lirası çekmek isteyen bir kimsenin, yeterince 200 Türk lirası elde edinceye kadar, üst üste para çekmesinin tek bir fiil teşkil ettiği şüphesizdir. Bu durumda zincirleme şeklinde işlenen bir suç değil, tek bir fiille işlenen tek bir suç söz konusudur.

Burada banka muhasebe kayıtlarıyla oynanması ile hesaba geçirilen paranın kullanılması arasındaki ilişkiye de değinmek gerekmektedir. Banka hesapları üzerindeki değişikliğin, TCK m. 243/1 ve 244/2,3 ve 4 hükümlerinde yer alan suçları oluşturduğu ve hesaba geçirilen

[65] Dolandırıcılık suçunda elde edilen menfaatin herhangi bir ekonomik fayda olması yeterlidir. *Bkz.* Muhammed Yasin Yavrutürk, *Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenen Dolandırıcılık Suçu*, 1. baskı (Ankara: Adalet Yayınevi, 2023), 118; Ekici Şahin, 332.; Görünüşte bir alacağı elde etmiş olan fail, menfaat sağlamıştır. Bu menfaatin daha sonra alacağın devrinin geçersizliğiyle bertaraf edilebilecek olması suçun oluşumuna etki etmez. Hile ile elde edilen senedin hükümsüzlüğünün ispat edilmesi hâlinde, senet bedeli tahsil edilmese de menfaat koşulunun sağlandığı yönündeki örnek için *krş.* Ekici Şahin, 332 ff.

bakiyenin kullanımının da hırsızlık ve dolandırıcılık suçlarının bilişim yoluyla işlenmesi teşkil ettiği durumlarda bir fikrî içtima durumu söz konusu değildir. Zira burada bir suç, diğerinin işlenmesini mümkün kılmaktaysa da suç fiilleri farklıdır. Arada yalnızca araç suç – amaç suç ilişkisi bulunmaktadır.

Belirtmek gerekir ki; mevduat alacağının üçüncü kişiye temlikini gerçekleştirebilmek için failin mutlaka parayı önce kendi hesabına geçirmesi gerekmez. Doğrudan doğruya, başkasına ait bir hesaptan sahte havale emri düzenleyerek de hesaplarda değişiklik yapabilir. Bu durumda TCK m. 243/1 ve 244/2, 3 ve 4 hükümleri ile aşağıda zikredeceğimiz suçlar arasında fikrî içtima gündeme gelir.

1. ATM'lerden para çekilmesi

Otomatik para çekme makinesi anlamındaki *Automated Teller Machine* ifadesinin kısaltması olarak yaygın biçimde ATM adıyla hayatımızın bir parçası olan cihazlar, bankaların dijital muhasebe kayıtlarına telekomünikasyon yoluyla bağlı olup para çekme – yatırma işlevi gören bilgisayarlardır. Türkiye'de ilk defa Türkiye İş Bankası tarafından 25 Aralık 1987'de Ankara'da hizmete sunulmuş[66] olan bu cihazların günümüzde daha da yaygınlaşması ve gelişmesiyle para çekme ve yatırma dışında da pek çok bankacılık işleminin yapılması olanaklı hâle gelmiştir. Öyle ki halk arasında bu cihazlar, *bankamatik* olarak da adlandırılmaktadır.

Banka müşterisi, fizikî banka kartı ve parola kombinasyonuyla ya da mobil bankacılığa elverişli cihazlarla doğruladıktan sonra ATM'lerde işlem yapabilir. Gerek kimlik doğrulama gerekse ATM üzerinden yapılacak işlemler, tamamen otomasyona bağlı olup herhangi bir banka çalışanının dahli söz konusu değildir. Bu bakımdan banka hesabında bir şekilde gerçek dışı mevduat bakiyesi oluşturmayı başarmış kimse, ATM'den para çekerken herhangi bir insanı, bankadan mevduat alacağı bulunduğu konusunda ikna etmek zorunda değildir. Dolayısıyla insana yönelik bir hile söz konusu değildir ve dolandırıcılık suçundan söz edilemez.[67] Otomasyon, para çekme (mevduat alacağını tahsil etme) talebini, banka muhasebe kayıtlarını bilişim sistemi üzerinden doğrulayacak ve şartlar uygunsa para çekmek isteyen kimseye nakit ödeme yapacaktır. Dolaysıyla aslında var olmayan bir mevduat alacağını ATM kanalıyla tahsil eden kimse, TCK m. 142/2-e bağlamında bilişim sistemlerini kullanmak suretiyle hırsızlık suçunu işlemiş olur. Suçun mağduru, çekilene kadar paranın zilyedi olan bankadır.

