"TÜRK CEZA HUKUKU'NDA BİLİŞİM SUÇLARI" ESKİ TCK BAĞLAMINDA HUKUKUMUZDA YER ALAN İLK DÜZENLEMELER VE 5237 SAYILI YENİ TÜRK CEZA KANUNU'NUN İLGİLİ HÜKÜMLERİNİN YORUMU

Ö. Umut EKER*

GİRİŞ

Teknoloji, sıklıkla insanoğlunun maddi gelişiminin ve uygarlığının somut görüngüsünü teşkil edebilecek nitelikte bir gelişmişlik ölçütü olarak ele alınmaktadır. Ve onun getirisi olan her türlü yenilik de toplumsal alanda çok kısa bir süre içerisinde yankı bulmaktadır. Söz konusu etki ise, toplumun bu tür bir yeniliğe hazır olma derecesi, uyum gösterme kabiliyeti, yeniliğin niteliği ve kapsamı ve toplumun yeniliği algılayış şekline göre hem müspet hem de menfi biçimlere bürünebilmektedir. Hukuk da topluma düzen kazandırmayı ve bireyler arası/toplumsal ilişkileri de hak ve nesafet, adalet ilkeleri çerçevesinde yeniden biçimlendirmeyi amaç edindiğinden ötürü söz konusu teknolojik yeniliklere karşı da bir tavır almak zorunda kalmaktadır. Böylece hayatın dinamiği, hukuku yenilikler karşısında canlı, devingen ve güncel olmaya zorlamaktadır.

Nihayetinde dört bir yanımızın elektronik/elektromanyetik ağlarla örülü olduğu ve bilgisayarların hayatımızın ayrılmaz bir parçası haline gelmeğe başlandığı günümüzde, bilişim sistemlerinin toplumsal yaşamla iç içe bulunduğu ölçüde özel bir hukuki rejimle düzenlemeye ihtiyaç göstermesi doğal bir sonuç olarak karşımıza çıkmaktadır. İşte gereksinilen bu hukuki düzenleme biçimlerinden bir kısmını da cezai düzenlemeler teşkil etmektedir. Zira gerçek anlamda iletişim özgürlüğünün tesisi için de özgürlük anlamından kopan hak ihlallerinin ve diğer gayri meşru-

* Ankara Barosu üyesi.

lukların da önleyici yahut telafi edici mekanizmalarla engellenmesi gereklidir. Bu bağlamda, konumuz giderek yaygınlaşan sosyo-teknolojik, sosyo-kültürel bir görüngünün hukuki çerçeveye oturtulması açısından işlenmeye muhtaçtır.

A. BİLİŞİM SUÇU NE DEMEKTİR?

Bilişim suçlarını incelerken öncelikle bazı temel kavramların aydınlatılması lazım gelir. Bu çaba gerek konunun daha anlaşılır kılınması gerekse de ceza hukukunun temel ilkelerinden kanunilik ilkesinin muğlaklık/ belirsizlik handikabıyla zedelenmemesi için gereklidir.

Bilişim (informatics, informatique) terimi ana hatlarıyla, bilginin sayısal ve elektronik olarak işlenmesi sonucu her türlü verinin saklanması, otomatik olarak işlenmesi, yeniden düzenlenmesi ve aktarılması hallerini ifade eder.[1] Bununla birlikte, bilişim, bilgi-işlem, veri-işlem olarak da ifade edilen süreçleri betimlemek için de kullanılmaktadır.[2]

Bu yoldan bilhassa vurgulanması gereken önemli bir husus da şudur: Bilgisayar (computer) ile bilişim sistemleri (informatic systems, data-processing systems) birbirlerinden ayrı olarak mütalaa edilmesi gereken kavram ve fenomenlerdir. -Bu konudaki açıklama birazdan (aşağıda) yapılacaktır.-

I. Terminoloji ve Tanım Sorunu

Ceza hukuku açısından tipiklik unsurunun gereğince tebarüz ettirilmesi ve kanunilik ilkesinin muğlak kavramlarla sakatlanmaması amaçları doğrultusunda iyi ifade edilmiş, sınırları belirlenmiş bir tanım yapmak önemlidir. Bilişim suçları gibi hukukun alanına yeni dahil olmuş, henüz yeterince işlenmemiş/oturmamış teknik bir olgunun da tanımlanıp müesseseleşebilmesi için multi-disipliner bir yaklaşım içerisinde ilgili alanların uzmanlarının ortak bir çalışma yapması olgunun

---

1 Bkz., Ersoy, Yüksel, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *AÜSBFD,* C. 49, S. 3-4, 1994, s. 151; Aydın, Emin D., *Bilişim Suçları ve Hukukuna Giriş,* Doruk Yayınları, Ankara 1992, s. 3; Yenidünya, Caner - Değirmenci, Olgun, *Mukayeseli Hukukta ve Türk Hukukunda- Bilişim Suçları,* Legal Yayıncılık, İstanbul 2003 (bundan sonra bu eser kısaca *Bilişim Suçları* olarak anılacaktır): s. 27.

2 *Bilişim Suçları,* s. 28.

aydınlatılması, sınırlarının anlaşılması ve her şeyden önce tanımlama kriterlerinin belirlenmesi gerekmektedir. Doktrinde öne sürülen söz konusu ölçütler genelde şunlardan ibarettir:

• "*Bu kriterlerden ilki, bilgisayarın amaç veya araç olmasını arayanların ileri sürdüğü görüştür. Bu görüş, bilgisayarın fiilin aracı ya da hedefi olduğu davranışları bilişim suçları olarak tanımlamaktadır.*"[3]

• Bu ölçütte bilişim suçları esasen malvarlığı aleyhine suçlar hipotezi üzerinden algılanmaktadır. "*Bu görüşe göre, bilişim suçları elektronik veri işlem tesisi verileriyle konu bağlantısı olan, kasıtlı ve hukuka aykırı malvarlığı ihlalleridir.*"

• "*Üçüncüsü, bilişim sistemleriyle herhangi bir şekilde bağlantılı olan suçları esas alan kriterdir. Bu kriteri ileri süren Parker'a göre, bilişim suçları bilgisayarla ve veri iletişimiyle bağlantılı mağdur veya mağdurların zarar gördüğü veya görme ihtimali olduğu her tür suçu kapsamaktadır.*

• *Dördüncüsü, bilgisayar kullanımını esas alan kriterdir. Bu kriteri esas alan görüş, bilişim suçlarının işlenmesinde bilgisayar kullanımının zorunlu olmasını suçların belirleyici özelliği olarak kabul etmektedir.*

• *Beşincisi, suçu işleyen faili esas alan kriterdir. Bilişim suçlarını belirleyebilmek için ileri sürülen bu kriterde, sınırlandırma, bilgisayar bilgisine sahip olanların işlendikleri suçlar açısından yapılmaktadır.*"[4]

Doktrindeki tanımlamalar sıklıkla bu ölçütlerden yola çıkılarak yapılmaktadır. Fakat üzerinde uzlaşma sağlanmış genel bir tanım henüz ortaya çıkmış değildir. Tanımlama sorunu aynı zamanda olgunun yeniliğinin yanı sıra bilişim teknolojilerinin sürekli devinim ve gelişme içerisinde bulunması ve dolayısıyla her geçen gün bir yeniliğin ve varolan teknolojilerin farklı, değiştirilmiş/dönüştürülmüş biçimlerinin (varyasyonlarının) gündeme gelmesi gibi sebeplerden kaynaklanmaktadır. Böylece kanun koyucular bilişim suçlarını kesin sınırlar çerçevesinde tanımlamaktan çekinmişler, yapılan tanımlar ise sıklıkla genellemeler, betimlemeler düzeyinde bırakılarak bilişim teknolojilerinde yakın gelecekte gerçekleştirilecek yeniliklere açık hale getirilmeye çalışılmıştır.

---

[3] Akbulut, Bozdoğan Berrin "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* Milenyum Armağanı, C. 8, S. 1-2, 2000, s. 550.

[4] Akbulut, *a.g.y.*, s. 550.

Doğrusu o ki, güncel gelişmeler, söz konusu endişelerin yersiz olmadığını göstermektedir.

Tanımlama hususundaki bir başka sorun da söz konusu olgunun adı açısından çıkmaktadır. Olguyu adlandırma çabalarında gündeme farklı isimlerle karşılaşılmaktadır. Amerikan doktrininde yaygın olarak kullanılan *"bilgisayar suçları"*[5] (computer crimes) tabirinin yanı sıra, *"bilgisayar bağlantılı suç"* (computer-related crime), *"bilgisayar-yardımlı suç"* (computer-assisted crime), *"bilgisayara karşı suçlar"* (crimes against computer) ve hatta *"siber suçlar"* (cyber crimes), *"ileri teknoloji suçları"* (high-tech crimes) ve *"teknolojik suçlar"* (techno-crimes) terimlerinin de kullanıldığı görülmektedir.[6] Ancak tüm bu terim enflasyonuna karşın bilişim tabirinin kullanılması ve yaygınlaştırılması/standartlaştırılması çok daha isabetli bir yaklaşım olacaktır. Çünkü bilişim terimi, bilgisayara nazaran daha kapsayıcı ve üst bir kavramdır; bilgisayarı da kapsamakla birlikte bilgisayar destekli cihazları, elektronik/elektromanyetik diğer bilişim sistemlerini ve daha önemlisi sadece veri-işlemi ve depolanmasını değil, ayrıca veri-iletişimini de bünyesinde barındırmaktadır. Dar anlamda bilgisayar, her ne kadar en yaygını olsa da genel anlamda bilişim sistemlerini ifade etmek için açık ve seçik biçimde yetersizdir. Hatta bu nedenlerden ötürü bilişim sistem ağları ile işlenen birtakım suçlara *"internet suçları"*[7] adı verildiği, bazen de internet dışındaki diğer bilişim sistemi ağlarını da kapsar biçimde bir üst kavram olarak siber-uzay tabirinden yola çıkılmak suretiyle *"siber suçlar"* teriminin de tercih edildiği görülmektedir.[8] Oysa ki, bilişim suçları teriminin kullanımı, belirttiğim

---

[5] Aslına bakılırsa "bilgisayar suçları" tabiri hukuk mantığı açısından yanlış bir yaklaşımın ifadesidir. Zira burada bilgisayar yalnızca suç vasıtası konumundadır. Hasan Dursun'un da belirttiği gibi: "Eğer bir kimse bıçakla suç işlerse nasıl biz bu durumu bıçak suçu olarak adlandırmıyorsak aynı şey burada da geçerlidir, eğer bir kimse bilgisayar ile suç işlerse biz bunu bilgisayar suçu olarak adlandırmayız, bilgisayar vasıtası ile işlenen suçlar diyebiliriz." Bkz., Dursun, Hasan, "Bilgisayar ile İlgili Suçlar", *Yargıtay Dergisi,* C. 23, S. 3, 1998, s. 339.

