

5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları ve 5377 Sayılı Yasa İle Yapılan Değişiklikler

Murat Volkan Dülger[□]

I. Bilişim Suçu Kavramı ve Genel Olarak TCK

A. Bilişim Suçu Kavramı ve Tanım

TCK'da yer alan bilişim suçu tiplerinin açıklamasına geçmeden önce bu konuda yer alan kavramların belirtilmesi ve bilişim suçu kavramının tanımlanması konun daha iyi anlaşılabilmesi için yararlı olacaktır.

1. Kavram

Bilişim suçları ilk olarak, bilgisayarın da geliştirildiği Amerika Birleşik Devletleri'nde ortaya çıktığı için bu yeni suç tipinin adlandırılması da bu ülke hukukçuları tarafından yapılmıştır. Amerikan öğretisi ve uygulamasında bu suç tiplerine genel olarak “computer crime” denilmektedir¹.

Bu suç tiplerini adlandırmak üzere Alman Hukuku'nda “computermisbrauch”, İtalyan Hukuku'nda “la criminalità informatica”, Fransız Hukuku'nda ise “Des atteintes aux systèmes de traite automatisé de données” kavramları kabul edilmiştir.

Ülkemizde ise bu konuda “siber suç, sanal suç, internet suçu, bilgisayar suçu, bilişim suç hukuku, bilgisayar ile ilgili suç, bilişim sistemi aracılığıyla işlenen suç, bilişim alanında işlenen suç” gibi bir çok kavram kullanılmıştır.

Bu suç tiplerini karşılamak için hem genel nitelikte ve kapsayıcı oluşu, hem diğer kavramlara getirilen eleştirileri dışlaması² hem de öğretilde özellikle bu kavram üzerinde uzlaşmaya varılması nedeniyle “bilişim suçu” kavramının kullanılmasının yerinde olduğu belirtilmelidir.

[□] Avukat; İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilimdalı doktora öğrencisi.

¹ Murat Volkan Dülger, Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2004, s.63.

² Bu eleştiriler için bkz: Dülger, Bilişim Suçları, s.65,66.

2. Tanım

Bilişim suçlarının tanımı, ne ulusal hukuk düzenlemelerinde ne de uluslararası hukuk düzenlemelerinde yer almamaktadır. Bu düzenlemelerde her hangi bir tanım yapılmaksızın bilişim suçu olarak nitelendirilen eylemlere suç tipi olarak yer verilmesi tercih edilmiştir³.

Öğretide ise bilişim suçu kavramının pek çok tanımı yapılmış ancak bir tanım üzerinde uzlaşmaya varılamamıştır. Bilişim suçlarının tanımlanabilmesi için altı ölçütün bulunduğu ve bunları içeren bir tanımın geçerli ve yeterli bir tanım olduğu belirtilmiş ancak bu ölçütlerden yola çıkılarak yapılan tanımdan da uzlaştırıcı ve yeterli bir sonuca ulaşılamamıştır. Bunun üzerine bir tanım yapılmasından çok bu kavram altında hangi suç tiplerinin düzenlenmiş olduğu önem kazanmıştır⁴.

Bilişim suçlarına ilişkin genel ve kapsayıcı bir tanım yapılmasının zorluğuna ve bu konudaki çekincelere rağmen bilişim suçu, “verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar” şeklinde tanımlanabilir⁵.

B. 765 sayılı TCK ile 5237 sayılı TCK’da Düzenlenen Bilişim Suçlarının Karşılaştırılması

Bilişim suçları, 5237 sayılı TCK’da şu numara ve başlıklar altında yer almaktadır:

“Kişilere karşı suçlar” kısmının dokuzuncu bölümünde “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında m. 132 “haberleşmenin gizliliğini ihlal suçu”, m. 135 “kişisel verilerin kaydedilmesi suçu”, m. 136 “kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu”, m.138 “verileri yok etmeme suçu”.

“Topluma karşı suçlar” kısmının onuncu bölümünde “bilişim alanında suçlar” başlığı altında m.243 “hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu”, m.244/1-2 “bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu”, m.244/4 “bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu”, m.245 “banka veya kredi kartlarının kötüye kullanılması suçu”.

Bunların yanı sıra YTCK’da yalnızca bilişim suçu olarak nitelendirilemeyecek, diğer işleniş biçimlerinin yanı sıra bilişim sistemleri aracılığıyla da işlenmesi mümkün olabilecek suç tipleri bulunmaktadır⁶. Bunlara örnek olarak aşağıdaki suç tipleri gösterilebilir:

“Kişilere karşı suçlar” kısmının dokuzuncu bölümünde “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında m.132 “haberleşmenin gizliliğini ihlal suçu”, “kişilere karşı suçlar” kısmının yedinci bölümü olan “hürriyete karşı suçlar” bölümünde m.124 “haberleşmenin engellenmesi suçu”; sekizinci bölüm olan “şerefe karşı suçlar” bölümünde m.125 “hakaret suçu”; malvarlığına karşı suçlar bölümünde m.142 fkr.2 b. ‘e’ “nitelikli hırsızlık suçu”, m.158 fkr.1 b. ‘f’ “nitelikli dolandırıcılık suçu” ile “topluma karşı suçlar” kısmının yedinci bölümü olan “genel ahlaka karşı suçlar” bölümünde m.226 “müstehcenlik suçu”, m.228 “kumar oynanması için yer ve imkân sağlanması suçu”.

³ Carlo Sarzana di S. Ippolito, “Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalya’daki Durum” Çev: Vesile Sonay Daragenli, İÜHFM Prof. Dr. Türkan Rado’ya Armağan Sayısı, İstanbul, C:LV, S:3, 1997, s.393.

⁴ Öğretide yapılan bu tanımlar ve tanım için kullanılan ölçütler hakkında ayrıntılı bilgi için bkz: Dülger, Bilişim Suçları, s.66,67.

⁵ Dülger, Bilişim Suçları, s.67.

⁶ Dülger, Bilişim Suçları, s.211.

765 sayılı TCK ile 5237 sayılı TCK'nın bilişim suçları yönünden maddeler arası karşılaştırması ise şöyledir:

TCK m.525 a/1 TCK tasarısı m.135, m.136

TCK m.525 b/1 TCK tasarısı m.244/1-2

TCK m.525 b/2 TCK tasarısı m.244/4, 245, 158 fkr.1 b. 'f', m.142 fkr.2 b. 'e'⁷.

5237 sayılı TCK ile bilişim suçları açısından yapılan düzenlemede, bilişim suçları açısından 765 sayılı TCK için en yoğun eleştirilerin yapıldığı sistematik değiştirilmiş; bilişim suçları, suçla korunan hukuksal değer gözetilerek düzenlenmiş, suç tipleri arasında bunların korudukları hukuksal değerlerin niteliğine göre ayırım yapılmıştır⁸.

Bu karşılaştırma sonucu ortaya çıkan tabloya göre, 5237 sayılı TCK'nın 243. maddesinde bulunan "hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu" ile ilgili düzenleme 765 sayılı TCK'da hiç yer almamasına karşın, 5237 sayılı TCK ile yeni bir suç tipi olarak öngörülmüştür⁹. Böylelikle önemli bir yenilik olarak verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine girilmesi ve orada kalınması suç tipi olarak düzenlenmiştir¹⁰. Aynı şekilde 5237 sayılı TCK'nın 138. maddesinde yer alan "verileri yok etmeme suçu" da ilk kez bu yeni yasa ile suç tipi olarak düzenlenmiştir.

Bazı suç tipleri ise 765 sayılı TCK'da seçimlik hareketli suç tiplerinin, tanımında bulunan hareketlerden birisiyken, 5237 sayılı TCK ile bağımsız olarak yeni bir suç tipi olarak düzenlenmişlerdir. Buna göre 5237 sayılı TCK'nın 135. maddesinde düzenlenen "kişisel verilerin kaydedilmesi suçu", 136. maddesinde düzenlenen "kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu", 245. maddesinde düzenlenen "banka veya kredi kartlarının kötüye kullanılması suçu", 142. madde fkr.2 b. 'e'de düzenlenen "nitelikli hırsızlık suçu", 158. madde fkr.1 b. 'f'de düzenlenen "nitelikli dolandırıcılık suçu" 765 sayılı TCK'dan farklı olarak bağımsız suç tipleri şeklinde düzenlenmişlerdir.

765 sayılı TCK'nın 525 a/2 maddesinde düzenlenen suç tipine ise; öğretideki özellikle FSEK'de 4110 sayılı yasayla yapılan değişiklikler karşısında bu suç tipinin gereksiz olduğu ve uygulamasının hiç bulunmadığı yönündeki eleştiriler dikkate alınarak 5237 sayılı TCK'da yer verilmemiştir¹¹.

Bilişim suçlarının düzenlenişi açısından 5237 sayılı TCK ile getirilen ve yerinde olan bir başka değişiklik de, öğretide eleştiri konusu olan "bilgileri otomatik olarak işleme tabi tutan sistem" ifadesinin yerine "bilişim sistemi" kavramının kullanılmasıdır. Böylelikle "bilgileri otomatik olarak işleme tabi tutan sistem" kavramı nedeniyle ortaya çıkan karışıklıklar önlenilecektir¹². Ancak yasa metnindeki bu olumlu düzenlemeye rağmen 243. maddenin gerekçesinde bilişim sisteminin "verileri toplayıp yerleştirdikten sonra bunları

⁷ **Murat Volkan Dülger**, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", Kazancı hukuk, işletme ve Maliye Bilimleri Dergisi, S.5, Ocak 2005, s.114.