2. Banka şubelerinden tahsilat yapılması

Banka şubelerinden mevduatını tahsil edecek mudi, şubeye bizzat veya temsilcisi aracılığıyla başvurmalıdır. Kimlik doğrulamasının ardından banka görevlileri tarafından çekilmek

[66] Mehmet Sığırcı, ATM: Kim, Ne Zaman İcat Etti?, https://bilimgenc.tubitak.gov.tr/makale/atm-kim-ne-zaman-icat-etti, Erişim 22.10.2025.

[67] Hilenin bir insana değil, otomasyona yöneldiği durumlarda dolandırıcılık suçunun oluşmayacağı yönünde bkz. Gani Kamışlı, *Dolandırıcılık Suçu*, 3. baskı (Ankara: Seçkin Yayıncılık, 2023), 145 ff.; Yavrutürk, *Dolandırıcılık Suçu*, 114; Fulya Korkmaz, "Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 69, sayı 3 (2020): 1424; Mahmutoğlu, "Bilişim Alanındaki Suçlar", 885.

istenen para miktarınca mevduat bakiyesinin var olduğu teyit edildikten sonra kendisine makbuz karşılığı ödeme yapılır.

Hesabındaki gerçek olmayan mevduat bakiyesini banka şubesinden para olarak tahsil etme fiilinin, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık (TCK m. 158/1-f) suçunu oluşturduğu kanaatindeyiz. Bilişim araçları vasıtasıyla dolandırıcılıktan söz edebilmek, hilenin bilişim araçları vasıtasıyla gerçekleştirilmesini, başka bir ifadeyle, mağdurun bilişim sistemine güven duyarak aldanmasını gerektirir.[68] Burada da daha önce değiştirilmiş olan dijital banka kayıtları kullanılmak suretiyle banka çalışanı, bankanın faile borçlu olduğuna ikna edilmektedir. Banka bilişim sistemlerinde söz konusu hesapta olması gerekenden daha fazla bakiye görünmesini kullanarak banka çalışanını aldatmak, dolandırıcılık suçunun hile unsurunu oluşturur. Zira kanaatimizce bilişim sistemleri vasıtasıyla işlenen nitelikli dolandırıcılık için failin bizzat bilişim sistemini değiştirmesi gerekmez. Mağdurun yanlış veri içeren bilişim sistemine güvenmesini sağlamak; örneğin, banka çalışanına bilişim sistemindeki yanlış veri üzerinden teyit edileceğini bilerek para çekme talebinde bulunan kimse icraî olarak hile fiilini gerçekleştirmiştir ve TCK m. 158/1-f hükmünden sorumlu tutulmalıdır. Bankanın bir kamu bankası olması durumunda (e) bendi ve banka hesabındaki mevduata duyulan güveni kullanarak kredi çekilmesi durumunda da (j) bendi gerçekleşmiş olacağından birden çok seçimlik ağırlaştırıcı sebep gerçekleşeceğinden temel cezanın belirlenmesinde alt sınırdan uzaklaşılmalıdır.

Dikkat edilmesi gereken husus; gerçek olmayan mevduat bakiyesinin oluşturulması sırasındaki eylemlerin TCK m. 243/1, 3 ve 244/2, 3, 4 kapsamında suç teşkil etmesi durumunda içtima hükümlerinin ne şekilde uygulanacağıdır. Eğer bilişim sistemine girilmesi ve sistemin değiştirilmesi, bilişim suçu oluşturacak şekilde, fail tarafından gerçekleştirilmiş ise ve mevduatın tahsili fiili ile zaman, mekân, failin planı, fiilin sosyal değeri gibi ölçütler bağlamında tek bir fiil teşkil ediyorsa farklı nev'iden fikrî içtima gereğince yalnızca en ağır cezayı gerektiren suçtan, nitelikli dolandırıcılık suçundan, ceza verilmelidir. Aksi durumda iki ayrı fiil, iki ayrı suç bulunmaktadır.

Burada suçun mağduru kavramı üzerinde de durmak gerekir. Eğer suçun mağdurunun tüzel kişi olamayacağı görüşü savunulursa, suçun mağduru, dolandırılan banka memuru olup suçtan zarar gören ise bankadır.[69] Ancak tüzel kişilerin suçun mağduru olabileceği görüşü benimsenirse, bu durumda, bankayı mağdur kabul etmek gerekecektir. Bu kabulün sonucu olarak, farklı banka çalışanlarına karşı, farklı zamanlarda hile yapılarak para çekilmesi hâlinde, suç, aynı mağdura, bankaya, karşı işlenmiş olacağından zincirleme suç hükümleri de uygulama alanı bulacaktır.[70]

[68] Korkmaz, "Dolandırıcılık Suçunun", 1427.
[69] Bu yöndeki görüş için *bkz*. Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 17. baskı (Ankara: Seçkin Yayıncılık, 2024), 117.
[70] Ekici Şahin, *Dolandırıcılık Suçu*, 168 ff.