[6] *Bilişim Suçları,* s. 30; Beceni, Yasin, *Siber Suçlar,* III. Bölüm s. 1, http://www.hukukcu.com (03.04.2004).

[7] Yukarıdaki dipnotta vurgulandığı üzere burada da "internet suçları" tabirini kullanmak hukuk mantığı açısından uygunsuzdur. Zira suçun işlendiği ortam suçu nitelendirmek/adlandırmak amacıyla yanlış bir şekilde kullanılmaktadır. Bu bağlamda, daha doğru bir ifade olarak "internet aracılığıyla işlenen suçlar" tabiri kullanılabilirdi. Aynı doğrultuda bkz., *Bilişim Suçları,* s. 32.

[8] *Bilişim Suçları,* s. 31; Sınar, Hasan, *İnternet ve Ceza Hukuku,* Beta Basım Yayım Dağıtım, İstanbul 2001, s. 69.

üzere, çok daha genel/kapsayıcı ve yerinde/isabetli bir tercih olarak bu yeni gelişen alanın daha kolay ve tartışmasız müesseseleşmesini temin etmeye uygun ve bu suretle terim kargaşasını önleyici nitelikte bir deyimdir. Ortaya konmuş bulunan diğer ifadeler ise ancak bu genel alanın daha özeldeki kısımlarının kategorizasyonunda işlev görebilirler.

Nihayetinde ana-hatlarıyla, kapsayıcı ve karma bir tanım yapılmaya çalışılırsa, bilişim suçları -yukarıda belirtildiği biçimiyle-, bilişim araçlarına/sistemlerine karşı veya bilişim araçları/sistemleri vasıtasıyla işlenen, verilerle, veri-işlem ile veri-aktarımlarıyla ilgili olan suç şekillerine karşılık gelmektedir.

II. Kriminolojik Açıdan Bilişim Suçları

Kriminolojik açıdan bilişim suçları pek çok kere *"beyaz yaka suçları"* (white-collar crimes) kategorisinde değerlendirilmiştir. *"Beyaz yaka suçları"*, şiddete dayanmayan ve genellikle suçlunun, mesleği dolayısıyla sahip olduğu bazı yetkileri ve avantajları kötüye kullanmasıyla ortaya çıkan zimmete geçirme, güveni kötüye kullanma benzeri suçlar olup iş dünyasında yaygın olarak rastlanan suçlardandır. Bu bağlamda bilişim suçları, genellikle ekonomik amaçlarla, maddi çıkar sağlamak için işlenmektedir ve dolayısıyla maddi ceza hukuku açısından mala/ mülkiyete karşı suçlar kategorisinde ele alındığı görülmektedir (ki, bizim kanun koyucumuz da bu sistemi benimsemiş gibidir). Fakat, elbette ki diğer nedenlerin de bu suç tipleri için güdüleyici olması mümkündür. Ayrıca bu tip suçları işleyenler de sıklıkla fırsat ve ihtiras suçluları kategorisinden çıkmaktadır. Bütün bunların yanı sıra, bilişim teknolojilerindeki hızlı gelişme ve bilişim teknolojilerinin/sistemlerinin kullanımındaki artış, yaygınlık, bilişim suçlarını, kriminolojik açıdan *"beyaz yaka suçları"* çerçevesinde ele almayı güçleştirmekte, giderek olanaksız kılmaktadır.[9]

Bilişim suçları gerçekten de çok çeşitlilik arz etmektedir. *"Veri hırsızlığı"*ndan (theft of information) *"veri tahribi"*ne (malicious destruction of information) ve *"elektronik sabotaj"*a (electronic sabotage); bilişim sistem ağları vasıtasıyla dolandırıcılıktan (fraud) emniyeti suiistimale (pilferage, embezzlement); telif hakları, para, mal ve hizmet hırsızlığından (theft of copyright or money, property or services) bilgisayar sahteciliğine ka-

[9] Bkz., Aydın, *a.g.e.*, s. 33.

dar hatta kalpazanlıktan (counterfeit) adam öldürmeye (örneğin hastane kayıtlarını ağ aracılığıyla değiştirerek hastanın durumunu ağırlaştırmak suretiyle) kadar varabilen çeşitli suçlar işlenebilmektedir.[10]

İnternetin de ortaya çıkıp olağanüstü bir hızla yaygınlaşması sonucunda bilişim suçlarında da büyük bir artış görülmüş, suça elverişli bir ortam olarak internetin gelişmesiyle bu tip suçların işlenmesi hem kolaylaşmış hem de işleniş biçimleri çeşitlenmiştir.[11]

Günümüzde işlenmekte olan bilişim suçları ise genellikle internet aracılığıyla gerçekleştirilmektedir. Gerek bilgisayar korsanlarının (hacker)[12] yetkisiz giriş eylemleri yahut sistem kırıcıların (cracker) sisteme kötü-niyetle sızarak verilere zarar vermeleri veya verileri değiştirmeleri gerekse de zararlı ve casus programlar (spyware, vandalware: virüs, truva atı, solucan, mantık bombası vs.) vasıtasıyla girişilen eylemler bilişim suçlarının önemli, sık rastlanan örneklerini teşkil etmektedir.

Bu sorunların yaşanmasında ise, temelde, internette merkezi, etkin ve düzenleyici bir otorite, yönetim/denetim mekanizmasının bulunmayışı ve hatta olanaksızlığı, ihlallerin takip edilmesindeki/fark edilmesindeki güçlüklerle birlikte internetin anonim bir ortam olması ve böylece *"doğası ve hatta varlık nedeni gereği, iletişim ve ifade özgürlüğünün en yoğun ve kapsamlı olarak kullanıldığı bir alanı ifade etmesi"*[13] gibi nedenler yatmaktadır.[14]

Düşünce ve ifade özgürlüğünün olanağı/maddi koşulları ancak gerçek bir iletişim özgürlüğü ile sağlanabileceği için, bu özgürlüğün en yaygın ve yoğun bir şekilde yaşandığı internette de baskıcı/sansürcü bir yaklaşımdan ziyade, kendi iç dinamiklerini, oto-kontrol mekanizmalarını hayata geçirecek nitelikte özgürlükçü, çerçeve çizici, bürokratik kısıtlamalardan uzak bir hukuki düzenlemenin yapılması gerekmektedir.[15]

---

[10] Ayrıca bkz., Dursun, *a.g.y.*, s. 336; İlginç bir örnek olarak Lambda Moo sanal tecavüz (virtual rape) vakası hakkında bkz., Sınar, *a.g.e.*, s. 74-76.

[11] Akbulut, *a.g.y.*, s. 551.

[12] "Hacker"lar hakkında daha fazla bilgi için bkz., *Bilişim Suçları*, s. 58-60

[13] Sınar, *a.g.e.*, s. 46 ve ayrıca bkz., Sınar, *a.g.e.*, s. 31 ve 49.

[14] Bununla beraber belirtmek gerekir ki, internet içeriğinin diğer kitle iletişim araçlarına kıyasla görsel ve etkileşimli (visual & interactive) oluşu ve çok büyük kitlelere kolayca ve hızla ulaşabilmesi nedeniyle çok etkili olması, bu gücün kötüye kullanımının, suç amaçlı eylemlerin etkisini ve tehlikelilik halini arttırmaktadır.

[15] Bu konuya yönelik Amerikan Federal Yüksek Mahkemesi'nin (Supreme Court) dikkat çekici ve meşhur kararı için bkz., Sınar, *a.g.e.*, s. 94, 95.

Aslına bakılırsa bilişim suçlarının internetle birlikte ulaşmış olduğu çeşitlilik, orijinallik, geleneksel ceza hukuku kavramları ve sorumluluk biçimleri üzerinden çözüm üretilmesini olanak dışı bırakmakta ve geleneksel ceza hukuku müesseselerini zorlamaktadır. Bu bağlamda, bilişim suçlarını ayrı bir genel suç kategorisi olarak biçimlendirmek ve özel/kendine has, ciddi ve incelikli düzenlemeler öngörmek bir zorunluluk olarak karşımıza çıkmaktadır. Bu sebeplerden ötürü yapılacak hukuki düzenlemelerin de doğrudan cezalandırıcı normlara değil de nitelikli emniyet tedbirlerine ağırlık vermesi isabetli olacaktır.