⁸ **Dülger**, Bilişim Suçları, s.210.

⁹ **Dülger**, Bilişim Suçları, s.211.

¹⁰ **Berrin Akbulut**, "Türk Ceza Hukukunda Bilişim Suçları", Yayınlanmamış Doktora Tezi (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı), Konya, 1999, s.78; **Olgun Değirmenci**, "Bilişim Suçları", Yayınlanmamış Yüksek Lisans Tezi (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı), İstanbul, 2002, s.152, 153.

¹¹ **Dülger**, Bilişim Suçları, s.211.

otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler” olarak tanımlanması yerinde olmamıştır. Yasa koyucunun bilişim sistemini tanımlamayıp bunu öğretiye bırakması en doğru yaklaşım olacaktı; buna rağmen bir tanım yapılmak isteniyorsa bu konuda artık aşılmış ve hatalı olan bu tanımın yerine öğretide yer alan, hem daha kapsayıcı hem de daha doğru olan tanımlardan birinin tercih edilmesi gerekirdi.

Kavramlar konusunda 5237 sayılı TCK ile getirilen bir diğer yeni ve olumlu düzenleme ise “diğer her hangi bir unsur” kavramının da maddelerden çıkartılarak yalnızca “veri” kavramının kullanılmış olması ve bunun, tüm suçların üzerinde işlendiği suçun maddi konusu olduğunun kabul edilmesidir¹³.

II. 5237 sayılı TCK ‘da Düzenlenen Bilişim Suçları

A. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tipleri

1. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu (m.243)

YTCK’da bilişim suçlarının ayrı bir başlık altında düzenlendiği ikinci kitabın “topluma karşı suçlar” başlıklı üçüncü kısmının “bilişim alanında suçlar” başlıklı onuncu bölümünün ilk maddesinde “bilişim sistemine girme” başlığıyla bu suç tipi düzenlenmiştir. Bu maddeyle yasa koyucu “bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme” eylemini suç tipi haline getirmiştir.

Bu maddede yer alan suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. maddesinde öngörülen “hukuka aykırı erişim” düzenlemesine paralellik sağlanmaktadır¹⁴.

765 sayılı TCK’nın 525 a/1 maddesindeki verilerin ele geçirilmesi suçunun düzenlenişi açısından öğretide getirilen en önemli eleştiri, bu suçun gerçekleşebilmesi için bilişim sisteminde bulunan verilerin fail tarafından ele geçirilmesinin gerektiği, oysa sanal alanda en sık karşılaşılan ihlal çeşitlerinden birisi olan bilişim sisteminin güvenliğinin kırılarak sisteme hukuka aykırı olarak girilmesi ve orada kalınması eylemlerinin, düzenlemenin bu şekli nedeniyle yaptırımsız kaldığıydı. İşte bu düzenlemeyle, 5237 sayılı TCK’da öğretilen gelen bu eleştiriler dikkate alınarak yasanın 243. maddede veriler ele geçirilmeksizin verilere yetkisiz erişim eylemleri suç tipi haline getirilmiştir¹⁵.

5237 sayılı TCK’nın 243. maddesi ile bilişim sistemine girişlerin cezalandırılması için “verilerin ele geçirilmesi” şartı kaldırılmakta ve veri ele geçirilsin ya da geçirilmesin bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınması yani bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmektedir¹⁶. 5237 sayılı TCK’nın 136. maddesiyle verilerin hukuka aykırı olarak ele geçirilmesinin ayrı bir suç tipi olarak düzenlendiği göz önünde bulundurulduğunda, aslında hukuka aykırı olarak bilişim sistemine girme ve sistemde

¹²Yılmaz Yazıcıoğlu, “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Y:1, S:1, Ocak-Mart 2004, s.175; Değirmenci, Bilişim Suçları, s.152; Akbulut, Ceza Hukukunda Bilişim Suçları, s.78.

¹³ Dülger, Bilişim Suçları, s.212.

¹⁴Yazıcıoğlu, 2001 Tasarısının Değerlendirilmesi, s.177.

¹⁵ Murat Volkan Dülger, “Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi”, Türk Ceza Kanunu Tasarısı: Türk Ceza Hukuku Derneği Toplantısı (10 Temmuz 2004): İstanbul Barosu-Türk Ceza Hukuku Derneği Toplantısı (10 Eylül 2004): Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul, İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını, 2004, s.111.

¹⁶Yazıcıoğlu, 2001 Tasarısının Değerlendirilmesi, s.177; Akbulut, Ceza Hukukunda Bilişim Suçları, s.78; Değirmenci, Bilişim Suçları, s.153.

kalma suçunun ilk defa bu yeni yasayla getirilen bir suç tipi olduğu görülmektedir. Hemen belirtilmelidir ki özellikle bilişim korsanlarına karşı etkili olabilecek bu düzenleme son derece yerinde ve çağdaş bir düzenlemedir¹⁷.

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçuna karşılaştırmalı hukukta birçok ülke hukukunda yer verilmektedir, bu suç tipi genellikle verilerin ele geçirilmesi suçuyla birlikte düzenlenmektedir. Buna örnek olarak; Fransa CK. m.323-1, Alman CK. m.202a, Danimarka CK. m.193 ve 263, Norveç CK. m.145/2, İtalyan CK. m.616/2, 617quarter, 617 quinquies, 618, Lüksembourg CK. m.309, İrlanda Criminal Damage Act'de m.5/1, Hollanda CK. m.98, 98a, 98b, 98c, ve 273 verilebilir¹⁸.

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçuyla korunan hukuksal değer bilişim sisteminin güvenliğidir. Bilişim sistemine hukuka aykırı erişimin engellenmesiyle, sistemin maliki ya da kullanıcısı gibi bir şekilde sistemden faydalanan kişilerin çok sayıdaki farklı türden çıkarları korunmaktadır. Bu kişilerin çıkarları; verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabilmektedir. Ancak tüm bunların üstünde ve bunları kapsayacak şekilde yer alan hukuksal değer bilişim sisteminin güvenliğidir¹⁹.

Öğretide bazı yazarlar ise bu suçla korunan hukuksal değer bilişim sisteminin güvenliği olmadığını belirtmekte, ancak korunan hukuksal değer ne olduğunu ifade etmemektedirler. Bunun yerine suçun maddi konusunda açıklanması gereken, suçun seçimlik hareketli mi yoksa bağlı hareketli bir suç mu olduğu konusunu incelemekte bu suçla yetkisiz erişim ve sistemde kalmaya devam etmenin birlikte gerçekleşmesi halinde suçun oluşacağını belirtmektedirler²⁰. Yukarıda da belirttiğimiz gibi bu açıklama suçun maddi unsuruna ilişkindir. Suç tipinin ister seçimlik hareketli ister bağlı hareketli olduğu kabul edilsin sonuç değişmemekte bu suçla korunan hukuksal değer bilişim sisteminin güvenliği olmaktadır.

Bu suçun maddi unsurunun hareket kısmını, hangi yolla olursa olsun bir bilişim sistemine girilmesi ve bilişim sisteminde kalınmaya devam edilmesi oluşturmaktadır. Görüldüğü üzere bu suç tipi bağlı hareketli olarak düzenlenmiştir, bu nedenle fail öncelikle hukuka aykırı olarak bilişim sistemine girmeli ve hukuka aykırı olarak bilişim sisteminde kalmaya devam etmelidir^{21;22}.

¹⁷ **Murat Volkan Dülger**, "Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler", 2. Polis Bilişim Sempozyumu, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s.201.

¹⁸ **Stein Schjolberg**, "The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries" (Çevrimiçi) <http://www.mosstingrett.no/info/legal.html#37>, 08.02.2004; **Değirmenci**, Bilişim Suçları, s.128.

¹⁹ **Necati Meran**, Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara, Seçkin Yayıncılık, 2005, s.363; **Dülger**, Bilişim Suçları, s.214.

²⁰ **Ali Karagülmez**, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara, Seçkin Yayıncılık, 2005, s.167.

²¹ **Levent Kurt**, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, 2005, s.151; **Meran**, a.g.e., s.365; **Karagülmez**, a.g.e., s.167.

²² Biz bu konuda Bilişim Suçları isimli kitabımızda suç tipinde "veya" bağlacı kullanıldığından hareketle suç tipinin seçimlik hareketli olduğunu savunmuştuk. Ancak görüldüğü üzere suç tipinde "ve" bağlacı kullanılmış ve suç bağlı hareketli bir suç olarak tanımlanmıştır. Bu nedenle biz de bu çalışmada konu hakkında doğru görüş belirten diğer yazarların görüşüne katılıyoruz. **Dülger**, Bilişim Suçları, s.217.

2. Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (m.244/1-2)

5237 sayılı TCK'nın 244.maddesinin 1. ve 2. fıkralarında bilişim sistemine ve verilere her ne yöntemle olursa olsun zarar verme eylemleri düzenlenmiştir. Bunlardan birinci fıkrada “bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması” eylemleri ikinci fıkrada ise “bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi” eylemleri suç tipi haline getirilmiştir.

Bu suç tipiyle, Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen “verileri etkileme” ve 5. maddesinde öngörülen “sisteme etki” düzenlemelerine paralellik sağlanmaya çalışıldığı belirtilmelidir²³.

Bu suç tipi 5237 sayılı TCK'da, 765 sayılı TCK'nın 525 b/1 maddesinde düzenlenen “verilere veya veri işleme zarar vermek suçunun” yerine geçmek üzere yer almaktadırlar.