3. Mevduat borç ve alacağının transferi

Kendi banka hesabında aslında sahibi olmadığı bir mevduat bakiyesi bulunan kimse, bu bakiyeyi üçüncü bir kişiye havale edebilir. Kişi, bu havaleyi, çevrimiçi bankacılık kanallarıyla yapsa dahi bilişim sistemlerine hukuka aykırı biçimde girmeden söz edilemez. Zira kendisine tahsis edilen kullanıcı ve parola ile işlem yapmıştır.

Olmayan bir alacağın üçüncü bir kimseye devredilmesi durumunda, somut olayın koşulları içerisinde, özellikle üçüncü kişiden mal veya hizmet alınmışsa, nitelikli dolandırıcılık suçu (TCK m. 158/1-f) gerçekleşir. Örneğin failin, bir cep telefonu satın alımında, banka havalesi yoluyla ödeme yapması ancak aslında hesabında böyle bir mevduat bakiyesi bulunmaması durumunda; kendisine devredilen alacağın gerçek olduğu zannıyla hareket eden cep telefonu satıcısı, dolandırıcılık suçunun mağduru olmuştur. Burada olmayan bir mevduat alacağı hileli biçimde var gösterilmiş ve bunun devri karşılığında cep telefonu alınmıştır. Hileli davranış, bilişim araçları vasıtasıyla gerçekleştirilmiştir. Bu nedenle dolandırıcılık suçunun nitelikli hâli (TCK m. 158/1-f) söz konusudur. Bir güven kurumu olan bankanın[71], cep telefonu satıcısı ile arasındaki sözleşme veya başka bir gerekçeyle ödeme yapıp yapmayacağı, dolandırıcılık suçunun oluşumu bakımından önemli değildir. Bankanın veya sigorta şirketinin cep telefonu satıcısına ödeme yapması durumunda, alacağa halef olması söz konusu olsa dahi suçun mağduru, banka veya sigorta şirketi olarak değerlendirilemez.

Üçüncü kişiye yapılan havale ivazsızsa, örneğin bağışlama söz konusuysa, üçüncü kişinin dolandırıldığı söylenemez. Ancak faili, başkasının hesabındaki bakiyeyi önce kendi hesabına aktarmışsa ve daha sonra üçüncü kişiye aktarım gerçekleşmişse, ilk aşamada burada tek bir fiil olup olmadığı incelenmeli ve eğer hukukî anlamda tek fiil söz konusu değilse ikinci bir bilişim suçunun işlendiği kabul edilmeli, ancak zincirleme suç (TCK m. 43/1) hükmünün uygulanması cihetine gidilmelidir.

Kendisine havale yapılan üçüncü kişinin, bankanın durumu bilerek yaptığı ödeme hariç olmak üzere, parayı çekmesi veya tahsil etmesi durumunda, bankaya karşı işlenen nitelikli hırsızlık veya nitelikli dolandırıcılık suçları da dolaylı faillikle gerçekleştirilmiş olur. Bunun için elbette ki çekilen tutarın, üçüncü kişinin gerçekte var olan mevduat alacağından fazla olması gerekir. Bu hâlde kanaatimizce iki ayrı içtima incelemesi yapılmalıdır. Birincisi hesapların değiştirilmesi ile paranın ATM'den yahut şubeden çekilmesini sağlamak fiilleri arasındadır ki buna dair açıklama yukarıda mevcuttur. İkinci içtima ilişkisi ise üçüncü kişinin hem ATM'den hem de şubeden para çekmesi durumudur. Dolaylı failin uzamış eli (*longa manus*) konumundaki üçüncü kişi, bankadan paraları farklı zaman ve yerlerde alsa da dolaylı fail açısından değerlendirildiğinde üçüncü kişinin bu şekilde davranmaya sevk edilmesi bakımından fiiller kısmî bir aynılık içerisindedir ve hukukî anlamda tek bir fiil söz konusudur. Farklı nev'iden fikrî içtima hükümlerine göre en ağır cezayı gerektiren suçtan hüküm kurulmalıdır.

[71] Necati Meran, *Dolandırıcılık – Sahtecilik – Güveni Kötüye Kullanma*, 4. baskı (Ankara: Seçkin Yayıncılık, 2016), 213; Abdurrahman Savaş, "İnternet Bankacılığı ve Tarafların Yükümlülükleri", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 19, sayı 2 (2011): 160, https://doi.org/10.15337/SUHFD.2017.87.