B. MADDİ CEZA HUKUKU BAĞLAMINDA BİLİŞİM SUÇLARI[16]

I. Uluslararası Gelişmeler ve Mukayeseli Hukuk

Bir önceki bölümde vurgulandığı üzere, bilişim suçları, geleneksel ceza hukuku kavramları, müesseseleri ile kavranması güç olan yeni bir kriminolojik olgudur. Bu açıdan bilişim alanındaki hukuki ihlallerin cezalandırılabilmesi amacıyla ülkeler mevzuatlarında çeşitli düzenlemeler gerçekleştirme ihtiyacı duymuşlardır. Zira her ne kadar, bazılarınca, bu yeni suç biçimlerinin geleneksel suçların farklı bir ortamda, yani siber uzayda, bilişim sistemleri üzerinde ve/veya farklı teknik araçlar vasıtasıyla, yani bilişim sistemleri ve çoğunlukla bilgisayarlarla gerçekleştirilmesinden ibaret de olsa; bu yaklaşım, söz konusu olgunun "*sui generis*" (kendine has, orijinal) tabiatı ve çeşitliliği karşısında tutarlı ve isabetli değildir. Zaten bir alternatif olarak metinlerin geniş yorumlanması yaklaşımı da tercihe şayan değildir; çünkü hem ceza hukukundaki mevcut kıyas yasağı ve yoruma ilişkin kısıtlamalar (ki bu bağlamda "*maddi ceza hukukunun suç ve cezaları belirleyen hükümleri bakımından kıyas yoluyla genişletme ve kural yaratma esası uygulanamaz*"; "*in dubio pro reo*" -şüphe halinde sanık lehine yorum yapılır- ilkesi sadece ceza muhakemesi hukukunda geçerlidir) hem de suçların ve cezaların kanuniliği "*nullum crimen sine lege, nulla poena sine lege*" ilkesi bunun için hukuki anlamda ciddi ve makul/mantıki bir engel teşkil etmektedir. "*Söz gelimi dolandırıcılık suçu kişilerin aldatılmasını sağlayan uygulamalarla,*

[16] Usül hukuku açısından yaşanan sorunlar ve kovuşturmaya ilişkin hususlar için bilhassa bkz., *Bilişim Suçları,* s. 85-90, 106, 107; Sınar, *a.g.e.,* s. 86-92, 127-133; Özel, Cevat - Ahi, Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", *Güncel Hukuk,* S. 6 (Haziran 2004), s. 21-23.

mülkiyete ilişkin menfaatlerin ihlalini cezalandırmaktadır. Bu itibarla bilgisayar işlemlerine karşı işlenen füllerin dolandırıcılık sayılıp sayılmayacakları şüphelidir. Aynı suretle sahtecilik, cismi olan şeylerle ifade edilmiş beyanların, varakanın sahte olarak teşkilini gerektirir; böyle olunca bilgisayara yerleştirilmiş bilgilerin tahrifi sahtecilik teşkil etmeyebilir."[17] Benzer bir durum nas-ı ızrar suçu için de geçerlidir.[18]

İşte bu gibi nedenlerden ötürü çeşitli ülkeler mevzuatlarında yeni düzenlemeler yahut değişiklikler gerçekleştirmişlerdir. Bahsedilen düzenlemelerde temelde üç ayrı yol/yöntem benimsenmektedir:

• Bu yollardan birincisi, ceza kanunlarına bilişim suçlarına yönelik ayrıca özel hükümler eklemek şeklinde olup bu yönteme örnek olarak Fransa ve İtalya ve de bizim 1.3.1926 tarihli eski Ceza Kanunu'nun izlediği sistem verilebilir.[19] Ayrıca 5237 sayılı Yeni Ceza Kanunu'nun benimsemiş olduğu karma sistemde de yine bilişim suçlarına yönelik özel hükümler mevcuttur.

• Bir diğer yol mevzuatlarda hali hazırda yer almakta olan geleneksel suç tiplerinin yeniden tanımlanması, daha doğrusu geleneksel suç tiplerinin tariflerinin/tanımlarının genişletilmesi yahut mevcut hükümlere yeni fiillerin eklenmesi biçiminde ortaya çıkmaktadır. Bu yönteme başvuran ülkeler olarak da Yunanistan, Kanada, Finlandiya gibi ülkeler gösterilebilir.[20]

• Nihayetinde 5237 sayılı Yeni Ceza Kanunu'nun benimsemiş olduğu karma sistemin bir parçası olarak bizim hukukumuzda da benzeri düzenlemelerin yer aldığı görülmektedir. Böylece ceza kanunumuz izlediği karma sistem gereği olarak hem bilişim sistemlerine karşı suçları ayrı bir babda inceleyerek (bkz., 5237 sayılı Türk Ceza Kanunu, İkinci Kitap, Üçüncü Kısım, Onuncu Bölüm) özel hükümler ihdas etmiş hem de geleneksel suç tiplerini düzenleyen ceza normlarının birkaçına yeni modaliteler/fiiler ekleyerek (bkz., TCK 142/II-e ve 158/I-f maddeleri) tanım genişletme yolunu benimsemiştir.

---

[17] Dönmezer, Sulhi, *Kişilere ve Mala Karşı Cürümler,* Beta Basım Yayım Dağıtım, İstanbul 2001, s. 615'ten naklen.

[18] Maddi ceza hukuku açısından daha fazla bilgi için bilhassa bkz., Aydın, *a.g.e.,* 39-65.

[19] Bkz., Dönmezer, *a.g.e.,* s. 616; Sınar, *a.g.e.,* s. 98-100.

[20] Dönmezer, *a.g.e.,* s. 616.

• Sonuncu yaklaşımda ise söz konusu olguyu düzenleyen ayrı ve özel kanunlar çıkartma yolu benimsenmektedir. Bu yönteme başvuran ülkelere örnek olarak da ABD ve İngiltere gösterilebilir.

Ulusal düzeydeki çabalarla beraber bilişim suçları alanında uluslararası platformda da bazı çalışmalar yapılmış ve özellikle internetin gelişip yaygınlaşmasıyla gündeme taşınan sorunlarla, bilgisayarla bağlantılı/bilgisayar ve bilişim sistem ağlarıyla işlenen suçlarla etkin biçimde mücadele edilebilmesi amacıyla çeşitli uluslararası örgütler tarafından çalışmalar yapılarak uluslararası koordinasyonun sağlanması ve bazı kararlar alınması yoluna gidilmiştir. Bahis edilen çalışmalar sonucunda alınan kararlar, ilgili alanda gerçekleştirilen bazı eylemlerin ceza müeyyidesi ile karşılanması doğrultusunda öneriler ortaya çıkarmıştır.

"Uluslararası platformdaki ilk karşılaştırılmalı bilgisayar suçları ile ilgili ceza yasalarının birbirleriyle uyumlaştırması çalışmaları OECD bünyesinde başlatılmıştır. Bu bağlamda OECD'nin 1983 yılında başlattığı çalışmalar 1986 yılında yayınlanan 'Computer-Realted Crime: Analysis of Legal Policy' raporu ile somutlaşmıştır . Bu raporda üye ülkelere aşağıdaki ihlalleri cezai müeyyide ile karşılamaları önerilmiştir. Raporda ayrıca aşağıda sayılan ihlallerin tahdidi olmadığı ilk olarak bu ihlallerin cezai müeyyide ile karşılanması konusunda konsensüse varılması gerektiği bildirilmiştir. Bu ihlaller;

• *Bilgisayar yoluyla dolandırıcılık*

• *Bilgisayar yoluyla sahtecilik*

• *Bilgisayar program ve verilerinde değişiklik yapılması*

• *Bilgisayar programlarının telif haklarına aykırı olarak kopyalanması,-çoğaltılması ve dağıtılması*

• *Telekomünikasyon sistemlerinin,bilgisayarın diğer fonksiyonların ve iletişimin değişikliğe uğratılması"*[21] şeklinde sayılmıştır.

Bununla birlikte Birleşmiş Milletler bünyesinde gerçekleştirilen *"Sınır Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi"* sempozyumunda *"14 Aralık 2000 tarihinde düzenlenen panelde üye ülkelerin aşağıda belirtilen eylemleri cezai müeyyide ile karşılamaları önerilmiştir. Bu eylemler;*

[21] Beceni, *a.g.e.,* IV. Bölüm s. 5, 6'dan naklen.

• *Bilgisayar sistemlerine yetkisiz giriş,*

• *Bilgisayar veya bilgisayar sistemlerinin hukuka uygun kullanılmasına engel olunması,*

• *Bilgisayar sistemleri içersindeki verilerin yok edilmesi veya değiştirilmesi,*

• *Gayri fiziki ekonomik değer taşıyan objelerin çalınması,*

• *Aldatma yoluyla değer elde edilmesi (elektronik sistemleri içeren)"* şeklindedir.

Son olarak Avrupa Konseyi'nin çalışmalarına bakılacak olursa Konsey'in yukarıda bahsedilen OECD *"raporunu referans alarak belirlenen ihlallerin üye ülkeler nezninde cezai müeyyide altına alınmasını benimsemiş ve ayrıca bir takım prensiplere ve OECD'nin raporunda belirtilmeyen ihlallere de dikkat çekilmiştir... OECD'nin raporunda belirtilen eylemlere ek olarak bilgisayarla bağlantılı suçlarla ilgili korunma, engellenme, mağdurlar, usulü bir takım kurallar örneğin uluslararası araştırmalar, veri bankalarına el konulması ve bilgisayar suçlarının soruşturulması ve kovuşturulmasında uluslararası işbirliğine gidilmesi konuları bir taslak halinde sunulmuştur. Üye ülkelere kanunlaştırma çalışmalarında yol gösterici nitelikte olan bu taslak daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 13 Eylül 1989 tarihinde benimsenerek yürürlülüğe girmiştir.*

Avrupa Konseyi ikinci çalışmasını 1995 yılında gerçekleştirmiştir. Bu çalışmayla ceza usul yasalarının bilişim teknolojileri ile birleştirilmesiyle ilgili problemler masaya yatırılmış ve bunlara çözüm yolları aranmıştır. 11 Eylül 1995 yılında Bakanlar Komitesi tarafından kabul edilen metinde bilişim teknolojilerin getirdiği yeniliklere uygun olarak ceza usul yasalarındaki soruşturma ve el koymaya ait hükümlerin revize edilmesi, elektronik delil, şifreleme sistemlerinin kullanılması, uluslararası işbirliği başlıkları altında usul yasalarında yapılacak düzenlemeler için yol gösterici nitelikte kurallar gösterilmiştir."[22]

[22] Beceni, *a.g.e.,* IV. Bölüm s. 8'den naklen.