Günümüzün modern yaşama düzenin ana konularını oluşturan ekonomi, sağlık, eğitim, bilimsel araştırmalar, idare, savunma vb. gibi pek çok yaşamsal alanda bilişim sistemleri vazgeçilmez araçlar olmuşlar, bu alanların pek çok yerinde geri dönülmez şekilde insanların yerini almışlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin kendisinin ya da içerdiği verilerin zarar görmesi ya da bu sistemlerin geçici süreyle de olsa çalışmaması çok büyük zararlara neden olabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsleri, kurtçuklar, truva atları gibi zarar verici yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana sokan faillerinin dahi öngördüğünden daha fazla zarara yol açabilmektedir. Yasa koyucu da bu büyük tehlikeyi öngörerek verilere ya da veri işleme zarar verme eylemlerini bu maddeyle suç haline getirmiştir.

Bu düzenleme ile bilişim sisteminin her nasıl olursa olsun çalışmasının engellenmesi ya da sistemin bozulması cezalandırılmak istenmektedir. Maddenin gerekçesinde de, bu maddeyle bilişim sistemlerine yöneltilen ızzar eylemlerinin ayrı bir suç haline getirildiği belirtilmektedir. Ayrıca yine maddenin gerekçesinde, yapılan düzenleme ile “aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçunun konusu oluşturmaktadır” denilerek bilişim sisteminin somut ve soyut bütün unsurlarının bu suçun konusunu oluşturacağı ifade edilmektedir. Gerekçede “özel bir ızzar eylemi” denilmek suretiyle bilişim sisteminin çalışmasını engellemeye yönelik eylemler kastedilmektedir. Düzenlemede yerinde bir yaklaşımla 765 sayılı TCK'da yer alan düzenlemeden farklı olarak “zarar verme” tabiri kullanılmamakta, böylelikle bilişim sisteminin donanım kısmına mala zarar vermek kastıyla yapılan eylemler, bu maddenin kapsamı dışında tutulmaktadır²⁴. Bu düzenlemeyle, öğretide bu konuda ortaya çıkan tartışmaların dikkate alındığı görülmektedir.

Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu da hukuka aykırı olarak bilişim sistemine girilmesi veya sistemde kalınması suçunda olduğu gibi hemen her ülke hukukunda düzenlenmiştir. Buna örnek olarak; Fransa CK. m.323-2, Alman CK. m.303a, Avusturya CK. m.126/a1, Finlandiya CK. 35. kısım

²³Yazıcıoğlu, 2001 Tasarısının Değerlendirilmesi, s.179.

²⁴Karşı görüşte bkz: Değirmenci, Bilişim Suçları, s.154; Özel, İletişim Faaliyetleri, s.860, 865; Yazıcıoğlu, 2001 Tasarısının Değerlendirilmesi, s.179.

m.1/2, Avustralya CK. m.76C, Danimarka CK. m.279a, Norveç CK. m.151b, İrlanda Criminal Damage Act’de m.2/1 ve 2/a verilebilir²⁵.

3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m.244/4)

5237 sayılı TCK’nın 244. maddesinin 4. fıkrasında “bilşim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu” düzenlenmiştir. Bu suç tipi söz konusu fıkra 1. ve 2. fıkralarda yer alan eylemlere atfı yapılarak düzenlenmiştir, her iki fıkra birlikte okunduğunda 244. maddenin 4. fıkrasında yer alan suç tipi şu şekilde olmaktadır: “bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemin içerdği verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde,... cezasına hükmolunur”.

Bu suç tipi 765 sayılı TCK’da 525 b/2 maddesinde çok geniş bir şekilde düzenlenmiş ve durum öğretide eleştirilmiş, uygulamada ise çeşitli zorluklara yol açmıştır. 5237 sayılı TCK’da bilişim suçları düzenlenirken öğretilen gelen bu eleştiriler dikkate alınmış ve TCK’daki suç tipi olması gerektiği gibi dört parçaya bölünmüştür. Buna göre 765 sayılı TCK’nın 525 b/2 maddesinin içerdği bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak, banka ve kredi kartlarını kötüye kullanmak, bilişim sistemi aracılığıyla dolandırıcılık ve bilişim sistemleri aracılığıyla hırsızlık eylemleri farklı suç tipleri olarak düzenlenmiştir. İşte inceleme konusu olan suç tipiyle de yalnızca “bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama” eylemleri düzenlenmiş ve bunların nasıl gerçekleştirileceği suç tipinde açıkça belirtilmiştir.

Ayrıca suç tipinin düzenlendiği 4. fıkra “başka bir suç oluşturmaması halinde” ifadesi kullanılarak aynı eylemlerin gerçekleştirilerek hukuka aykırı yarar elde edilmesi ancak bunun bir başka suç tipinde düzenlenmiş olması halinde bu suç tipinin uygulanmayacağı belirtilmiştir. Yasa yapma tekniği bakımından pek uygun olmayan bu düzenleme ile ne anlaşılması gerektiği yasanın gerekçesinde belirtilmiştir; buna göre “bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir”.

4. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (m.245)

5237 sayılı TCK ile bilişim suçları açısından getirilen önemli ve olumlu değişikliklerden birisi de, yasanın 245. maddesinde “banka veya kredi kartlarının kötüye kullanılması” eylemlerinin ayrı bir maddede suç tipi olarak düzenlenmesidir.

765 sayılı TCK’nın 525 b/2 maddesinde düzenlenen “bilişim sistemi aracılığıyla hukuka aykırı yarar elde edilmesi suçunun”, banka kartlarının veya kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesi eylemlerini de kapsayıp kapsamadığı konusunda çeşitli görüşler ileri sürülmüştür. Yargıtay Ceza Genel Kurulu’nun bu konuda verdiği bir karara²⁶ kadar uygulamada da bu konuda farklı yaklaşımlar ortaya çıkmıştır. 5237 sayılı TCK’da bu eylemler ayrı bir maddede açık bir şekilde düzenlenerek bu tartışmalara son verilmek

²⁵Schjolberg, a.g.y.; Değirmenci, Bilişim Suçları, s.129, 130; Yazıcıoğlu, Bilgisayar Suçları, s.182, 183.

²⁶Yargıtay Ceza Genel Kurulu, K.t. 10.04.2001, E.2001/76-30 K.2001/757, Yargıtay Kararları Dergisi, Haziran 2001, s.913-915.

istenmiştir; öğretide söz konusu Yargıtay Ceza Genel Kurulu kararının, yasaya aktarılması amacıyla bu düzenlemenin yapıldığı da belirtilmiştir²⁷.

Söz konusu eylemler özellikle yukarıda anılan Yargıtay Ceza Genel Kurulu kararından sonra hem öğretide hem de uygulamada 765 sayılı TCK'nin 525 b/2 maddesinde yer alan "bilişim sistemi aracılığıyla hukuka aykırı yarar elde etme suçunun" kapsamı içinde değerlendirilmiştir; ancak bu kez de suçun aracı olan kartın ele geçiriliş ve kullanılış biçimine göre çeşitli ayrımlar oluşturularak söz konusu eylemlerin klasik dolandırıcılık suçunu mu yoksa bilişim sistemi aracılığıyla hukuka aykırı yarar elde etme suçunu mu oluşturduğu tartışılmıştır.

İşte bu düzenlemeyle söz konusu tartışmalara ve ayrımlara da son verilmek istenmiş²⁸ ve kredi veya banka kartıyla gerçekleştirilen her türlü hukuka aykırı yarar sağlama eylemlerinin bu suç tipini oluşturacağı maddenin gerekçesinde de belirtilmiştir²⁹.

Banka veya kredi kartlarının kötüye kullanılması suçu, 765 sayılı TCK'da 525 b/2 maddesi yer alan "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçu" içerisinde değerlendirilen "banka veya kredi kartlarının yetkisiz kullanımı eylemi" ile örtüşmektedir. İşte 765 sayılı TCK'da bir suçun maddi unsuru oluşturan eylemlerden biri olan söz konusu kötüye kullanımlar 5237 sayılı TCK'nın 245. maddesinde bağımsız bir suç tipi haline getirilmiştir.

Yasanın bu maddesiyle yasa koyucu sahte kredi veya banka kartlarının üretilmesini kaynaktan durdurmak istemekte, bu kartların üretilmesinden kullanılmasına kadar geçen dört aşamayı cezalandırmaktadır. Bu aşamalardan ilki kartın sahte olarak üretilmesi, ikincisi satılması ya da devredilmesi, üçüncüsü satın alınması ya da devir alınması ve dördüncüsü de bunların haksız yarar elde temek amacıyla kullanılmasıdır. 245. maddenin 2. ve 3. fıkralarında söz konusu bu aşamalar ayrı ayrı tanımlanarak cezalandırılmaktadır.

5237 sayılı TCK'nın 245. maddesi "Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanun" başlıklı 29.06.2005 tarih ve 5377 sayılı yasa ile değiştirilmiştir. Maddenin ilk halinde ikinci fıkra olarak yer alan düzenleme üçüncü fıkra haline getirilmiştir ve yeni bir suç tipi olarak ikinci fıkra eklenmiştir. Ayrıca kişisel cezasızlık hali öngören dördüncü fıkra da bu son yasa değişikliğiyle madde metnine eklenmiştir. Yapılan değişiklikle bazı eksiklikler giderilemeye de hemen belirtilmelidir ki madde olumlu yönde olarak değiştirilmiştir³⁰.