Fail, hukuka aykırı olarak kendi hesabına geçirdiği bakiyeyi, başka bir bankadaki kendisine veya üçüncü kişiye ait bir başka mevduat hesabına transfer edebilir. Böyle bir durumda, alıcı üçüncü kişi ise bu kişi bakımından alacağın temliki söz konusu olacağı gibi; bankalar arasında da olmayan bir borcun nakli ortaya çıkacaktır. Diğer bir bankaya borcun naklinde ise bankalar arası cari hesap kesildiğinde, bir bankadan diğerine olmayan bir borcun ödemesi söz konusu olur. Hesapları onaylayıp ödeme yapan çalışanlar, bilişim sistemi yoluyla aldatılmak suretiyle, birinci banka zarar ettirilerek ikinci banka lehine menfaat sağlanmıştır. Dolayısıyla nitelikli dolandırıcılık suçu sübut bulur.

4. Banka yatırım araçlarının satın alınması

Bankalar, paralarını Türk lirası olarak değerlendirmek istemeyen mudilerine birtakım seçenekler sunmaktadır. Altın ve döviz hesapları ile bunlara endeksli Türk lirası hesapları buna örnektir. Bu tür yatırım araçları satın alındığında, esasen, farazî bir alım satım söz konusudur; yani banka, o paranın karşılığınca 'altın' alıp kasaya koymamaktadır. Bu işlemler yoluyla yapılacak yatırımlar ile mevduattaki bakiye artırılabilir veya azaltılabilir. Eğer mevduattaki para, faizli bir mevduat hesabına yatırılmışsa, bu defa, bakiyenin azalması söz konusu olmaz; ancak bakiyenin artışı, belirlenen mevduat faizi oranında gerçekleşir.

Esasen bir şekilde kendi hesabında gerçek dışı bir bakiye oluşmasıyla fail, banka karşısında bir alacaklı görünümü elde eder. Fail, bu gerçek olmayan mevduat bakiyesini elde ettiği gibi faizli mevduat hesabına yatırıyorsa veya yatırım araçları satın alıyorsa, hâlâ tek bir fiil ve suç söz konusudur. Ancak özellikle bu araçların satın alınma zamanı gibi somut olayın özelliklerinden, bu yatırım araçlarını satın almanın yahut parayı faizli mevduat hesabına yatırmanın, bütünlük arz etmeyen, yeni bir fiil olduğu görülüyorsa, banka sistemlerinde bir değişiklik daha yapılmış olur. Yani TCK m. 244/2, 3 ve 4 çerçevesinde yeni bir veri değiştirme yoluyla menfaat temini söz konusu olur. Menfaatin gerçekleşmesi için gerçek olmayan bakiyede bir artış gerçekleşmesi gerekir, eğer yatırım araçları kâr getirmezse yalnızca verileri değiştirmekten sorumluluk doğar. Gerçek olmayan mevduat bakiyesinin şubeden veya ATM'den çekilmesine dair yukarıdaki açıklamalarımız geçerliliğini korumaktadır.

Yatırım işlemlerinin otomasyonla değişik şubeden yapılmasında dolandırıcılık suçu söz konusu olur. Bu durumda sahip olmadığı bir parayla yatırım yapmak konusunda banka çalışanına talimat veren fail, bankanın bilişim sistemlerindeki sahte kayıtları kullanarak hile yapmaktadır. Bu yolla eğer sahte bakiye yönünden pozitif bir görünüm elde edilmişse, bu kâr kullanılsın veya kullanılmasın, nitelikli dolandırıcılık suçu tamamlanır. Kâr elde edilememişse teşebbüs aşamasında kalır. Kâr elde edildikten sonra zarara geçilmesi, suçun oluşumunu etkilemez.

C. Yeni Bir Suç Tipine Duyulan İhtiyaç

Belirtilmelidir ki Yargıtay'ın benimsediği çözüm, çok daha pratiktir. Tespit ettiğimiz neticeler ise uygulamada hayli zorluk çıkartabilecek karmaşıklıktadır. Ancak hukuka aykırı bir çözümün ne kadar pratik olduğunun hiçbir ehemmiyeti yoktur. Üstelik TCK m. 244/4, banka hesaplarındaki bakiyenin artırılması veya azaltılmasında yaptırım yönünden yetersiz kalmaktadır. Yine de nitelikli hırsızlık suçunun bu fiiller bakımından tipikliği karşılamadığı,

kaydî para içtihadının ceza hukukunun temel prensiplerine uygun düşmediği açıktır. Mevcut kanunî düzenleme çerçevesinde yapılacak incelemenin ise birden çok değişkene bağlı olması ve karmaşık bir incelemeyi zorunlu kılması karşısında uygulamada güçlük arz edeceği görülmektedir. Zira oluşturulan sahte mevduat bakiyesinin kullanılacağı çeşitli ihtimallerin ne şekilde gerçekleştiğini her bir somut olayda araştırıp hukukî niteliğini ve sonuçlarını analiz etmek, hukuk uygulaması için azımsanmayacak bir yüktür. Kanunun açık ve anlaşılır olmasının yanında mahkemelerin iş yükü de gözetilerek, mer'i mevzuatın, teknolojik gelişmelerle uyumlu hale getirilmesi gerekmektedir.