II. Ülkemizdeki Düzenlemeler

Bilişim suçları açısından ülkemizdeki, hukukumuzdaki ilk düzenleme 1.3.1926 tarih 765 sayılı eski[23] Türk Ceza Kanunu'na *"Bilişim Alanında Suçlar"* başlıklı 11. babın eklenmesi ile vücut bulmuştur. *"Bu bap, 6.6.1991 tarih ve 3756 sayılı Kanun'un 20. maddesiyle TCK'ya eklenmiştir ve 525a-525d nolu dört maddeyi içermektedir. 525a, 525b ve 525c maddeleri 1989 TCKT'dan aynen, suçlardan dolayı fer'i cezaları gösteren 525d maddesinin ise 1. bendindeki ceza alınmıştır. TCKT'deki hükümlerin tertibinde YFCK Ön Tasarısı'ndaki 321-1 - 323-7 maddelerinden esinlenilmiştir."*[24]

§. Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemle İlgili Olarak

a. Ele Geçirme (Programları, Verileri veya Diğer Bir Unsuru Hukuka Aykırı Olarak Ele Geçirme) Suçu (m. 525/a-1)

Kanuni Unsur: Söz konusu suçun gerçekleşebilmesi için ön koşul, ilgili fıkrada (525/a-1) belirilen ortamdan, yani *"bilgileri otomatik işleme tabi tutmuş sistem"*den (ki bundan sonra kısaca bilişim sistemi denilecektir) yine belirtilmiş bulunan unsurların *"program, veri veya diğer bir unsur"*, hukuka aykırı olarak elde edilmesi/ele geçirilmesidir. Ancak bu fıkrada (525/a-1) bahsedilen unsurlar bir bilişim sistemi vasıtasıyla ele geçirilmelidir; aksi takdirde öngörülen suç vücut bulmaz. Bununla birlikte söz konusu unsurlar fıkranın metninden de anlaşılacağı üzere bir bilişim sisteminin yazılım (software) türündeki unsurlarıdır; dolayısıyla bu norm donanım (hardware) türündeki unsurları himaye etmemektedir.[25]

Korunan Hukuki Yarar: Bu norm ile özel hayatın gizliliği, sırrın masuniyeti ve hatta iletişim özgürlüğü, ayrıca ilgili unsurlar üzerindeki mülkiyet hakkı himaye altına alınmaktadır.

---

[23] Açıklayıcı Not: Çalışmanın bu bölümünün tamamladığım sıralarda 26.09.2004 tarihinde TBMM'ce kabul edilip kanunlaştırılan 5237 sayılı Yeni Türk Ceza Kanunu henüz tasarı halindeydi; şu halde gerek çalışmanın bütünlüğü gerekse tarihsel ve içtihadı/yorumsal değeri açısından bu kesiminin olduğu gibi korunarak yayınlanmasını uygun gördüm.

[24] Dönmezer, *a.g.e.*, s. 613; Fransız Ceza Kanunu'ndaki düzenlemeler hakkında bilhassa bkz., Erem, Faruk, *TCK Şerhi, C. 3, Özel Hükümler,* Ankara 1993, s. 2254-2259.

[25] Bkz., *Bilişim Suçları,* s. 51, 52.

Fail: Öngörülen suç fail açısından herhangi bir özellik göstermemekte olup herkes tarafından işlenebilir.

Mağdur: Tıpkı failin durumunda olduğu gibi mağdurun durumu da bu suç biçimi bakımından özellik arz etmemektedir. Mağdurun fıkrada belirtilmiş bulunan unsur(lar) üzerinde hak sahibi olması yeterlidir.

Maddi Unsur: Ele geçirme fiilidir. Ele geçirme, failin fıkrada belirtilen unsuru/ unsurları kendi tasarrufu altına sokması, içeriklerine ulaşması şeklinde vücut bulur. Bu noktada ilgili unsurlara ulaşmak ve onları hakimiyeti altına almak suçun gerçekleşmesi için yeterli olup failin içeriği anlaması yahut içeriğe nüfuz edebilmesi gibisinden bir koşul mevcut değildir.[26]

Burada düzenlenen suç icrai nitelikte suç bir suç olup aynı zamanda şekli/neticesi harekete bitişik bir suçtur; dolayısıyla ani bir suçtur, zira hareket gerçekleştirildiği anda vücut bulur, ancak hareketin bir süreç biçiminde gerçekleşmesi halinde (ağ üzerinden veri aktarımı gibi) muhtemel mütemadi suç gündeme gelebilir. Hareket her türlü elverişli fiille gerçekleştirilebilir.[27]

Hukuka Aykırılık Unsuru: İlgili fıkranın metninde de belirtildiği üzere, bu suçun gerçekleşmesi için eylemin *"hukuka aykırı olarak"* gerçekleştirilmesi gerekmektedir. Dolayısıyla hukuka uygunluk nedenlerinin bulunması halinde bu çeşit bir eylem suç teşkil etmeyecektir. Yine aynı mayanda hak sahibi kişinin/kişilerin rızası da aynı etkiyi yaratmaktadır. Bu noktada failde, işlediği eylemin hukuka aykırı olduğu bilinci aranmaktadır. Ancak bu durum özel bir kast aranması anlamına gelmez; yalnızca failin doğru olmayan, hukuk düzenince cevaz verilmeyen bir şey yapmakta/yapmış olduğunun bilincini taşıması yeterlidir. Bu bağlamda hukuka aykırılık bilinci her somut olayda ayrıca gözetilecektir.

Manevi Unsur: Bu suç genel kast ile işlenir, özel kast aranmaz. Taksir hipotezinin uygulanması da mümkün değildir.

• Öngörülen suç teşebbüse müsaittir. Ancak neticesi harekete bitişik bir suç olduğundan ötürü tam teşebbüs hipotezi uygulanamaz, eksik teşebbüs mümkündür.[28]

---

[26] Bkz., *Bilişim Suçları,* s. 63.

[27] *Bilişim Suçları,* s. 63, 64 hareket adına örnek fiiller için bkz., s. 64, 65.

[28] Teşebbüs hakkındaki tartışmalar ve bu suçun içtima ve iştirak açısından gösterdiği özellikler için ayrıca bkz., *Bilişim Suçları,* s. 79-82.

b. Tasarruf (Bir Programı, Verileri Veya Diğer Herhangi Bir Unsuru Başkasına Zarar Vermek Üzere Kullanma, Nakletme, Çoğaltma) Suçu (m. 525/a-2)

Kanuni Unsur: Bu fıkrada da 525a'nın ilk fıkrasında olduğu gibi suçun gerçekleşebilmesi için ön koşul, normda belirtilmiş bulunulan eylemlerin bir bilişim sistemi üzerinde ve ilgili unsurlar hakkında gerçekleştirilmesidir; yani suçun gerçekleşme ortamı bir bilişim sistemi olmalıdır. 525a'nın birinci fıkrası hakkında yapılan açıklamalarda da belirtildiği üzere bu norm ile korumadan faydalanan unsurlar bilişim sisteminin soyut (yani yazılım türündeki) unsurlarıdır.

Korunan Hukuki Yarar: Yukarıda yapılan açıklamalar bu norm için de geçerli olup kişilerin mülkiyet ve özel hayatlarının gizliliği/sırrın masumiyeti hakları korunmaktadır. Ancak; belirtilmelidir ki bu norm açısından ziyadesiyle ekonomik çıkarlar özel bir himaye altına alınmaya çalışılmıştır. Zira fıkrada belirtilen (525/a-2) *"kullanmak", "nakletmek"* ve *"çoğaltmak"* eylemleri daha ziyade ekonomik menfaatleri tehdit eder görünmektedir; ayrıca *"çoğaltmak"* fiili fikri hakları da ihlal eder niteliktedir.

Fail: Öngörülen suç fail açısından herhangi bir özellik göstermemekte olup herkes tarafından işlenebilir.

Mağdur: Bu suçun mağduru en genel ifadeyle hakları zarara uğrama tehlikesi altında bulunan kimsedir. Kural olarak bu kimse bilişim sisteminin maliki olmakla birlikte suça sırasında kullanılan bilişim sisteminin maliki olmamasına rağmen sistemde yer alan içerik (program, veri yahut diğer unsurlar) üzerinde hak sahibi olan (örneğin fikri mülkiyet hakkı) kişiler de olabilir.

Maddi Unsur: Burada düzenlenen suç seçimlik hareketli bir suçtur; dolayısıyla suçun vücut bulması için ilgili fıkrada (525/a-2) belirtilen eylemlerden birinin gerçekleştirilmesi yeterlidir. *"Seçimlik hareketlerden hepsinin birden yapılması suçun birden fazla olduğuna işaret etmez. Ortada yine de tek suç vardır. Ancak bu ihtimalde hakim cezayı yukarı hadden tayin edebilir."*[29]

[29] *Bilişim Suçları,* s. 96'dan naklen.

İlgili fıkrada hüküm altına alınmış bulunan suçun işlenebilmesi için gereken eylemler şunlardır:

1. Kullanmak: Normda belirtilen unsurların çalıştırılması, söz konusu unsurlardan faydalanılması anlamındadır.

2. Nakletmek: Normda belirtilen unsurların herhangi bir yöntemle bir yerden (orijinal yerinden) başka bir yere taşınması, götürülmesi, gönderilmesi eylemidir.

3. Çoğaltmak: Yine normda belirtilmiş bulunan unsurların aslının yahut kopyasının çoğaltılması, tekrarlanan röprodüksiyonlarının yapılması eylemidir.

Aynı zamanda, bu normla düzenlenen suç, icrai nitelikte ve neticesi harekete bitişik bir suçtur.

Hukuka Aykırılık: Yukarıda 525/a-1 fıkrası için yapılan açıklamalar bu norm için de aynen geçerlidir.

Manevi Unsur: Bu suçun manevi unsuru kasttır. Fakat genel kastın yanında başkasına zarar verme iradesiyle şekillenen özel bir kastın da bulunması gerekmektedir. Taksirli şekli yoktur; bu suçta taksir hipotezi işletilemez.

• Öngörülen suç eylemi parçalanabildiği derecede eksik teşebbüs mümkün olup netice harekete bitişik bir suç olması nedeniyle tam teşebbüs mümkün değildir.

c. Tahrip ve Bozma (Başkasına Zarar Vermek veya Kendisine veya Başkasına Yarar Sağlamak Maksadıyla Bir Sistemi veya Verileri veya Diğer Herhangi Bir Unsuru Kısmen veya Tamamen Tahrip veya Değiştirmek veya Silmek veya Sistemin İşlemesine Engel Olmak veya Yanlış Biçimde İşlemesini Sağlamak) Suçu (m. 525/b-1):

Kanuni Unsur: Bu norm esas itibariyle bir bilişim sistemine yönelik zarar verici eylemleri karşılamaktadır; burada söz konusu edilen suça konu olan bilişim sisteminin fiziksel unsurlarının yanı sıra elektronik/elektromanyetik ortamı üzerinde gerçekleştirilen bir fiildir. Bununla beraber, bu çeşit eylemlerin cezalandırılabilmesi için ortada bir yarar sağlama ya da zarar verme amacı bulunmalıdır.