Değişiklik yasasının 27. maddesiyle TCK'nın bu maddesinde düzenleme yapılmıştır. Bu düzenlemeyle ilk halinde iki fıkra olan madde dört fıkraya çıkarılmış, suç tipine eklenen 2. fıkrayla suçun yeni bir işleniş biçimi tanımlanmış ve 4. fıkrayla da bir kişisel cezasızlık nedeni oluşturulmuştur. Suç tipinin değiştirilmeyen 1. ve 3. (eski 2.) fıkralarında ise öngörülen cezalarda değişiklik yapılmıştır.

Bu suç tipi, gelişen teknolojiyle birlikte artık günümüz yaşamının vazgeçilmez ekonomik araçlarından biri olan banka veya kredi kartlarının kötüye kullanılarak bu kartları üreten finans kurumlarına ya da kartların kullanıcısı olan kişilere zarar verilmesi eylemlerini

²⁷ **Cevat Özel**, "Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, İstanbul, C.LXXV, S.7-8-9, Eylül 2001, s.863.

²⁸ **Yazıcıoğlu**, 2001 Tasarısının Değerlendirilmesi, s.182.

²⁹ "Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirmeleri uygun görülmüştür."

³⁰ **Murat Volkan Dülger**, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Güncel Hukuk Dergisi, İstanbul, S:23, Kasım 2005, s.28-30.

önlemek, bu gerçekleştiğinde ise cezalandırmak üzere düzenlenmiştir. Dolayısıyla bu suç tipiyle korunan hukuksal değer kişilerin mal varlığıdır³¹. Bu nedenle inceleme konusu suç tipi açısından sürekli olarak dile getirdiğimiz eleştiriye bir kez daha belirtmekte yarar bulunmaktadır³². TCK’da suçlar, korudukları hukuksal değere göre sınıflandırılmışlardır; bu her ne kadar bilişim sistemleri aracılığıyla işlenebilen bir suç tipi olsa da, koruduğu hukuksal değer esas olarak kişilerin mal varlığı olduğuna göre yasada “mal varlığına karşı suçlar” bölümünde yer alması gerekir. Ancak yasanın hazırlık çalışmalarından beri ısrarla dile getirdiğimiz bu önemli eleştiriye karşın, TCK’da değişiklik yapan 5377 sayılı yasada bu yönde bir değişiklik yapılmamıştır.

Maddenin değişiklikten önceki ilk halinde de yer alan 1. fıkrasında “başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlama” eylemi, yine maddenin özgün halinde yer alan 3. fıkrasında ise “sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla hukuka aykırı yarar sağlama” eylemi düzenlenmiştir. Buna göre maddenin birinci fıkrasında başkasına ait banka ya da kredi kartının, nasıl olursa olsun ele geçiren ya da elinde bulunduran kişi tarafından, kart sahibinin ya da kartın verilmesi gereken kişinin rızası olmaksızın kullanılması ve bu yolla failinin kendisine ya da üçüncü bir kişiye hukuka aykırı yarar sağlama eylemi suç tipi haline getirilmiştir. Maddenin 3. fıkrasında ise sahte olarak üretilen ya da üzerinde işlem yapılarak sahte hale getirilen gerçek bir kredi ya da banka kartının kullanılması yoluyla failin kendisine veya bir başkasına hukuka aykırı yarar elde etmesi eylemi düzenlenmiştir³³. Yukarıda da belirttiğimiz üzere bu maddelerde öngörülen cezalar dışında bir değişiklik yapılmamıştır.

Banka veya kredi kartlarının kötüye kullanılması suçunda 5377 sayılı yasayla yapılan esas değişiklik maddeye eklenen ikinci ve dördüncü fıkralarla olmuştur. Bunlardan ikinci fıkrayla suçun farklı bir işleniş biçimi tanımlanırken dördüncü fıkrayla da birinci fıkra açısından geçerli olan bir kişisel cezasızlık nedeni düzenlenmiştir.

245. maddenin 2. fıkrasında “başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi” eylemleri suç tipi olarak tanımlanmıştır. Görüldüğü üzere esas olarak bu maddeyle “sahte banka veya kredi kartı üretilmesi ve bunun dağıtımının yapılması” eylemleri düzenlenmiştir. Maddenin değişiklikten önceki ilk haline bakıldığında birinci fıkrada rıza dışı kart kullanımının, ikinci fıkrada ise sahte olarak üretilen ya da üzerinde sahtecilik yapılan kart kullanımının cezalandırıldığı görülmektedir; ancak maddenin bu ilk halinde önemli bir eksiklik olarak yalnızca sahte kart üretiminin ve bunun dağıtımının yapılmasının cezalandırılmadığı görülmektedir. 5377 sayılı yasanın 27. maddesiyle yeniden düzenlenen 5237 sayılı TCK’nın 245. maddesinde bu önemli eksiklik giderilmiş ve söz konusu eylemler de maddeye dahil edilerek bunlar suç tipi olarak tanımlanmıştır.

Buna göre failin başka kişilere ait banka hesaplarıyla bağlantılı olarak sahte banka veya kredi kartı üretmesi, satması, devretmesi eylemi suç oluşturacağı gibi bu şekilde üretilen kartların satın alınması ya da kabul edilmesi eylemleri de suç oluşturacaktır. Yasa koyucu böylelikle söz konusu sahte kartların üretilmesini kaynaktan durdurmak istemekte, bu kartların üretilmesinden kullanılmasına kadar geçen dört aşamayı cezalandırmaktadır. Bu aşamalardan ilki kartın sahte olarak üretilmesi, ikincisi satılması ya da devredilmesi, üçüncüsü satın alınması ya da devir alınması ve dördüncüsü de bunların haksız yarar elde etmek

³¹ Dülger, Bilişim Suçları, s.252.

³² Bu konuda bkz: Dülger, Bilişim Suçları, s.252.

³³ Dülger, Bilişim Suçları, s.254.

amacıyla kullanılmasıdır. İşte sahte kartlar açısından geçerli olan bu dört aşamadan ilk üçü 245. maddenin 2. fıkrasıyla ayrı ayrı tanımlanmıştır. Yasanın maddesinde kartların el değiştirmesinin maddi bir karşılıkla olup olmaması açısından bir ayırım yapılmamış ve her türlü el değiştirme cezalandırılmak istenmiştir.

Suç tipinde “başkalarına ait banka hesaplarıyla ilişkilendirilerek” denilmek suretiyle suç oluşması açısından bir ön şart getirilmiştir. Ancak failin, kart çıkaran bir finans kurumunun ya da bankanın bilişim sistemine girerek hukuka aykırı bir biçimde kendisi ya da aslında hiç olmayan hayali bir kişi adına yeni bir hesap açması ve bu hesapta yine hayali olarak yaptığı transferlerle para bulundurması, ayrıca bu hesaba bağlı olarak kredi kartı üretmesi ve bu kartı kullanması ya da satması durumunda, fail 245. maddenin 2. fıkrasında tanımlı suçu işlemiş olacak mıdır? Söz konusu bu ön şart nedeniyle faili bu maddeden sorumlu tutmak mümkün değildir; çünkü fail bu örnekte başkasına ait bir hesapla ilişkilendirerek kart oluşturmamış, tamamen hayali olan ancak başkasına ait olmayan bir hesapla ilişkilendirerek kart oluşturmuştur. Bu durumda fail öncelikle hukuka aykırı olarak bilişim sistemine girip hayali bir hesap açmak ve buraya para transfer etmekle TCK’nın 158. maddesinin 1. fıkrasının f bendinde tanımlı “bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle” nitelikli dolandırıcılık suçunu işlemiş olacaktır. Failin bu yöntemle ürettiği sahte kartı kullanması halinde ise ayrıca 245. maddenin 3. fıkrası nedeniyle sorumlu tutulması mümkündür. Ancak failin bu şekilde ürettiği sahte kartı kullanmayıp satması ya da devretmesi halinde 245. maddenin 2. fıkrası nedeniyle cezalandırılması mümkün değildir, çünkü bu halde fıkra da tanımlı ön şart gerçekleştirilmemiş yani başkasına ait bir hesapla bağlantı kurulmamış olacaktır.

245. maddenin 2. fıkrası son derece yerinde olarak düzenlenmiş ve madde metnine eklenmiş, böylelikle bu konudaki önemli bir eksiklik giderilmeye çalışılmıştır. Özellikle günümüzde gittikçe yaygınlaşan ve önemli bir sorun haline gelen “phishing” (oltaya alma)³⁴ eylemlerine karşı caydırıcı bir etkisi olabileceği gibi bu yöntemi kullanarak sahte kart üreten ve bunun ticaretini yapanların da cezalandırılmasını sağlayacaktır.

Ancak fıkranın başına eklenen “başkalarına ait banka hesaplarıyla ilişkilendirilerek” ön şartı yukarıda verilen örnekte görüldüğü üzere suç tipinde eksiklik oluşturmaktadır. Bu nedenle bu ifadeye yer verilmeden suçun tanımlanması yukarıda verilen örnekte ve benzerlerinde olduğu gibi tüm eylemlerin kapsanması açısından gereklidir. Mutlaka böyle bir ifadeye yer verilmek isteniyorsa “herhangi bir banka hesabıyla ilişkilendirilerek” ifadesi tercih edilmelidir.

Bunların yanı sıra bu suç tipi açısından belirtilmesi gereken bir başka konu da failin önce sahte kredi kartını üretmesi, sonrasında ise kartı kendisinin kullanması halinde hem 245. maddenin 2. fıkrası hem de 3. fıkrasında belirtilen eylemlerden ayrı ayrı cezalandırılmayacak olmasıdır. Çünkü kartı üreten ile kullananın aynı kişi olması durumunda, kullanmak için öncelikle sahte kartın üretilmesinin gerektiği göz önünde bulundurulacak ve bu durumda fail yalnızca 245. maddenin 3. fıkrasından dolayı sorumlu tutulacaktır.