Olması gereken hukuk (*de lege feranda*) bağlamında, bilişim sistemleri vasıtasıyla banka muhasebe kayıtlarının hukuka aykırı olarak değiştirilmesini suç sayan ve bu yollarla elde edilen mevduat bakiyesinin kullanılmasını da cezayı ağırlaştıran bir nitelikli hâl olarak düzenleyen bir kanun hükmünün ihdasının isabetli olacağı kanaatindeyiz. Böylece hem ceza miktarı yönünden işlenen fiilin ağırlığı ile orantılı bir ceza verilmiş hem de bir özel norm ihdas edilerek karmaşık içtima durumları bertaraf edilmiş olacaktır.

Kanaatimizce, yapılacak yeni düzenlemede yaptırım belirlenirken TCK m. 142, 244 ve 245 hükümlerindeki ceza miktarları dikkate alınmalıdır. Ayrıca, suçun yıkıcı etkileri karşısında faili eski durumu iade etmeye teşvik eden düzenlemelere yer verilmelidir. Bu çerçevede, TCK'ya aşağıdaki şekilde bir madde eklemenin isabetli olabileceği düşünülmektedir:

Banka Bilişim Sistemlerinin Kötüye Kullanılması Madde 244/A-

(1) Bir banka veya kredi kurumuna ait bilişim sistemine hukuka aykırı olarak giren, sistemde kalan veya verileri değiştiren, bozan ya da yok eden kişi hakkında iki yıldan dört yıla kadar hapis cezasına hükmolunur.
(2) Birinci fıkradaki fiil sonucunda kendisi veya başkası lehine haksız bir mevduat bakiyesi veya alacak kaydı oluşturan kişi hakkında, altı yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur. Hakkında iddianame düzenlenmeden önce haksız mevduat bakiyesini yahut alacağı eski durumuna iade eden kimse hakkında verilecek hapis cezası yarı oranında azaltılır.

SONUÇ

Bilişim sistemleri vasıtasıyla bir başkasının banka hesabı bakiyesinin değiştirilmesi ve bu şekilde hesaba geçirilen bakiyenin kullanılması fiilleri mer'i mevzuat bağlamında (*de lege lata*) değerlendirildiğinde failin eylemlerini somut olay özelinde değerlendirmek gerekir. Yerleşik yargı uygulamasında ise banka hesap kayıtlarının değiştirilmesi, kaydî bir paranın alınması olarak sayılmakta ve fiilin nitelikli hırsızlık teşkil ettiği kabul edilmektedir. Oysa bu farazî değerin gerçek bir eşya yerine konularak hırsızlık suçuna konu edilmesi kanunilik prensibine uygun düşmez.

Kanaatimizce; failin, banka bilişim sistemine hukuka aykırı girmesi (TCK m. 243/1) ve dijital muhasebe kayıtlarını değiştirerek kendisine haksız bir mevduat alacağı (menfaat) sağlaması, TCK m. 244/2, 3 ve 4 hükümlerindeki bilişim sistemindeki verileri değiştirerek menfaat sağlama suçunu oluşturur. Bu iki suç arasında farklı nev'iden fikri içtima (TCK m.

44) ilişkisi olup fail daha ağır cezayı gerektiren TCK m. 244/4 hükmünden sorumlu tutulmalıdır. Fail daha sonra bakiyeyi bir ATM'den çekerse, insana karşı hile unsuru bulunmadığından ve parayı bir makineyi maniple ederek makineden 'aldığından' nitelikli (bilişim sistemini araç olarak kullanarak) hırsızlık" (TCK m. 142/2-e) suçunu işlemiş olur. Fail, eğer bakiyeyi bir banka gişesinden çekerse yani banka görevlisini sahte dijital kayıtlara dayanarak aldatıp hile yoluyla ödeme alırsa veya bakiyeyi mal veya hizmet alımı için bir üçüncü kişiye havale ederek olmayan bir alacağın temlikiyle menfaat edinirse, nitelikli dolandırıcılık suçu (TCK m. 158/1-f) söz konusu oluşur. Bu suçların farklı biçimlerde gerçekleşmesi, birlikte veya ayrı ayrı işlenmesi gibi ihtimaller de dikkate alındığında içtima hükümlerinin uygulanması güçlük arz eder.