Korunan Hukuki Yarar: Bu norm ile himaye gören hukuki menfaat temel olarak bilişim sistemi yahut onun veri veya diğer unsurları üzerindeki ekonomik çıkarlar ve bunların üzerindeki ayni haklar ile en geniş anlamda mülkiyet hakkıdır.

Fail: Bu suç için bir özellik göstermez.

Mağdur: Himaye gören hukuki menfaatlere,yani bilişim sistemi, veriler yahut diğer ilgili unsurlar üzerinde haklara malik olan kişiler; en genel ifadeyle hakları zarara uğrama tehlikesi altında bulunan kimselerdir.

Maddi Unsur: Bu suç icrai, seçimlik hareketli ve şekli bir suçtur; suçun tamamlanması için ilgili fıkrada (525/b-1) belirtilen eylemlerden birinin gerçekleştirilmesi yeterlidir. Bu fıkrada bahis edilen suça vücut verici eylemler ise şunlardır:

Bir bilişim sistemini veya verileri yahut diğer bir ilgili unsuru:

1. Tahrip etmek: Tahrip eylemi yukarıda belirtilen varlıkların yok edilmesi ya da işlemez hale getirilmesi anlamındadır. Burada tahrip eyleminin yöneldiği nesne, bilişim sisteminin somut/fiziksel unsurları olabileceği gibi, aynı zamanda elektronik/elektromanyetik ortamı yahut onun soyut unsurları olmalıdır. Zira kanun koyucu, bu fıkra hükmü ile bilişim sistemine, sistem verilerine ve diğer unsurlarına yönelik ızrar fiillerini genel nas-ı ızrar hipotezi dışında ayrıca düzenleme ihtiyacı duymuştur.[30] Her ne kadar bilişim sisteminin somut/fiziksel unsurlarının tahribine yönelik bir eylemin nas-ı ızrar suçuna ilişkin hükümlerle (TCK m. 516) karşılanabilecek olması mümkünse de kanun koyucu bu noktada gündeme gelebilecek tereddütleri engellemek adına bu hükmü vazetmiş olsa gerektir.

2. Değiştirmek: Veriler yahut diğer unsurlar açısından söz konusudur. Hali hazırda mevcut olanların yerine başkalarını koymak eylemini ifade eder.

3. Silmek: Bu fiil de veriler yahut diğer unsurlar açısından söz konusu olacaktır. Kısaca kayıtların ortadan kaldırılması anlamındadır.

---

[30] Bkz., Savaş, Vural - Mollamahmutoğlu, Sadık, *Türk Ceza Kanunu'nun Yorumu,* IV. Cilt, Seçkin Yayınevi, Ankara 1999, s. 5863.

4. Sistemin İşlemesine Engel Olmak: Suça konu olan bilişim sisteminin işlevini yerine getirmesini engellemek yahut sistemi geçici veya daimi şekilde durdurmak anlamındadır.

5. Yanlış Biçimde İşlemesini Sağlamak: Bilişim sisteminin sağlıklı çalışarak olağan işlevlerini gereği gibi yerine getirmesini engelleyecek arızalar yaratmak, sistemin genel işleyişini bozmak suretiyle sistemin istenmeyen faaliyetler görmesine neden olmak eylemidir.

Hukuka Aykırılık: Bu hususta yukarıdaki açıklamalar geçerlidir. Genel hukuka uygunluk sebeplerinin yanı sıra, mağdurun rızası da - mağdurun zarara uğrayan şey üzerinde münhasıran tasarrufta bulunma yetkisi bulunduğu müddetçe- hukuka aykırılığı ortadan kaldırır.

Manevi Unsur: Genel kastın yanı sıra, suçun vücut bulması için *"başkasına zarar vermek"* yahut *"kendisine veya başkasına yarar sağlamak"* biçiminde bir amacın, yani özel kastın bulunması gereklidir. Bu sebepten ötürü yanlışlıkla/hataen bu çeşit bir duruma neden olunması halinde ilgili eylem(ler) suç teşkil etmeyecektir.

d. Yarar Sağlama (... Bir Sistemi Kullanarak Kendisi veya Başkası Lehine Hukuka Aykırı Yarar Sağlamak) Suçu (m. 525/b-2):

Kanuni Unsur: Bu norm ile mala/mülkiyete karşı işlenebilecek hırsızlık, dolandırıcılık, emniyeti suiistimal gibi bazı geleneksel suçların bir bilişim sistemi vasıtasıyla işlenmesi halinde doğabilecek tereddütlerin önlenmesi[31] ve cezai yaptırım öngörülebilmesi amacı güdülmüştür. Geleneksel normlarla yaşanabilecek bir ihtilaf halinde bir bilişim sisteminin araç olarak kullanılması biçiminde beliren ayırıcı ölçüt gözetilerek daha özel olan 525/b-2 normuna göre hükmolunmalıdır. Ayrıca vurgulamak gerekirse, 525/b-2 fıkrası için yasadaki gerekçe manidar ve fıkranın yorumu için aydınlatıcı niteliktedir: *"Sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlanmasını yani sistem vasıtası ile dolandırıcılığı cezalandırmaktadır."*[32]

İlgili fıkrada (525/b-2) yer alan *"yarar sağlamak"* tabiri geniş bir şekilde anlaşılmaya müsaittir; böylece sağlanabilecek her türlü maddi,

[31] Bkz., yukarıda sayfa 11.

[32] Aktaran, Öngören, Gürsel, *İnternet Hukuku,* IV. Bölüm A-1 http://www.hukukcu.com (03.04.2004) s. 3.

manevi fayda bu çerçevede değerlendirilebilir.[33] Fakat söz konusu *"yarar"*ın ekonomik bağlamda olması lazım gelmektedir.[34]

Korunan Hukuki Yarar: Bu norm ile himaye gören hukuki menfaat temel olarak mülkiyet hakkı olmakla beraber, aynı zamanda, uygulamada rastlanan örnekler göz önüne alındığı takdirde, kamunun bilişim sistemlerine yönelik itimadı ve ekonomik işlemlerde güvenilirlik hususlarının da dolaylı olarak himaye gördüğünden bahsedilebilir.

Fail: Herkes bu suçun faili olabilir; ayrıca bir özellik göstermemektedir.

Mağdur: Bir önceki fıkraya ilişkin açıklamalar burada da geçerlidir.

Maddi Unsur: İcrai bir hareketle işlenen bir suçtur. Normda bahsedilen *"kullanarak"* tabiri bir bilişim sistemini suç işlemek için araç olarak kullanmayı ifade eder. Böylece suça konu olan bilişim sistemini etkileyerek olağan dışı işlemler yaptırarak yahut sisteme yanlış veya eksik bilgiler girerek sistemin doğru işlemesini önlemek ve bu suretle sistemi hukuka aykırı biçimde menfaat edinmek amacıyla kullanmayı temin edecek/yönlendirecek eylemler, kısaca yetkisiz müdahale eylemi suçun maddi unsurunu oluşturmaktadır.

Hukuka Aykırılık: Failin ilgili bilişim sistemine bu çeşit bir müdahalede bulunma yetkisinin bulunmayışı hukuka aykırılık unsurunu teşkil etmektedir. Diğer hususlarda yukarıdaki açıklamalara bakılabilir.

Manevi Unsur: Bu suç da özel kast ile işlenmektedir; bu bağlamda failin, kendisine yahut bir başkasına hukuka aykırı bir şekilde yarar sağlamak amacını da taşıması gereklidir.

• Teşebbüse elverişlidir, cezalandırılabilmesi için eylemin tamamlanmış olması şartı aranmaz.

---

[33] Ersoy, *a.g.y.*, s. 178.
[34] Bkz., Dönmezer, *a.g.e.*, s. 618.

E. Delil Tahrifi (Hukuk Alanında Delil Olarak Kullanılmak Maksadıyla Sahte Bir Belgeyi Oluşturmak İçin Verileri veya Diğer Unsurları Yerleştiren veya Var Olan Verileri, Diğer Unsurları Tahrif Etmek) Suçu (Tahrif Edilmiş Verileri Bilerek Kullanmak Fiili Dahil) (m. 525/c):

Kanuni Unsur: Bu suçun gerçekleşmesi için ortada düzenlenmiş bir sahte belge olmasına lüzum yoktur. Zira bu norm aslında bir teşebbüs halini cezalandırmaktadır. Fail sahte belge düzenleyip kullanmak için bir bilişim sistemini araç olarak kullanmalı ve suça konu olan bilişim sistemine bu yolda veri yerleştirmelidir.

Korunan Hukuki Yarar: Bu norm ile sahtecilik suçunun koruduğu hukuki yararın aynısı himaye görmektedir; *"yani varakaların ve hukuki ilişkilerde sonuçları olan diğer vesikaların güvenlik ve güvenilirliği"*,[35] kamunun itimadı, diğer taraftan ise sosyal yaşamda itibar edilen belirli bazı unsurların/kanıtlayıcı vasıtaların sahihliği/doğruluğu bağlamında vücut bulan özel menfaatler koruma altına alınmaktadır.

Fail: Suç eylemini icra eden kişidir; ayrıca bir özellik göstermemektedir.

Mağdur: Buradaki mağdur söz konusu suç ile menfaatleri ihlal edilenlerdir; bu açıdan kamu ile birlikte suçtan zarar görülmesi halinde özel kişiler suçun mağdurudur.

Maddi Unsur: Maddenin gerekçesinde: *"suçun maddi unsuru, gerçeğe uygun olmayan bilgi veya diğer unsurları tahrif etmek veya tahrif edilmiş unsurları bilerek kullanmaktır."* diye ifade olunmaktadır. Böylece bir bilişim sistemi vasıtasıyla hem sahte belge oluşturma/düzenleme hem de bu belgeyi kullanma amacı doğrultusundaki eylemler öngörülen suça vücut verecektir. Bu bağlamda, maddi unsuru teşkil eden icra hareketi seçimlik nitelikte olup temel olarak iki şekilde ortaya çıkmaktadır:

1. Yerleştirmek: Verileri veya diğer unsurları bahsedilen amaç doğrultusunda bir bilişim sistemine yerleştirmek, yani hukuken delil olarak kullanılması amaçlanan sahte bir belgenin bir bilişim sistemi/bilgisayar yahut ağ ortamında imal edilmesi, yaratılması anlamındadır.[36] Buradaki

[35] Dönmezer, *a.g.e.,* s. 619'dan naklen.
[36] Bkz., Dönmezer, *a.g.e.,* s. 620.

anlamıyla söz konusu eylemin ziyadesiyle fikri sahtekarlık biçiminde gelişmeye uygun olduğu iddia edilebilir.