5377 sayılı değişiklik yasasıyla yapılan bir başka değişiklik de söz konusu bu iki fıkranın yaptırımlarında gerçekleştirilmiştir. Buna göre 1. fıkranın hürriyeti bağlayıcı

³⁴ “Phishing” İngilizce “fishing” (balık tutma) kelimesinden türetilen ve Türkçeye “oltaya alma” olarak çevrilebilecek bir kelimedir. Bu eylem kısaca, fail tarafından mağdurun kullandığı bankanın, elektronik postanın ya da buna benzer mağdurun kişisel bilgilerini girmesi gereken bir web sitesinin kopyasının yapıp mağdurun aldatılarak kişisel bilgilerinin alınması ve böylelikle fail tarafından haksız yarar elde edilmesini sağlayan bir tür bilişim sistemleri aracılığıyla gerçekleştirilen dolandırıcılıktır. Bu konuda bkz: (Çevrimiçi) <http://www.antiphishing.org/>, 17.08.2005; “Sanal Dolandırıcılıkta Son Nokta Phishing”, (çevrimiçi) <http://www.iem.gov.tr/iem/?idno=147>, 17.08.2005.

cezasında deęişiklik yapılmazken fıkranın ilk halinde “adli para cezası verilir” şeklindeki düzenlenmesi “beşbin güne kadar adli para cezası verilir” şekline dönüştürülmüştür. Üçüncü fıkra da ise hürriyeti bağlayıcı ceza açısından deęişikliğe gidildięi gibi ayrıca adli para cezası da bu fıkraya eklenmiştir; buna göre fıkranın içerdiği yaptırım “dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır” şeklinde düzenlenmiştir. Birinci fıkranın ilk halinde belirsiz olan adli para cezasının hakime takdir yetkisi de tanınarak sınırlandırılması ceza hukukunun belirginlik ilkesi açısından olumludur. Aynı şekilde maddenin üçüncü fıkrası açısından adli para cezasının öngörülmesi de yerinde bir düzenleme olmuştur. Ancak üçüncü fıkranın ilk halinde yedi yıl olan hürriyeti bağlayıcı cezanın üst sınırı sekiz yıla çıkartılarak adeta 245. maddenin ilk iki fıkrasında üç yıl, üçüncü fıkrasında ise dört yıllık alt sınırlar belirlenerek, üst sınırlarında artan bir derecelendirme yapılmıştır. Ancak hemen belirtilmelidir ki bunlardan özellikle ikinci ve üçüncü fıkralarda düzenlenen eylemler biri diğerine göre daha hafif ya da daha ağır olan eylemler değildir. Her üç fıkra da düzenlenen eylemler banka ve kredi kartlarının kötüye kullanımlarının farklı eylemler gerçekleştirilmesi halidir. Ancak ilk fıkra da sahtecilik ya da bilişim sistemiyle gerçekleştirilen dolandırıcılık söz konusu değilken ikinci ve üçüncü fıkralarda bunlar söz konusudur. O halde birinci fıkraya göre diğer fıkraların cezalarının daha ağır olması gerekir. Ancak görüldüğü üzere birinci ve ikinci fıkra da yer alan hürriyeti bağlayıcı cezaların alt sınırları aynıdır. Diğer yandan benzer biçimde adeta biri diğerinin tamamlayıcısı nitelikte olan ikinci ve üçüncü fıkra da yer alan eylemlerin cezalarında bir farklılığa gidilmesi gerekli değilken bu kez bu fıkralarda yer alan hürriyeti bağlayıcı cezaların hem alt sınırlarında hem de üst sınırlarında farklılık yaratılmasının bir açıklaması bulunmamaktadır. Nitekim bu düzenlemenin hangi gerekçeyle yapıldığı açıklanmamıştır.

Yeri gelmişken burada değinilmesi gereken bir konu da özellikle 5271 sayılı CMK’nın yapılması aşamasında hukuk dünyamıza giren “gerekçesiz yasa yapma tekniğinin” bu yasayla sürdürülmeye devam edildiğidir. Gerçekten de 5377 sayılı yasanın gerekçesi bulunmamaktadır. Yasa Cumhurbaşkanınca görüşülmek üzere bir daha meclise iade edildiğinde, yalnızca gerekçede gösterilen maddeleri savunan bir rapor TBMM Adalet Komisyonunca hazırlanmıştır. Bunun dışında söz konusu deęişikliklerin genel nedenini ve tek tek deęişiklik yapılan maddelerde neden deęişiklik ihtiyacı duyulduğunu ve hangi amaçla deęişiklik yapıldığını gösteren gerekçeler ne yazık ki bulunmamaktadır. Bu nedenle de diğer maddelerin yanı sıra 245. maddenin 3. fıkrasında hürriyeti bağlayıcı cezanın üst sınırının hangi nedenle cezalandırıldığını gösteren bir gerekçe mevcut değildir.

TCK’nın 245. maddesinde 5377 sayılı yasanın 27. maddesiyle yapılan son deęişiklik ise, maddeye eklenen 4. fıkradır. Bu fıkrayla, maddenin birinci fıkrasında yer alan suç tipi açısından bir “kişisel cezasızlık durumu” düzenlenmiştir. Bu düzenleme bir hukuka uygunluk nedeni değildir. Çünkü bu fıkrayla eylem bu kişiler hakkında hukuka aykırı eylem olmaktan çıkarılmamakta yalnızca söz konusu eylemin fıkra da belirtilen kişiler tarafından işlenmesi halinde bu kişilere ceza verilmeyeceği belirtilmektedir. Bunun doğal sonucu olarak, failin ya da faillerden birinin fıkra da tanımlı bir kişi tarafından yine fıkra da tanımlı bir başka akrabasına karşı işlenmesi halinde bu kişiye ceza verilmeyecek ancak suça katılan diğer suç ortaklarına gerçekleştirdikleri bu eylemden dolayı ceza verilecektir. Bu fıkra da uygulamada çok sık karşılaşılan bir durum olması nedeniyle kişisel cezasızlık nedeni düzenlenmiştir. Ancak burada suç tipinin, söz konusu kişiler açısından takibi şikayete bağlı bir suç olarak düzenlenmesinin daha yerinde olacağını düşünmekteyiz. Çünkü bu eylemle hukuka aykırı bir eylem gerçekleştirilmiş ve bir suç işlenmiştir; fıkra da belirtilen kişiler her ne kadar akraba da olsalar böyle bir durumla karşılaştıklarında çeşitli düşüncelerle (örneğin akrabası olan failin cezasını çekip akıllanması ve bir daha böyle bir işe kalkışmaması için) eylemi gerçekleştiren

kişilerin cezalandırılmasını isteyebilirler. Bu durumda failin akrabası olan mağdura şikayette bulunma yetkisinin tanınmayıp, fail açısından tamamen cezasızlık halinin düzenlenmesi yerinde olmamıştır.

Kısacası, bu maddeyle söz konusu kartların haksız, hukuka aykırı olarak kullanılması yoluyla bankaların ve kart sahiplerinin zarara sokulması ve bu suretle hukuka aykırı yarar sağlanması önlenmek istenmektedir³⁵. Bu durum maddenin gerekçesinde de açık bir şekilde ifade edilmektedir³⁶.

Bu suçun gerçekleştirilmesiyle kişilerin mal varlığı üzerinde büyük zararlar verilebilmektedir, nitekim bu güne kadar gerçekleşen olaylardan ve Yargıtay kararlarına yansıyan eylemlerden bu durum açık bir şekilde görülmektedir. Dolayısıyla bu suçla korunan hukuksal değer kişinin mal varlığı olarak belirlenmektedir.

Suçla korunan hukuksal değer bu şekilde belirlenmesinden sonra bu suç tipinin düzenlenişi açısından önemli bir eleştiri ifade edilmelidir. Banka veya kredi kartlarının kötüye kullanılması suçunun koruduğu hukuksal değer bireyin mal varlığı olmasına rağmen bu suç mal varlığına karşı suçlar bölümünde değil, bilişim alanında suçlar bölümünde düzenlenmiştir. Bu düzenleme şekli ise yasanın sistematığına aykırı olduğu için değiştirilmeli ve bu suç tipi “mal varlığına karşı suçlar” bölümüne alınmalıdır³⁷.

Bu maddede aslında birbiriyle ilgili ve birbirinin adeta tamamlayıcısı nitelikte olan üç farklı suç tipi düzenlenmektedir. Birinci fıkrada “başkasına ait bir banka veya kredi kartının kullanılarak hukuka aykırı yarar sağlanması suçu”, ikinci fıkrada “sahte banka veya kredi kartı üretilmesi ve dağıtılması suçu”, üçüncü fıkrada ise “sahte kredi veya banka kartının kullanılmasıyla haksız yarar sağlanması suçu” tanımlanmaktadır.

B. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri

Veri korunması hukuku, hangi kişisel verilerin kim tarafından ve kimin için elde edildiğinin öğrenilmesi hakkını içerir. Türk hukuk düzeninde verilerin korunması konusu şu ana kadar yeterli ve gerekli ilgiyi görmemiştir. Bu konuda herhangi bir yasal düzenlemenin yokluğu bu konunun öncelikle kişilik haklarının korunması konusunun altında incelenmesini gerekli kılmıştır. Bu bağlamda kişisel verilerin korunması genel olarak MK’nın 24. maddesi altında değerlendirilmektedir. Kişisel verilerin izinsiz ele geçirilmesi dolayısıyla kişilik hakkının ihlali halinde ihlalin özel hukuk açısından sonlandırılması ve zararın tazmini Medeni Kaunu’nun 25 ve Borçlar Kanunu’nun 41 vd. maddelerine göre gerçekleştirilmektedir³⁸. Dolayısıyla kişilik hakkı ihlali ve bunun sonuçlarıyla ilgili MK ve BK maddeleri, kişilik ihlali hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin uygulama alanına sahiptir; çünkü ceza hukukunda hâkim olan suçta ve cezada yasallık ilkesi özel hukukta geçerli değildir³⁹.

Kişisel verilerin bilişim sistemi aracılığıyla ihlali, hukuka aykırı olarak ele geçirilmesi, kötüye kullanılması gibi eylemlerin yukarıda anılan ilke nedeniyle ceza hukuku açısından

³⁵Özel, İletişim Faaliyetleri, s.862; Değirmenci, Bilişim Suçları, s.158, 159.

³⁶ “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.”

³⁷ Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi, s.109; Dülger, Bilişim Suçları, s.252.

³⁸Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, 2004, s.100-103; Nilgün Başalp, “Kişisel Verilerin Korunması ve İnternet”, İnternet ve Hukuk, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.6.

³⁹Sibel Özel, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, Ankara, Seçkin Yayıncılık, 2004, s.168.

ayrıca düzenlenmesi ve bu eylemlerin suç tipi haline getirilmesi gerekmektedir. Bu açıdan Almanya’da bu alanda yapılan yasal düzenleme gibi, kişisel verilerin korunmasına ilişkin özel bir yasaya gereksinim olduğu belirtilmektedir⁴⁰. Ayrıca 765 sayılı TCK’nın 525 a/1 maddesinde düzenlenen verilerin ele geçirilmesi suçunun bu açıdan yeterli ve gerekli korumayı sağlamadığı belirtilmektedir⁴¹.

Kişisel verilerin ele geçirilmesi yoluyla kişilik haklarının ihlal edilmesi eylemlerinde dikkat edilmesi gerek bir konu da, devletin resmi güvenlik kuruluşları dışında birçok kurum ve kuruluşun da bireyler hakkında özel bilgiler toplaması ve bu bilgilerle kişilik haklarını ihlal etme olanağına sahip olmasıdır. Hastalar hakkında çok özel bilgileri bilişim sistemlerinde bulunduran hastaneler, DNA ve parmak izi analizi yapan ve bunun sonuçlarını bilişim sistemlerinde saklayan adli tıp kurumları, cep telefonu işletmecisi olan şirketlerin bulundurdıkları veriler bunlara örnek olarak verilebilir. Bu nedenle kişisel verilerin korunması açısından yapılacak düzenlemede yalnızca resmi kuruluşların bu bilgileri toplaması ve kullanması konusundaki çerçeve değil, söz konusu bilgileri depolayıp kullanabilme yetkisine ve teknolojisine sahip özel kuruluşlar açısından da yasal çerçeve belirlenmelidir⁴².

Yukarıda anılan görüş ve eleştiriler dikkate alınarak, 5237 sayılı TCK’da kişisel verilerin hukuka aykırı olarak oluşturulması, kullanılması ya da açıklanması eylemleri ayrı maddeler halinde düzenlenmiştir. Böylelikle 765 sayılı TCK’nın bilişim suçlarına ilişkin düzenlemesi açısından söz konusu olan önemli bir boşluk giderilmiştir.

Bu düzenlemenin bilişim suçları açısından olumlu bir tarafı da kişisel verilere ilişkin suç tiplerinin “bilişim alanında suçlar” başlıklı bölümde diğer suç tipleriyle bir arada değil, bu suçlarla korunan hukuksal değere göre, benzer hukuksal değerlerin korunduğu “özel hayata ve hayatın gizli alanına karşı suçlar” bölümünde düzenlenmiş olmasıdır⁴³.

Söz konusu suç tipleri aşağıda maddeler halinde ayrıntılı olarak incelenmektedir:

1. Kişisel Verilerin Kaydedilmesi Suçu (m.135)

5237 sayılı TCK’nın 135. maddesinin 1. fıkrasıyla, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi suç haline getirilmiştir. Maddenin 2. fıkrasıyla ise kişilerin siyasal, felsefi ve dinsel görüşlerinin, ırksal kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak yerleştirilmesi eylemleri suç tipi olarak düzenlenmiştir⁴⁴.

Gelişen bilişim teknolojisiyle birlikte çok sık karşılaşılan ve aynı zamanda kişilik haklarına bir saldırı niteliği de taşıyan eylem türü, kişilerin rızaları olmaksızın kişisel verilerinin bilişim sistemlerine yerleştirilmesidir.

Özellikle hastanelerin hastalarıyla ilgili, finans kurumlarının ve sigorta şirketlerinin müşterilerinin kredi olanağı ve ödeme gücüyle ilgili, ticari şirketlerin ise reklâm ve pazarlama

⁴⁰Yener Ünver, “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.LIX, S.1-2, İstanbul 2001, s.93,94: bu amaçla Adalet Bakanlığı tarafından “Kişisel Verilerin Korunması Kanunu Tasarısı” adıyla bir tasarı hazırlanmış ancak henüz yasalaşmamıştır. Bu tasarının ayrıntılı incelemesi için bkz: Başalp, Kişisel Verilerin Korunması ve Saklanması, s.107-126.

⁴¹Yener Ünver, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, Prof. Dr. Nurullah Kunter’e Armağan, İstanbul, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, 1998, s.437.

⁴²İbrahim Cerrah, “Bilişim Teknolojileri ve Etik: Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının ‘Etik Boyutu’ ve ‘Sosyal Sonuçları’”, Polis Bilimleri Dergisi, Ankara, C:4, S:1-2, Ocak-Haziran 2002, s.139.

⁴³Karşı görüşte bkz: Özel, İletişim Faaliyetleri, s.864.

⁴⁴Özel, İletişim Faaliyetleri, s.865; Değirmenci, Bilişim Suçları, s.156, 157.

amacıyla bu tür verileri toplayıp kullandığı bilinmektedir. İşte bu tür bilgilerin sanal ortama veri olarak aktarılması ve bu yapılırken bu verilerin ilgisinin izninin alınmaması inceleme konusu maddeyle suç tipi haline getirilmiştir. Bu durum maddenin gerekçesinde de açık bir şekilde belirtilmiştir⁴⁵.

Böylelikle maddenin gerekçesinde de belirtildiği üzere⁴⁶, Avrupa Konseyi'nin ürettiği belgelerden olan ve Türkiye'nin de usulüne uygun onayla tarafı olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili düzenlemeleri ülkemiz hukuku açısından geçerlilik alanı bulacaktır.

2. Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (m.136)

5237 sayılı TCK'nın 136. maddesiyle, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri bağımsız bir suç tipi olarak düzenlenmektedir; maddenin gerekçesinde de bu açıkça ifade edilmektedir⁴⁷.

Bu düzenleme özellikle Amerika Birleşik Devletleri ve İngiltere gibi ülkelerde çok sık karşılaşılan ve en fazla sayıda işlenen bilişim suçu olduğu ifade edilen kimlik hırsızlığı eylemlerine karşı uygulama alanı bulacak ve bu tür eylemler yaptırımsız kalmayacaktır. Gerçekten de günümüzde artık hemen tüm kişisel bilgiler ve kimlik bilgileri özellikle internette bulunmaktadır. Bu bilgilerin çoğu kişilerin verdikleri rızaya dayanarak çeşitli sitelere verilmektedir. İşte bu bilgilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da bu verilerin üçüncü kişiler tarafından ele geçirilmesinin suç tipi olarak düzenlenmesi yerinde bir düzenleme olmuştur.

3. Verilerin Yok Edilmemesi Suçu (m.138)

5237 sayılı TCK'nın 138. maddesiyle ise, yasal süresi dolmasına rağmen kişisel verileri sistem içinden yok etmekle görevli olan kişilerin bu görevlerini yerine getirmemeleri durumu suç haline getirilmektedir⁴⁸.

5237 sayılı TCK'da yer verilen bu suç tipiyle de hukuka uygun olarak sistemde bulunan kişisel verilerin sürekli olarak bu sistemlerde bulunması ve böylelikle her an ulaşılabilirliğinin sağlanmasının önüne geçilerek, verileri sistemden çıkarmayanlara yani bu konudaki görevlerini ihmal edenlere yaptırım öngörülmektedir.

İnsanlar doğaları gereği özgür varlıklardır. Bu nedenle sürekli olarak izlenen, haklarında bilgiler toplanan ve fişlenen bireyler olarak yaşamak istemezler. İnsanlarda sürekli izlendikleri duygusunun yaratılması, içinde bulundukları siyasal sisteme karşı da bir güvensizlik ve nefret duygusu yaratabilecektir; yani insanlar güven içinde ve özgür bir şekilde

⁴⁵ "Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alışveriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır. "

⁴⁶ "Bu bakımdan, söz konusu suç tanımı ile, Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanınmıştır."