Gerek kanunilik prensibinin gereklerini sağlayan gerekse ihlâl ile orantılı bir yaptırımın belirlenmesi adına kanaatimizce bir kanunî düzenlemenin yapılması yerinde olacaktır. Teknolojik gelişmelerin gündelik hayatımızda yaptığı köklü değişiklikten ileri gelen bu eylemleri klâsik suçlarla benzerlik kurarak çözmeye çalışmak veya tüm 'verileri' arz ettiği nitelikleri gözardı ederek tek bir hükümde toplamak ihtiyaca cevap verememektedir. Bu yaklaşımlar, ceza hukukunun temel prensiplerini ihlâl etmekte ve her bir somut vakayı bir başka labirente dönüştürmektedir. Bu nedenle, olması gereken hukuk (*de lege feranda*) kapsamında bir kanun değişikliğinin yapılarak banka bilişim sistemlerini konu alan özel bir suç tipi getirilmesinin, yaptırımın belirlenmesinde benzer suçlara verilen cezaların gözetilmesinin yanında faili eski durumun iadesine teşvik eden hükümlere yer verilmesinin yerinde olacağı düşünülmektedir.

KAYNAKÇA

Aksoyer, Ali. "Banka hesap şifrelerini kıran 'hacker' iş üstünde yakalandı", 03 Eylül 2006. https://www.hurriyet.com.tr/gundem/banka-hesap-sifrelerini-kiran-hacker-is-ustunde-yakalandi-5022308, Erişim 12 Ekim 2024.

Altunok, Ebru, ve Ali Fatih Vural. "Bilişim Suçları". *Denetişim*, sayı 8 (2011): 74–84.

Aşkın, Uğur, ve Korhan Yeğrim. "Hırsızlık Suçunda Malın Bulunduğu Yerden Alınması". *Trabzon Üniversitesi Hukuk Fakültesi Dergisi* 1, sayı 1 (2023): 47–73.

Aytekin, Murat. *Bilişim Sistemleriyle İşlenen Hırsızlık ve Dolandırıcılık Suçları*. 1. baskı. Ankara: Seçkin Yayıncılık, 2024.

Başbüyük, İsa. "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi". *Ceza Hukuku Dergisi* 8, sayı 21 (2013): 197–214.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, sayı 1-2 (Milenyum Armağanı) (2000): 545–55.

Doğan, Ramazan. *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*. 1. baskı. Ankara: Adalet Yayınevi, 2014.

Dönmezer, Sulhi. *Kişilere ve Malvarlığına Karşı Cürümler*. 16. baskı. İstanbul, 2001.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. 10. baskı. Ankara: Seçkin Yayıncılık, 2023.

Durmuş, Tezcan, Mustafa Ruhan Erdem, ve R. Murat Önok. *Teorik ve Pratik Ceza Özel Hukuku*. 21. baskı. Ankara: Seçkin Yayıncılık, 2023.

Dursun, Selman. "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler". *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni* 23, sayı 1-2 (Prof. Dr. Gülören TEKİNALP'e Armağan) (2003): 251–94.

Dursun, Selman. "Malvarlığına Karşı Suçlar". *Hukuki Perspektifler Dergisi*, sayı 2 (2004): 190–96.

Eker, Hüseyin. *Açıklamalı-İçtihatlı Hırsızlık Suçları*. 1. baskı. Ankara: HUKAB Yayınları, 2013.

Ekici Şahin, Meral. *Dolandırıcılık Suçu*. 1. baskı. Ankara: Adalet Yayınevi, 2019.

Er, Beyza. "Mevduat Sözleşmesinin Tanımı, Kurulması ve Türleri". *Türkiye Adalet Akademisi Dergisi* 13, sayı 49 (2022): 491–516.

Erdağ, Ali İhsan. "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)". *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 14, sayı 2 (2010): 275–303.

Erdem, Nuri. "Vadelerine Göre Mevduat Hesabı Türleri". *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi* 1, sayı 2 (2004): 253–72.

Erdoğan, Yavuz. "Bilişim Sistemine Girme ve Kalma Suçu". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, sayı Özel sayı (2010): 1363–1433.

Erem, Faruk. *Türk Ceza Kanunu Şerhi: Özel Hükümler*. 1. baskı. C. 3. Ankara: Seçkin Yayıncılık, 1993.

Ersoy, Yüksel. "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları". *Ankara Üniversitesi SBF Dergisi* 49, sayı 3 (1994): 149–83.

Gül, Ahmet. *Doğrudan - Dolaylı Bilişim Suçları*. 3. baskı. Ankara: Seçkin Yayıncılık, 2021.