2. Tahrif Etmek: Bir bilişim sisteminde yer alan ve hukuken hükmü haiz olan belge niteliğindeki verilerin içeriğine müdahale etmek suretiyle verileri değiştirmek/dönüştürmek eylemidir. Burada da maddi sahtekarlık durumuna vücut verildiği söylenebilir.

Ayrıca; Yukarıda sayılan eylemlerin faili olmamakla birlikte söz konusu eylemler yoluyla oluşturulmuş hukuki hükmü haiz bir belge niteliğindeki unsuru bilerek kullanmak da suç sayılmıştır.[37]

Hukuka Aykırılık: Hukuka aykırılık hususunda yukarıda bahsedilen genel hükümler geçerlidir.

Manevi Unsur: Özel kast aranır; bu açıdan yukarıda bahsedilen eylemlerin *"hukuk alanında delil olarak kullanılmak maksadıyla"* işlenmiş olması gerekmektedir. Bu yönde bir amaç gütmeyen eylemler bu madde açısından suç teşkil etmeyecektir.

Son olarak kanunun 525d maddesinden söz etmek gerekecektir.

TCK madde 525d: Bu maddede ise 525a ve b maddeleri açısından fer'i ceza gösterilmiştir. Madde metni şöyledir: *"525a ve 525b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten … yasaklanma cezası da verilir."*

Böylece failin konumu/sıfatı ve/veya fail ile mağdur arasındaki ilişki de fer'i cezanın hükmedilmesinde belirleyici olacaktır.

III. 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu

Bu bölümde ise 26.09.2004 tarihinde Türkiye Büyük Millet Meclisi tarafından kanunlaştırılarak 12.10.2004 tarihinde 25611 sayılı *Resmi Gazete*'de yayınlanan 5237 sayılı yeni Türk Ceza Kanunu'nun bilişim suçlarına ilişkin hükümleri irdelenecektir.

[37] Bu hususta ayrıca bkz., Ersoy, *a.g.y.*, s.180, 181.

a. Genel Olarak Kanun'un İzlediği Sistem

Türkiye Büyük Millet Meclisi tarafından kabul edilen 5237 sayılı Yeni Ceza Kanunu'nun bilişim suçlarına yönelik hükümlerin düzenlemesinde 1.3.1926 tarih 765 sayılı eski Ceza Kanunu'muzun sisteminden kısmen farklı bir yöntem izlenmiştir. Zira kanun metni incelendiği takdirde farkına varılacağı üzere, *İkinci Kitap*'ının -Özel Hükümler- Üçüncü Kısım, Onuncu Bölüm'ünde bilişim sistemlerine karşı suçlar düzenlenmiş bulunmaktadır. Burada ilgili bölümün başlığından da anlaşılacağı üzere yalnızca bilişim sistemlerine karşı suçlar düzenlenmiş bulunmaktadır. Kanun'umuzda bilişim suçlarının sınıflandırılması/kategorizasyonu bağlamında, daha önce belirtmiş olduğum: (1) Bilişim sistemlerine karşı suçlar ve (2) Bilişim sistemleri aracılığıyla işlenen suçlar ayrımının benimsenmiş olduğu görülmektedir. Şu halde Yeni Türk Ceza Kanunu eski Kanun'umuzun sisteminden ayrılarak bilişim suçlarını düzenleme de karma sistemi benimsemiş olmaktadır. Fakat açıktır ki kanun koyucu bilişim suçlarını ayrı bir kanun ile düzenlemek yerine yine karma bir yolu/yöntemi tercih ederek hem ceza kanununa bilişim suçlarını düzenlemek amacıyla yeni hükümler eklemiş hem de klasik/geleneksel suç tiplerini düzenleyen normların ihlalini düzenlerken bu suçların işleniş biçimlerini çeşitlendirerek bilişim suçlarına vücut veren yeni fiiller/modaliteler eklemiştir.

Kanun'da dikkat çeken bir başka husus da eski düzenlemede yer alan *"bilgileri otomatik işleme tabi tutmuş sistem"* tabiri yerine doğrudan *"bilişim sistemi"* tabirinin kullanılmış olmasıdır. Kanaatimce bu yaklaşım oldukça yerinde olmuştur; zira terminoloji ve tanım sorunu ile ilgili bahiste de vurguladığım üzere, hukuk terminolojisindeki birliği sağlamak ve ilgili suç hipotezlerinin istikrar ve tutarlılık göstererek bu yeni gelişen alanın müesseseleşmesi adına, bilişim teriminin kullanılması ve yaygınlaştırılması/standartlaştırılması gerekmektedir.[38] Ayrıca yine yeni Kanun'umuz ile birlikte ilk kez bir bilişim sistemine izinsiz (daha doğrusu hukuka aykırı) olarak girme suç sayılmıştır; bu bağlamda yine yukarıdaki ilgili bahiste belirtmiş bulunduğum, Birleşmiş Milletler bünyesinde gerçekleştirilen *"Sınır Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi Sempozyumu"*nda 14 Aralık 2000 tarihinde düzenlenen panelde üye ülkelere cezai düzenleme altına alınması salık

[38] Yukarıda (I. Terminoloji ve Tanım Sorunu) hakkındaki bölüme bakınız.

verilen *"bilgisayar sistemlerine yetkisiz giriş"* eylemi de cezai yaptırıma konu edilmiştir.

b. Ceza Kanunu'nun İlgili Hükümlerinin Yorumu

Bu bölümde yeni TCK'nın ilgili hükümleri iki ayrı bahis altında incelenecektir; böylece bilişim sistemleri aracılığıyla işlenen hırsızlık ve dolandırıcılık suçları ile bilişim sistemlerine karşı suçlar iki ayrı bahsi oluşturacaktır.

1. Bilişim Sistemleri Aracılığıyla İşlenen Suçlar: Kanun metninin 142 ve 158. maddelerinde, sırasıyla *"nitelikli hırsızlık"* ve *"dolandırıcılık"* suçlarını hüküm altına alan normların ilgili bentlerinde söz konusu suçun bilişim sistemleri aracılığıyla işlenmesi eylemi suçu ağırlaştıran etken olarak suçun nitelikli hali sayılmıştır.

Ancak bununla birlikte bilişim sistemleri aracılığıyla işlenen suçlar elbette ki yalnızca bunlardan ibaret değildir. Özellikle içerik suçları açısından geniş bir yelpazeye sahip olan ve çoğunlukla bilişim sistem ağlarıyla işlenen bu suçlar arasında en çok rastlanılan hakaret ve sövme, müstehcen yayınlar, çocuk pornografisi, suç işlemeye tahrik gibi suçlarla birlikte, basın ve ceza kanununda -ve hatta fikri ve sinai mülkiyet haklarını himaye eden kanunlarda bulunan cezai hükümler bağlamında- yer alan bazı geleneksel tipteki suçların bilişim sistemleri ve ağ aracılığıyla işlenen biçimleri yer almaktadır.

2. Bilişim Sistemlerine Karşı Suçlar: Kanun'un *İkinci Kitap*'ının -Özel Hükümler- Üçüncü Kısım, Onuncu Bölüm'ünde (243-246. maddeleri) *"Bilişim Sistemlerine Karşı Suçlar"* düzenlenmiş bulunmaktadır.

• **Bazı Temel Terim ve Tanımlar:** Kanun'da yer alan 243. maddenin gerekçesinde bilişim sistemi tanımlanmış bulunmaktadır. Buna göre; *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir."*

Yine Ceza Kanunu'nun 243. maddesinin III. fıkrasının gerekçesinde veri terimi de tanımlanmış bulunmaktadır. Buna göre:

"Sistem içindeki bütün soyut unsurlar, fıkrada geçen 'veri' teriminin kapsamındadır."

"Bilişim sistemine girme;

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir."

• Yukarıda da belirttiğim üzere bu norm ile ilk kez bir bilişim sistemine hukuka aykırı olarak girme(k)[39] suç haline getirilmiştir. Burada fail, yalnızca sisteme girmeyi kastetmiş yahut orada kalmaya devam etmeyi istemiş olmalıdır. Sisteme haksız olarak girilmesi suçun oluşması için yeterlidir. İlgili fıkranın metninde de belirtildiği üzere, bu suçun gerçekleşmesi için eylemin *"hukuka aykırı olarak"* gerçekleştirilmesi gerekmektedir. Dolayısıyla hukuka uygunluk nedenlerinin bulunması halinde bu çeşit bir eylem suç teşkil etmeyecektir. Yine aynı mayanda hak sahibi kişinin/kişilerin rızası da aynı etkiyi yaratmaktadır. Bu noktada failde, işlediği eylemin hukuka aykırı olduğu bilinci aranmaktadır. Ancak bu durum özel bir kast aranması anlamına gelmez; yalnızca failin doğru olmayan, hukuk düzenince cevaz verilmeyen bir şey yapmakta/yapmış olduğunun bilincini taşıması yeterlidir. Bu bağlamda hukuka aykırılık bilinci her somut olayda ayrıca gözetilecektir.

Bu suçun oluşması için ayrıca özel kast aranmaz; genel kast yeterlidir.

---

[39] *Avrupa Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu*'nda yer alan "izinsiz erişim" maddesine ilişkin açıklamalar burada incelenmekte olan yeni Türk Ceza Kanunu'nun ilgili hükmünde yer alan "bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme" biçiminde kurgulanan suç teşkil edici eylemin yorumunda yol gösterici olacaktır. "'Yasadışı erişim' terimi bilgisayar sistem ve verilerinin güvenliğine (yani gizlilik, bütünlük, kullanıma açıklık) yönelik tehlikeli tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Koruma ihtiyacı, kuruluş ve kişilerin sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme ihtiyaçlarını yansıtmaktadır. Sadece izinsiz girme yani 'hacking', 'cracking' ya da 'computer trespass' ilke olarak başlı başına yasadışı olmalıdır. Bu durum, sistemlerin ve verilerin meşru kullanıcılarının engellenmesine ve düzeltilmesi yüksek maliyet getiren değişiklik ve tahribata yol açabilir. Bu tür izinsiz girmeler gizli verilere (şifreler, hedeflenen sistemle ilgili bilgiler dahil olmak üzere) ve sırlara erişilmesine, sistemin ücretsiz kullanılmasına yol açabilir, hatta hacker'ları bilgisayarla ilişkili sahtecilik ve sahtekarlık gibi daha tehlikeli bilgisayarla ilişkili suç türlerine teşvik edebilir." *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu*, *Avrupa Suç Sorunları Komitesi (CDPC) Nihai Faaliyet Raporu* 29.06.2001, Hazırlayan: Siber Suç Uzmanları Komitesi (PC-CY), Strasbourg, 2. madde şerhi paragraf 1.