⁴⁷ "Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır. "

⁴⁸Özel, İletişim Faaliyetleri, s.865; Değirmenci, Bilişim Suçları, s.157.

yaşamak isterler⁴⁹. İşte yaşamlarının belli bir kesitinde hukuka uygun bir biçimde de olsa bazı kişisel bilgileri veri şeklinde çeşitli sistemlere girilen bireylerin bu kişisel bilgilerinin bir zaman sonra bu sistemlerden çıkarılması gerekmektedir. Bu verilerin yok edilmesini hem birey hem de devlet ister. Çünkü vatandaşları hakkında sürekli bilgi toplayan ve bunları kaydeden kısacası vatandaşlarını fişleyen bir devlet asla çoğulcu, özgürlükçü ve demokratik bir devlet olamaz ve vatandaşlarını da bu çağdaş ilkelere bağlı bir toplum haline getiremez. İşte söz konusu bu suç tipiyle bunun önüne geçilmek istenmektedir.

C. Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri

Yukarıda açıklanan suç tipleri dışında, 5237 sayılı TCK’da farklı bölümlerde düzenlenen ve bilişim sistemleri aracılığıyla işlenebilecek başka suç tipleri de bulunmaktadır. Bu suç tipleri ve bunlarla ilgili kısa açıklamalar şunlardır:

1. Haberleşmenin Gizliliğini İhlal Suçu (m.132)

5237 sayılı TCK’nın 132. maddesinin 1. fıkrasında, kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi eylemleri suç haline getirilmiştir. Bu eylem sırasında haberleşme içeriğinin kayıt edilmesi eylemi de bu fıkranın ikinci cümlesinde ayrı bir suç tipi olarak düzenlenmiştir. Bu suç haberleşmenin tarafı olmayan kişi tarafından işlenebilir. Maddenin 2. fıkrasında ise kişiler arasındaki haberleşmenin açıklanması eylemi suç haline getirilmiştir. Kişinin kendisi tarafından yapılan haberleşmenin bu haberleşmeyi yapan diğer tarafın izni olmaksızın açıklanması da maddenin 3. fıkrasında suç haline getirilmiştir. Bu haberleşmenin basın ve yayın yoluyla açıklanması da 4. fıkra da ağırlatıcı neden olarak öngörülmüştür.

Madde metninde görüldüğü gibi 5237 sayılı TCK’nın 195. maddesinde düzenlenen posta ve telefon haberleşmesinin gizliliği suçundan farklı olarak bu maddede yalnızca “haberleşme” kavramı kullanılmış ancak bunun nasıl gerçekleştirildiği belirtilmemiştir. O halde her türlü haberleşme bu maddenin koruma kapsamındadır.

Günümüzde gelişen teknoloji sayesinde bilişim sistemleri kullanılarak özellikle de internet aracılığıyla elektronik posta, elektronik sohbet (chat), internet üzerinden telefon görüşmesi ya da tele konferans gibi çeşitli yöntemlerle de haberleşme sağlanmaktadır. İşte bilişim sistemi aracılığıyla gerçekleştirilen bu yeni haberleşme yöntemleri de 5237 sayılı TCK’nın söz konusu maddesinin düzenlemesiyle koruma altına alınmakta ve bu tür haberleşmeyi ihlal edenler de cezalandırılmak istenmektedir. Bu durum maddenin gerekçesinde de açıkça belirtilmiştir. Böylelikle 765 sayılı TCK’nın 195. maddesi açısından “elektronik sohbet ya da elektronik posta” ile yapılan haberleşmenin bu madde kapsamında olup olmadığına ilişkin tartışmalar sona erecek ve veri iletim ağları aracılığıyla yapılan haberleşmeler de bu maddenin koruma kapsamında değerlendirilecektir.

2. Haberleşmenin Engellenmesi Suçu (m.124)

5237 sayılı TCK’nın ikinci kitabının kişilere karşı suçlar başlıklı ikinci kısmının hürriyete karşı suçlar başlıklı yedinci bölümünün 124. maddesinde düzenlenen “haberleşmenin engellenmesi suçunun” bilişim sistemleri aracılığıyla işlenmesi mümkündür. Yukarıda 5237 sayılı TCK’nın 134. maddesine ilişkin açıklamalar yapılırken belirtildiği üzere günümüzde gerçekleştirilen haberleşmenin büyük bir çoğunluğunu elektronik posta ve sohbet oluşturmaktadır. Bu yöntem diğerlerine göre hem daha ucuz hem de çok daha hızlı olması

⁴⁹ İnsanların sürekli olarak izlendikleri ve fişlendikleri ütöpik bir dünyayı ve bu dünyadaki insan davranışları göstermesi açısından bkz: **George Orwell**, Bin Dokuz Yüz Seksen Dört, Çev: Nuran Akgören, İstanbul, Can Yayınları, 1999.

nedeniyle artık daha çok tercih edilir hale gelmiştir. Bunların yanı sıra, veri iletim ağları üzerinden yapılan telefon görüşmeleri ve tele konferanslar da elektronik haberleşmenin diğer çeşitleri olarak görülmektedir.

5237 sayılı TCK'nın inceleme konusu maddesiyle yalnızca haberleşme denildiği, bu haberleşme araçları tek tek sayılmadığı için haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi inceleme konusu suç oluşturacaktır, nitekim bu durum maddenin gerekçesinde de açıkça ifade edilmiştir. Bu nedenle bilişim sistemi aracılığıyla gerçekleştirilen haberleşmenin engellenmesi eylemleri de 5237 sayılı TCK'nın 124. maddesinde düzenlenen suç tipinin koruma kapsamında değerlendirilecektir.

3. Hakaret Suçu (m.125)

5237 sayılı TCK'nın şerefe karşı suçlar başlıklı sekizinci bölümünün 125. maddesinde “hakaret suçu” düzenlenmiştir. Bu düzenleme ile 765 sayılı TCK'nın benimsediği hakaret ve sövme suçu ayrımı kaldırılmıştır.

Söz konusu maddenin 2. fıkrasında eylemin mağdura yönelik sesli, yazılı veya görüntülü bir iletiyle işlenmesi durumunda da hakaret suçunun gerçekleşeceği kabul edilmektedir. Buna göre hakaret suçunun bilişim sistemleri aracılığıyla işlenmesi de cezalandırılacaktır.

Ayrıca maddenin diğer fıkralarında belirtilen ağırlatıcı nedenlerden özellikle hakaret suçunun alenen veya sanal basın ve yayın yoluyla işlenmesinin veri iletim ağlarıyla gerçekleştirilmesi çok sık rastlanılan bir durumdur. 5237 sayılı TCK'nın bu düzenlemesiyle veri iletim ağlarıyla gerçekleştirilen ve alenen olan ya da sanal basınla gerçekleştirilen hakaret suçları ağırlatıcı neden olarak kabul edilmektedir.

4. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu (m.142 fkr.2 b.“e”)

5237 sayılı TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 142. maddesinde hırsızlık suçunun nitelikli halleri düzenlenmektedir. Bu maddenin 2. fıkrasının “e” bendinde ise “bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu” yer almaktadır. Gelişen teknoloji ile birlikte her gün yeni bilişim suçu işlenme şekillerinin ortaya çıkması böyle bir düzenlemenin yapılması gerekliliğini ortaya çıkarmıştır.

765 sayılı TCK'nın 525 b/2 maddesinde düzenlenen hukuka aykırı yarar elde etmek suçuyla düzenlenen eylemlerden birinin de bilişim sistemi aracılığıyla gerçekleştirilen hırsızlık eylemleri olduğu bu suç tipi işlenirken ifade edilmiştir. İşte 5237 sayılı TCK'nın bu maddesiyle “suçla korunan hukuksal değer” gözetilerek bu suç tipi ilgili olduğu bölümde ve ilgili olduğu suç tipinin içinde düzenlenmektedir. Hem de böylelikle 765 sayılı TCK'nın 525 b/2 maddesi açısından getirilen yasa maddesinin çok geniş olduğu eleştirisi karşılanmaya çalışılmaktadır.

Ancak bilişim hırsızlığı olarak adlandırılabilen bu suç tipine 5237 sayılı TCK'nın 144. maddesinde nitelikli hırsızlık hallerinden birisi olarak yer verilmesi yerinde bir düzenleme olmamıştır. Çünkü 143. maddede hırsızlık suçunun basit hali tanımlanmış ve bu tanımda suçun konusu olarak somut nesneler gösterilmiştir. Aynı maddenin ikinci bendinde her ne kadar elektrik enerjisinin de bu suçun konusunu oluşturacağı belirtilmiş de bilişim hırsızlığının konusunu oluşturan veriler ne somut bir nesne ne de elektrik enerjisidir.

Dolayısıyla 144. madde, 143. maddeyle çelişki halindedir. Bu nedenle bu suç tipinin yine mal varlığına karşı suçlar bölümünde ancak bağımsız bir suç tipi olarak düzenlenmesi gerekir.

Bilişim sistemiyle gerçekleştirilen hangi türlü hırsızlık eylemlerinin bu suçu oluşturacağı da bu düzenlemeden anlaşılamamaktadır. Bilişim sisteminin kullanılması yoluyla somut nesnelerin çalınması mı yoksa verilerin çalınması mı bu suç tipiyle düzenlenmek istenmiştir? Bilişim sistemi kullanılarak somut nesne nasıl çalınabilir? Eğer somut nesneler değil veriler kastedilmişse bu kez de suç tipinin düzenlenişi hatalı olmaktadır, çünkü suç tipinin tanımının yapıldığı suçun basit şeklinde suçun konusunu somut nesnelerin oluşturduğu açık bir şekilde ifade edilmektedir. Buna göre kişinin rızası dışında, failin kendisine veya başkasına yarar sağlamak amacıyla hareket edip kişinin eşya üzerindeki egemenliğine bilişim sistemi aracılığıyla son verilmesi eylemiyle bu suç gerçekleşecektir denilebilecektir. Ancak bu, en azından bugün için uygulamasına pek rastlanmayacak bir durum olarak gözükmektedir.