Hürriyet. "16 milyar liralık vurgun nasıl yapıldı? İşte Türkiye'nin konuştuğu Samsunlu Gezek kardeşler...", https://www.hurriyet.com.tr/gundem/16-milyar-liralik-vurgun-nasil-yapildi-iste-turkiyenin-konustugu-samsunlu-gezek-kardesler-42028241, Erişim 12 Ekim 2024.

Kamışlı, Gani. *Dolandırıcılık Suçu*. 3. baskı. Ankara: Seçkin Yayıncılık, 2023.

Karaca, Muhammet, ve Ensar Gül. "Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları". *Bilişim Hukuku Dergisi* 1, sayı 3 (2021): 1–30.

Karagöl, Yaşar. "Bilişim Suçları ve Önlemler". *Eskişehir Barosu Dergisi*, sayı 1 (2003): 65–66.

Keskin, Serhan. "Banka Müşterilerinin İnternet Bankacılığı Kullanmama Nedenlerinin Analizi". *Kırıkkale*

Üniversitesi Sosyal Bilimler Dergisi 9, sayı 1 (2019): 99–110.

Ketizmen, Muammer. "İnternet Bankacılığı Aracılığıyla Başkalarının Hesaplarında Usulsüz İşlemler Yapılması Suretiyle Yarar Sağlanmasında Suçun Mağduru". *Kırıkkale Hukuk Mecmuası* 4, sayı 2 (2024): 1001–15.

Koca, Mahmut, ve İlhan Üzülmez. *Türk Ceza Hukuku Genel Hükümler*. 17. baskı. Ankara: Seçkin Yayıncılık, 2024.

Koca, Mahmut, ve İlhan Üzülmez. *Türk Ceza Hukuku Özel Hükümler*. 8. baskı. Ankara: Adalet Yayınevi, 2022.

Korkmaz, Fulya. "Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi". *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 69, sayı 3 (2020): 1415–36.

"Londra'da siber saldırıya gözaltı: 5 bin kullanıcının banka bilgileri tehlikede! - Son Dakika Teknoloji Haberleri | NTV Haber". https://www.ntv.com.tr/teknoloji/londrada-siber-saldiriya-gozalti-5-bin-kullanicinin-banka-bilgileri-tehlikede1gZx1Y6c2keFLGd0gihWbw, Erişim 13 Kasım 2024.

Mahmutoğlu, Fatih Selami. "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 71, sayı 1 (2013): 855–89.

Meran, Necati. *Dolandırıcılık – Sahtecilik – Güveni Kötüye Kullanma*. 4. baskı. Ankara: Seçkin Yayıncılık, 2016.

Özbek, Veli Özer. "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 4, sayı 1 (2002): 101–58.

Özbek, Veli Özer, Koray Doğan, ve Pınar Bacaksız. *Türk Ceza Hukuku Özel Hükümler*. 18. baskı. Ankara: Seçkin Yayıncılık, 2023.

Özkan, Tuba, ve Osman Berna İpekten. "İnternet Bankacılığı Kullanımını Etkileyen Faktörler: Atatürk Üniversitesi Personeli Üzerine Bir Uygulama". *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 21, sayı 2 (2017): 647–64.

Özocak, Gürkan. "Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçu ve Uygulamadaki Saldırı Türleri". *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi* 21, sayı 1 (2024): 257–91.

Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK. 243 ve 244)". *Yaşar Hukuk Dergisi* 1, sayı 2 (2019): 295–352.

Savaş, Abdurrahman. "İnternet Bankacılığı ve Tarafların Yükümlülükleri". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 19, sayı 2 (2011): 137–66.

Sığırcı Mehmet. ATM: Kim, Ne Zaman İcat Etti?, https://bilimgenc.tubitak.gov.tr/makale/atm-kim-ne-zaman-icat-etti, Erişim 22.10.2025.

Society for Worldwide Interbank Financial Telecommunication,https://www.swift.com/about-us/who-we-are, Erişim 22 Ekim 2025.

Tutak, Serdar. "Mobil bankacılık işlemlerinde 'halka açık Wi-Fi kullanmayın' uyarısı". Anadolu Ajansı, https://www.aa.com.tr/tr/ekonomi/mobil-bankacilik-islemlerinde-halka-acik-wi-fi-kullanmayin-uyarisi/3348749, Erişim 12 Ekim 2024.

Türkiye Bankalar Birliği. "Dijital, Internet ve Mobil Bankacılık İstatistikleri (Rapor Kodu: DT22)", 2023.

Türkiye Cumhuriyeti Merkez Bankası, Elektronik Fon Transfer Sistemi - Elektronik Menkul Kıymet Transfer Sistemi - Fonların Anlık ve Sürekli Transferi (FAST) Sistemi, https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Sistemleri/Turkiyedeki+Odeme+Sistemleri/Elektronik+Fon+Transfer+%28EFT%29+Sistemi, Erişim 22 Ekim 2025.