Özel olarak verileri yok etme amacı güdülmesi ise bu suça değil 244/I'de hüküm altına alınmış olan suça vücut verecektir. Zira maddenin bu fıkrasının gerekçesinde: "*Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.*" denilmektedir.

Önemli olan bir başka husus ise, sistemin bir kısmına hukuka aykırı olarak girilmesinin de suça vücut vereceğidir. Fakat sistemin bir kısmı tabirinden neyin anlaşılması gerektiğini kanun koyucu kanunun ilgili gerekçesinde maalesef açıklamamıştır. Bu bağlamda uygulamada sorunlar çıkması kaçınılmaz görünmekle beraber *"kanunilik"* ilkesinin de tanımsızlıktan ötürü zedelenebilmesi muhtemeldir. Bu hususun yorumunda da yine Avrupa Siber Suçlar Sözleşmesi Şerhi yardımcı olabilir. Bu bağlamda bilişim sisteminin bir kısmına girilmesi tabirinden bilişim sisteminin, "*donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler*"[40] gibi unsurlarından bir yahut birkaçına girilmesi anlaşılabilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

• Kanun'un ilgili maddesinin bu fıkraya ilişkin gerekçesinde şöyle denilmektedir: "*İkinci fıkraya göre, birinci fıkrada tanımlanan füllerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir.*" Fakat burada, kanun koyucu, *"bedeli karşılığı yararlanılabilen sistemler"* hakkında başkaca açıklama yapmadığı gibi bu tür sistemler hakkında söz konusu suçun işlenmesinin hangi neden(ler)den ötürü daha az cezayı gerektirdiğini açıklamaya da lüzum görmemiştir. Sanırım ki burada özel bir tahfif nedeni oluşturulması, ilgili normların korudukları hukuki yararın ve suçun (muhtemel ve mümkün) mağdurlarının farklı olduğunun düşünülmesinden/farklı tasarlanmasından kaynaklanmaktadır.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, iki yıldan dört yıla kadar hapis cezasına hükmolunur.

---

[40] *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu,* 2. madde şerhi paragraf 3.

• Kanun'un 243. maddesinin üçüncü fıkrasında ise, ilgili maddenin ilk fıkrasında yer alan *"suçun neticesi sebebiyle ağırlaşmış hali düzenlenmiştir."* (ilgili madde gerekçesi) Zira: *"Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi halinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir."* (ilgili madde gerekçesi) -Suçun maddi unsurunu teşkil eden eylem açısından verilerin yok olması ve değişmesi tabirlerinden neyin anlaşılması gerektiği aşağıda anlatılacaktır.-

Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Madde 244: (1) Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

• Normun bu fıkrasını iki ayrı kesime ayırarak incelemek daha isabetli olacaktır. Zira bu fıkrada, suç konusunu teşkil eden bilişim sisteminin, hem somut/maddi unsurları (hardware) hem de soyut unsurları (yani veriler ve yazılımlar-software), kısacası bilişim sisteminin fizik varlığı ve sistemin işlemesini sağlayan tüm diğer unsurları aynı hüküm vasıtasıyla himaye altına alınmıştır.

Bu sebepten ötürü bahis konusu normu önce öncelikle bilişim sisteminin işleyişini engelleme ve bozma bağlamında sistemin fizik varlığına yönelen suç teşkil edici eylemler yönünden; sonra da sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme, yok etme bağlamında sistemin soyut unsurlarına, verilerine yönelen suç teşkil edici eylemler açısından ele almak daha sistematik bir yaklaşım teşkil edecektir kanaatindeyim. Yasa koyucunun da normu biçimlendirirken bu yaklaşımı benimsemesi, kanımca daha iyi olurdu.

a. Bilişim Sisteminin İşleyişini Engelleme ve Bozma: Bu normda, bilişim sistemine ilişkin mülkiyet hakkı korunmuştur. Bu bağlamda, gerekçede belirtildiği üzere bilişim sistemlerine yönelik ızrar fiilleri, genel

nas-ı ızrar hipotezi dışında ayrıca düzenlenerek özel bir suç sayılmıştır. Dolayısıyla *"aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."* Suçun maddi unsuru seçimlik hareketlidir, bundan ötürü suçun oluşması için fıkrada belirtilen eylemlerden herhangi birinin gerçekleştirilmesi yeterlidir. Söz konusu eylem formları ise iki tanedir: Bilişim sistemleriyle ilgili olarak;

• **İşleyişinin Engellenmesi:** Engelleme eylemi, bilişim sisteminin olağan işleyişini durdurmak, fonksiyonların doğru biçimde işlemesini engellemek (sistemin çalışma düzenini aksatmak) yahut benzeri sonuç doğurabilecek nitelikte bir eylemde bulunmak anlamındadır.[41] *"Cezai yaptırıma yol açması için engellemenin ayrıca 'ciddi ölçüde' olması gerekir."*[42]

• **Sistemin Bozulması:** Bozma eylemi ise sistemin çalışma düzenini aksatmak, işlemesini engellemekten öte, ayrıca bir sonucu doğuracak nitelikteki, yani sistemin artık işlemesinin olanaksız olduğu, hiçbir fonksiyonunu yerine getiremediği kronik bir çalışmama, bozulma durumunu yaratacak bir fiile tekabül eder.

b. Sisteme Hukuka Aykırı Olarak Veri Yerleştirme, Var Olan Verileri Başka Bir Yere Gönderme, Erişilmez Kılma, Değiştirme, Yok Etme: Bu normda ise bilişim sisteminin soyut/maddi olmayan (veri, program vb. gibi) unsurlarına dönük ızrar fiili ile birlikte özel hayatın gizliliği, sırrın masuniyeti ve hatta iletişim özgürlüğüne hukuka aykırı müdahaleler suç haline getirilmiş bulunmaktadır. Burada da seçimlik hareketli bir suç hipotezi öngörülmüş bulunmaktadır.

• **Veri Yerleştirme:** Bilişim sisteminin orijinalinde mevcut olmayan verilerin sisteme dahil edilmesi anlamındadır.

• **Var Olan Verileri Başka Yere Gönderme:** Hali hazırda sistemde yer alan orijinal verilerin herhangi bir surette (orijinal yerinden, konumundan) başka bir yere taşınması, götürülmesi, gönderilmesi eylemidir.

---

[41] Bkz., aynı doğrultuda, *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu, Avrupa Suç Sorunları Komitesi (CDPC) Nihai Faaliyet Raporu* 29.06.2001, Hazırlayan: Siber Suç Uzmanları Komitesi (PC-CY), Strasbourg, 5. madde şerhi paragraf 2.

[42] *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu*, 5. madde şerhi paragraf 3.

• **Erişilmez Kılma:** *"Bilgisayar verilerinin erişilmez kılınması, verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişi için verilerin ulaşılabilirliğini önleyen ya da sona erdiren herhangi bir fiil anlamındadır."*[43]

• **Değiştirme:** *"'Değiştirme' terimi mevcut verilerin farklı bir hale getirilmesi anlamındadır. Virüs ve Truva Atı gibi kötü amaçlı kodların sisteme sokulması da, bu nedenle, verilerin sonuçta farklı bir hale gelmesi gibi, bu paragrafın kapsamındadır."*[44] Kısaca orijinal verilerin yerine başkalarını koymak eylemini ifade eder.

• **Yok Etme:** Sistemde yer alan verilerin işlemez hale getirilmesi halidir. Burada tahrip eyleminin yöneldiği nesne bilişim sisteminin elektronik/elektromanyetik ortamı yahut onun soyut unsurları olmalıdır. *"... örtüşen fiiller olarak 'tahrip etmek' ve 'bozmak', özellikle veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz biçimde değiştirilmesiyle ilişkilidir. Verilerin 'silinmesi', fiziksel bir cismin imhasına eşdeğerdir. Veriler imha edilir ve tanınmaz hale getirilir."*[45]

(2) 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.

• 244. maddenin bu fıkrasında ise ilk fıkrada belirtilmiş bulunulan eylemlere ilişkin ağırlaştırıcı neden düzenlenmiştir. Bu ağırlaştırıcı neden ise ilk fıkrada belirtilen eylemlerin *"banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde"* uygulanacaktır. Bu fıkrada yer alan banka, kredi kurumu ve kamu kurum yahut kuruluşu ifadelerinden neyin anlaşılması gerektiği genel hükümlere göre yorumlanır.

(3) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.

---

[43] Bkz., *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu*, 4. madde şerhi paragraf 2.

[44] *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu*, *a.g.y.*

[45] *Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu, a.g.y.*

• Bu fıkra ile 244. maddenin ilk fıkrasında belirtilmiş bulunan eylemlerin, Ceza Kanunu'nun çeşitli maddelerinde yer alan bazı geleneksel suç biçimleriyle karşılanamayacak olması halinde boşluk yaratmamak adına veyahut söz konusu eylemler hakkında geleneksel hükümlerin tipiklik/modalite unsuru açısından uygulanmasında tereddüde mahal verilmemesi amacıyla ayrıca bir düzenlenme yapılarak bağımsız bir norm teşkili sağlanmaya çalışılmıştır. Böylece: "*... bir ve ikinci fıkralarda tanımlanan füllerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fülin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fülin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.*" (ilgili madde gerekçesi) İlgili madde gerekçesinden anlaşıldığı üzere bu fıkrada düzenleme altına alınan genel nitelikte bir hükümdür; bu yüzden daha özel nitelikteki bir normun saptadığı suç hipotezine uygunluk gösteren bir eylem gündeme geldiği takdirde bu norm değil, özel hüküm uygulanacaktır.