Uzun, Uğur, ve Murat Berberoğlu. "İnternet Bankacılığı Hizmetlerinin Banka Performansı Üzerine Etkisi". *Uluslararası İktisadi ve İdari İncelemeler Dergisi*, sayı 20 (2018): 51–62.

Yavrutürk, Muhammed Yasin. *Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenen Dolandırıcılık Suçu*. 1. baskı. Ankara: Adalet Yayınevi, 2023.

Yıldırım, Mesut. *Banka Muhasebesi*. 1. baskı. İstanbul: Türkiye Bankalar Birliği, 2008.

Yıldız, M. Emre. "İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi". *Ceza Hukuku Dergisi* 5, sayı 14 (2010): 129–50.

EXTENDED SUMMARY

Unauthorized Alteration of Bank Accounting Records through Information Systems

Assist. Prof. Burak Boz
Ankara Sosyal Bilimler University, burakboz.phd@gmail.com
https://orcid.org/0000-0002-8282-3523

Unauthorized access to banking information systems, alteration of accounting records and misuse of balances generated by such activities represent crimes that are increasingly encountered due to the rapid advancement of technology. This article examines how these acts are addressed within the framework of the Turkish Penal Code (TPC) and highlights typicality issues in the current legal framework. Drawing on Turkish Court of Cassation precedents, doctrinal interpretations, and proposed legislative amendments, it provides a comprehensive analysis of how these crimes should be classified under the current law. The focus is on unlawful acts carried out through internet and mobile banking systems, determining their characters within the scope of crimes such as unlawful entry into information technology systems (TPC art. 243/1), manipulation of data for unlawful gain (TPC art. 244/2, 3 and 4), qualified theft (TPC art. 142/2-e) and qualified fraud (TPC art. 158/1-f).

The article criticizes the established position of the Turkish Court of Cassation, which considers changes made to digital banking records and the resulting balances as "theft of recorded money", i.e., theft committed through information systems. The Court argues that "recorded money" constitutes a value representing tangible funds, and therefore the perpetrator's intention was to obtain this value unlawfully. Accordingly, the transfer of funds – regardless of whether they are subsequently used or not – is classified as qualified theft under Article 142/2-e of the TPC. However, this approach has been criticized on the grounds that it contradicts the principle of legality, given that recorded money does not have a physical form and therefore cannot serve as the material object of the theft. Some authors argue that these actions should be considered cybercrimes under Articles 243 and 244 of the TPC. On the contrary, some doctrinal views support the Court's interpretation and suggest that recorded money functions as a tangible element in digital transactions and therefore can be 'stolen'.

The article goes beyond summarizing these discussions and conducts an in-depth analysis of how these actions are classified under current law. It examines various scenarios, including the creation and subsequent use of altered account balances, and addresses situations such as ATM withdrawals, branch transactions, investment transactions, and third-party transfers.

This article argues that actions involving unauthorized access to banking systems and changes in account balances should be classified as illicit access to IT systems (TPC art. 243). Meanwhile, creating altered balances constitutes obtaining an unlawful benefit

through data manipulation (TPC art. 244/2, 3, and 4). In addition, if such balances are obtained fraudulently, for example by deceiving bank customers or employees, the crime of qualified fraud (TPC art. 158/1-f) occurs.

The article considers scenarios such as withdrawing money using altered balances at ATMs, requesting altered deposits at bank branches, investing in some banking instruments and transferring non-existent funds to third parties, and provides a detailed legal classification for each. The absence of human deception in ATM withdrawals leads to their classification as theft through information systems. In contrast, branch transactions and banking investment involving deceiving bank employees with altered bank accounts are considered qualified fraud. However, it is necessary to make profit to complete fraud on banking investments, otherwise attempted fraud would be occurred. On the other hand, it should be assessed whether there is a new data change in purchasing investment instruments from bank automation with a non-existent balance or depositing this amount into an interest-bearing deposit account, and if there is a new act, it should be accepted that a new manipulation of data for unlawful gain has been committed. However, if there is no increase in the non-existent deposit balance, no benefit is provided within the meaning of the TPC art. 244/4, only the data is manipulated. At last, fraudulent use of altered balances to purchase goods or services from third parties is considered a form of qualified fraud.

The article suggests legal reforms in its conclusions to increase the effectiveness of addressing these crimes. It suggests that actions involving unauthorized changes to bank accounting records through information systems and the abuse of the resulting balances should be defined as specific criminal offenses. It also suggests that the abuse of these balances should be considered an aggravating factor that requires more severe penalties. Such changes aim to ensure justice by providing clear and precise legislation and to reduce the workload of the courts.