Bu normda bahsedilen *"haksız çıkar"*ın kimin adına yahut kimin için, kimin lehine olduğu önemli değildir. Sözü edilen *"çıkar"* geniş manada anlaşılmalıdır; bu açıdan her türlü maddi ve manevi fayda bu çerçevede değerlendirilebilir.

Banka veya Kredi Kartlarının Kötüye Kullanılması

Madde 245:

• Uygulamada pek sık rastlanan bir suç olan banka ve kredi kartı dolandırıcılığı ve sahteciliğinin, geleneksel hükümler vasıtasıyla tecziyesinin tereddütler doğurmasını önlemek, kısaca bu kartların kötüye kullanılması engellemek amacıyla bu özel hüküm düzenlenmiş bulunmaktadır. Maddenin gerekçesinde, bu hususa yönelik olarak şu ifade mevcuttur: "*Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının Ratio Legis'lerinin tümünü de içeren bu füllerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirilmeleri uygun görülmüştür.*"

• 245. maddenin gerekçesinde banka ve kredi kartı tabirlerinin tanımları ayrıca verilmiş bulunmaktadır:

"Banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımı olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır.

Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır." (ilgili madde gerekçesi).

Korunan Hukuki Yarar: Gerekçede belirtildiği üzere bu madde ile korunan hukuki yarar, bankaların ve kart/kredi sahiplerinin ekonomik menfaatleridir. Zira: *"Madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır."* (ilgili madde gerekçesi).

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.

Suçun Kanuni Unsuru: Suçun gerçekleşebilmesi için ön koşul, başkasına ait -yukarıda tanımı verilen- bir banka yahut kredi kartını herhangi bir şekilde ele geçirmek veya elde bulundurmaktır.

Hukuka Aykırılık: Genel hukuka uygunluk sebepleri hipotezinin dışında ilgili kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızasının olmaması/yokluğudur.

Maddi Unsur: Maddenin gerekçesinde suça vücut veren eylemler şöyle belirtilmiştir: *"Maddeye göre, aşağıdaki şekillerde gerçekleştirilen hareketler bu suçu oluşturmaktadır:*

1. Başkasına ait bir banka veya kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası bulunmaksızın kullanılması veya kullandırttırılması ve bu suretle failin kendisine veya başkasına haksız yarar sağlaması.

2. Aynı fiilin, aynı koşullarla sahibine verilmesi gereken bir banka veya kredi kartının bunu elinde bulunduran kimse tarafından kullanılması veya kullandırttırılması; söz gelimi kartı sahibine vermekle görevli banka memurunun

kartı kendi veya başkası yararına kullanması." (ilgili madde gerekçesi).

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

• Bu norm ile de banka ve kredi kartı sahteciliği, sahtekarlığı düzenleme altına alınmış bulunmaktadır. Maddenin gerekçesine göre: *"... birinci fıkrada belirtilen fiillerin, oluşturulmuş sahte bir banka veya kredi kartını kullanmak suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektirmektedir. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir."* (ilgili madde gerekçesi).

Maddenin bu fıkrasında sözü edilen banka veya kredi kartının sahteliğini iki ayrı hipotez üzerinden incelemek gerekmektedir:

• **Sahte Oluşturulan:** Bu tabir ile maddenin gerekçesinde tanımları verilmiş bulunan banka ve kredi kartlarının sahte olarak düzenlenmesi, bahis edilen banka yahut kredi kartının gerçek olmaması hali kastedilmektedir. Böylece burada yaptırımla düzenleme altına alınan sahtelik biçimi evrakta sahtekarlık suçunun fikri sahtekarlık hipotezine uygunluk göstermekte ve onun bu bağlamdaki muadili olarak gündeme gelmektedir.

• **Üzerinde Sahtecilik Yapılan:** Bu tabir ile de hali hazırda mevcut ve geçerli olan bir banka veya kredi kartı üzerinde aldatma kastıyla oynamalar/değişiklikler yapılması suretiyle gayri sahih hale getirilerek sahtekarlık yapılması eylemleri yaptırım altına alınmıştır. Buradaki sahtekarlık fiili ise evrakta maddi sahtekarlık hipotezine uygunluk göstermektedir; şu halde sözü edilen sahtelik durumu sahih olmama halini imler.

Suçun oluşması için yukarıda belirtildiği şekilde sahte olan banka veya kredi kartının çıkar amaçlı olarak kullanılması gerekmektedir. Dolayısıyla manevi unsur açısından özel kast güdülmesi, suçun gerçekleşmesi için elzemdir. Bununla beraber, normda belirtilen *"yarar"* unsurunun kimin adına yahut kimin için, kimin lehine sağlandığı önemli değildir.

Son olarak gerekçede de belirtildiği gibi, suça vücut veren eylem(-ler)in daha ağır bir cezayı gerektiren başka bir suçu teşkil eder nitelikte olmaması gereklidir.

Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması

Madde 246: (1) Bu Bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

• Yeni Ceza Kanunu'yla birlikte ceza hukukumuza bir ilk girmiş ve ilk kez tüzel kişilere yönelik bir yaptırım formu ihdas edilmiştir. Bu ise "*tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine*" hükmolunabilmesidir. (Sözü edilen güvenlik tedbirlerinin neler olabileceğini ise yine yeni Ceza Kanunu'nun *Birinci Kitap*'ının Üçüncü Kesim İkinci Bölümü'nde düzenlenmiş bulunan güvenlik tedbirlerine ilişkin hükümlere ayrılmış olan bölümün "*Tüzel Kişiler Hakkında Güvenlik Tedbirleri*" başlıklı 60. maddesidir.)[46] Böylece Avrupa Siber Suçlar Sözleşmesi'nde

[46] Konuyla olan doğrudan ilgisi dolayısıyla yeni Türk Ceza Kanunu'nun ilgili 60. maddesini, madde metni ve gerekçesiyle buraya almaktayım:

"Tüzel kişiler hakkında güvenlik tedbirleri;

Madde 60: (1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir.

(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.

(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir.

(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır.

GEREKÇE:

Anayasamızda da güvence altına alınan ceza sorumluluğunun şahsiliği kuralının gereği olarak sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir. Ancak bu ilke, işlenen suç dolayısıyla özel hukuk tüzel kişileri hakkında güvenlik tedbiri niteliğinde yaptırımlara hükmedilmesine engel değildir.

Bu nedenle maddede, özel hukuk tüzel kişileri hakkında hükmedilebilecek güvenlik tedbirlerinin tür ve koşulları düzenlenmiştir.

Maddede öngörülen ilk güvenlik tedbiri, faaliyet izninin iptalidir. Bunun için ilk koşul özel hukuk tüzel kişisine, belirli bir faaliyette bulunabilmesine ilişkin bir kamu kurumunca verilen bir iznin varlığıdır. İkinci koşul ise, bu iznin sağladığı yetkinin kötüye kullanılması suretiyle tüzel kişi yararına kasıtlı bir suç işlenilmesidir. Dikkat edilmelidir ki, burada söz konusu olan suç, tüzel kişi yararına işlenmiş herhangi bir suç değildir. İşlenen suçla, verilen iznin kullanılması arasında nedensellik bağı

öngörülen kurumsal yükümlülükler ihdası önerisine somut bir düzenleme ile hayatiyet kazandırılmıştır. Burada kanun koyucunun hukuk tekniği açısından basiretsiz bir yaklaşımına tanık olmaktayız. Çünkü söz konusu hükmün lafzından çıkan anlamla yorum yapıldığı takdirde bahsedilen güvenlik tedbirlerinin uygulanabilmesi için suç teşkil eden eylemlerin ilgili tüzel kişiye haksız menfaat sağlaması yeterli olacaktır. Bu noktada ilgili suç eylemiyle tüzel kişi arasında uygun bir illiyet bağının kurulması için bu ölçüt yeterli değildir. Avrupa Siber Suçlar Sözleşmesi'nin şerhinde de belirtildiği biçimiyle bu babda bir cezai yükümlük doğması için sağlanması gereken şartlar arasında, suçun, tüzel kişinin yetkili bir yöneticisi yahut çalışanı, vekili tarafından yetkilerinin kullanılması sırasında işlenmesi şartlarının da haksız menfaat şartına eklenmesi hem hukuk tekniği hem uygulamada tutarlılık ve içtihat birliği hem de kanunilik ilkesi ve kusur sorumluluğu ilkesi adına daha isabetli olurdu.

olmalıdır. Ayrıca, özel hukuk tüzel kişisinin organ veya temsilcilerinin bu suçun işlenmesine iştirak etmeleri gerekir.

Örneğin uyuşturucu veya uyarıcı madde ticaretinden elde edilen gelirlere meşruiyet görüntüsü kazandırmak için bir döviz bürosunun kullanılması halinde, bu döviz bürosunu işleten özel hukuk tüzel kişisinin, döviz bürosu işletmek için aldığı izin iptal edilecektir. Yine, ilaç üretmek için izin alınmış olan bir laboratuarda uyuşturucu veya uyarıcı madde üretimi yapılması durumunda da, aynı sonuç doğacaktır.

Özel hukuk tüzel kişileri bakımından öngörülen ikinci güvenlik tedbiri ise müsaderedir. Buna göre, tüzel kişi yararına işlendiği belirlenen suç bakımından, müsadere hükümlerindeki koşullar da gerçekleşmiş ise, o suçla bağlantılı olan eşya ve maddi çıkarların müsaderesine hükmedilecektir. Bu halde iyi niyetli üçüncü kişilerin hakları korunacaktır.

Özel hukuk tüzel kişileri ile ilgili güvenlik tedbirlerinin uygulanmasında, işlenen suç dikkate alındığında, çok ağır sonuçlar doğabilir. Örneğin çok sayıda kişi işsiz kalabilir veya iyi niyetli üçüncü kişiler bakımından telafisi güç kayıplar meydana gelebilir. İşte bu gibi hallerde mahkeme maddedeki orantılılık ilkesine dayanarak bu güvenlik tedbirlerine hükmetmeyebilecektir.

Özel hukuk tüzel kişileri hakkında uygulanacak güvenlik tedbirlerine, her suç bakımından değil, kanunda özel olarak belirtilen hallerde hükmedilebilecektir."

ABONET REKLAMI -1-