Yine belirtilmesi gerekir ki bu suçun bağımsız bir suç tipi olarak düzenlenmesi ve suçun konusunun neler olduğu ile hangi eylemlerin cezalandırılmak istediğinin açıkça ifade edilmesi ileride doğabilecek uygulama ve yorum hataları ile karışıklıkları önleyecektir.

Ayrıca belirtmelidir ki, bilişim sistemi aracılığıyla gerçekleştirilen hukuka aykırı yarar elde edilmesi eylemleri genellikle bilişim sistemleri üzerinde gerçekleştirilen “manipülasyon eylemleri” ile oluşturulmakta, bu tür hileli hareketler de “dolandırıcılık suçu” kapsamında değerlendirilmektedir. Bu nedenle bugün için, bilişim sistemi aracılığıyla gerçekleştirilen hırsızlık suçunun uygulamasının yukarıda yapılan açıklamalar da dikkate alındığında az sayıda kalacağı görülmektedir. Ancak gelişen teknolojiyle birlikte bu tür eylemlerin işlenme şekillerinin artması olası olduğundan, bu tür bir düzenlemenin 5237 sayılı TCK’da yukarıda eleştirilen doğrultuda ve açıklanan şekilde yer alması yerinde bir düzenleme olacaktır; ancak suç tipinin düzenlenişinin bu hali kesinlikle hatalıdır.

5. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu (m.158 fkr.1 b.“f”)

YTCK’nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 158. maddesinde dolandırıcılık suçunun nitelikli halleri düzenlenmektedir. Bu maddenin 1. fıkrasının “f” bendinde “bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu” yer almaktadır. Yukarıda bilişim sistemlerinin kullanılması yoluyla işlenen hırsızlık suçunun düzenlenme nedenleri ve düzenleme yöntemine ilişkin olarak yapılan açıklamalar bu suç tipi açısından da geçerlidir.

Bu madde ile uygulamada bilişim suçlarının en sık karşılaşılan tiplerinden biri düzenlenmek istenmiş ve bilişim sistemleri üzerinde gerçekleştirilen hileli işlemler sonucu hukuka aykırı yarar sağlanması eylemleri cezalandırılmaya çalışılmıştır.

Ancak yukarıda hırsızlık suçu açısından getirilen eleştiri bu suç tipi açısından da söz konusudur. Dolandırıcılık suçunun basit şeklinin düzenlendiği 5237 sayılı TCK’nın 157. maddesinde hileli bir davranışla bir kimseyi aldatıp” ifadesi kullanılmak suretiyle bu suçun gerçekleşmesi için bir kişinin aldatılmasının gerekli olduğu belirtilmektedir. Bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık eylemlerinde ise aldatma eyleminin bilişim sistemine karşı yapılması gerekir; aksi durumda klasik dolandırıcılık söz konusu olmakta, bilişim sistemi burada yalnızca bir araç olarak görev yapmaktadır. Oysa 158. maddenin 1. fıkrasının “f” bendinde “bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık

suçu”, 157. maddedeki suçun basit şekli esas alınarak düzenlenmektedir. Suçun esas şekline bakıldığında ise bir kişinin aldatılmasının gerekli olduğu belirtilmektedir.

Görüldüğü üzere dolandırıcılık bu nitelikli hali, bilişim sistemlerinin ve bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık eylemlerinin kendine özgü yönleri dikkate alınmadan düzenlenmiştir. Bu durumda kişilerin aldatılmasında bilişim sisteminden yararlanılması dolandırıcılık suçunun nitelikli hali olarak değerlendirilecektir. Dolayısıyla bu düzenleme ile “bilişim sistemleri üzerinde gerçekleştirilen hileli işlemler sonucu hukuka aykırı yarar sağlanması eylemleri” düzenlenmemiş dolandırıcılıkta bilişim sisteminin basit bir araç olarak öngörülmesi düzenlenmiştir.

Yukarıda anılan suç tipi için ise ayrı, bağımsız bir suç tipinin düzenlenmesi gerekmektedir.

6. Müstehcenlik Suçu (m.226)

5237 sayılı TCK’nın topluma karşı suçlar başlıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 226. maddesinde “müstehcenlik suçu” düzenlenmektedir. Madde metninde müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına yönelik düzenlemeler yer almaktadır. Söz konusu zararlı yayınların bilişim sistemleri kullanılarak özellikle veri iletim ağlarıyla yayılması ve paylaşması olanaklı olduğundan bu suç tipi de bilişim sistemleri aracılığıyla işlenebilecektir.

Burada belirtilmesi gerek önemli bir konu da ucu açık, zamana göre değişen ve yorum gerektiren “müstehcen” kavramının yerine “pornografi” kavramının kullanılmasının suç tipini çok daha iyi ve belirlenebilir bir hale getireceğidir⁵⁰. Her ne kadar her iki kavramın sınırları tam belirlenemese de özellikle müstehcen kavramının içeriği ve anlamı, devirden devire değiştiği gibi ülkeden ülkeye ve hatta aynı ülke içinde farklı kültür grupları arasında değişmektedir⁵¹. Bu nedenle yasada söz konusu kavram yerine pornografi kavramına belirginlik ilkesi gereğince yer verilmelidir.

Söz konusu düzenlemede uygulamada karışıklıklara yol açmaması için veri iletim ağlarıyla da bu suçun gerçekleştirilebileceğinin belirtilmesi yerinde bir düzenleme olacaktır.

Bunun yanı sıra çocuk pornografisinin özellikle Avrupa Siber Suç Sözleşmesi’nin ilgili maddeleri örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişi YTCK açısından önemli bir eksiklik oluşturmaktadır.

Maddenin bu düzenlenişi yetersiz olsa da veri iletim ağlarıyla gerçekleştirilen müstehcen yayın eylemlerine uygulanabilecek durumdadır.

Ancak maddenin bu şekilde düzenlenişi de içerisinde çelişkiler barındırmaktadır. Özellikle müstehcen yayınların nasıl ve hangi yöntemle satılacağı, gösterileceği gibi durumlar ayrıntılı olarak düzenlenirken; bu tip ürünleri satanların, ihraç edenlerin, depolayanların ve diğer eylemlere de karışanların cezalandırılacağına ilişkin düzenleme yeterli değildir.

⁵⁰ **Şeref Dede**, “Topluma Karşı Suçlar”, Türk Ceza Kanunu Tasarısı: Türk Ceza Hukuku Derneği Toplantısı (10 Temmuz 2004): İstanbul Barosu-Türk Ceza Hukuku Derneği Toplantısı (10 Eylül 2004): Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul, İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını, 2004, s.63.

⁵¹ **Duygun Yarsuvat**, “Müstehcenliğin Neresindeyiz”, Güncel Hukuk, S:9, İstanbul, Eylül 2004, s.49; **Murat Volkan Dülger**, “Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla yayılmasına Karşı Yapılan Düzenlemeler”, İstanbul Barosu Dergisi, İstanbul, S.4, 2004, s.1490-1493.

Maddenin bu yapısından hangi eylemin, niçin, ne suretle yaptırımla karşılandığı açık bir biçimde anlaşılamamaktadır⁵².

6. Kumar Oynanması İçin Yer ve İmkân Sağlanması Suçu (m.228)

5237 sayılı TCK'nın topluma karşı suçlar başlıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 228. maddesinde “kumar oynanması için yer ve imkân sağlanması suçu” düzenlenmektedir. Suç tipinde sanal alanda bu eylemin gerçekleştirilmesi halinin cezalandırılacağına ilişkin somut bir ifade yoktur. Ancak bu suçla korunan hukuksal değer bireylerin kumar oynamanın kötülüklerinden korunması olduğu ve yasal tanımda sınırlama yapılmaksızın “yer ve imkân sağlanması” ifadesi kullanıldığı için sanal alanda kumar oynatılması da bu suç tipi içinde değerlendirilerek failer cezalandırılmalıdır.

Bugün gelişen teknoloji ile birlikte bir mekân içinde kumar oynatılmasından çok internet aracılığıyla bunun yapılması daha yaygın olarak görülmektedir. Failler açısından da hem yer ve imkân yaratılması hem de yakalanma riski açısından somut bir yerde eylemin gerçekleştirilmesi daha güçtür. Bunun yanında hem yer sağlama, hem yakalanma riskinin daha az olması hem de çok daha fazla sayıda kişiye ulaşma olanağının bulunması nedeniyle sanal alanda kumar oynatılması bu suç tipinin gerçekleştirilmesi açısından daha elverişlidir. Bu nedenle yasa koyucunun suç tipini serbest hareketli olarak düzenlerken bunu da düşünmüş olduğu kabul edilmelidir.

Ancak yine de sanal alanda kumar oynatılmasının madde metninde ayrıca belirtilmesi ve bunun suçun nitelikli hali olarak düzenlenmesi çok daha iyi bir düzenleme olur düşüncesindeyiz.

III. Bilişim Suçlarıyla İlgili Eleştiri ve Görüşler

Öncelikle belirtilmelidir ki, bilişim suçları olarak değerlendirilen suç tipleri, 5237 sayılı TCK'da suçla korunan hukuksal değer göz önüne alınarak ilgili oldukları bölümlerde korudukları hukuksal değere göre düzenlenmektedir. Koruduğu hukuksal değer karma nitelik gösteren suç tiplerine ise bilişim sistemi ortak alınarak ayrı bir bölümde yer verilmektedir. Ancak banka veya kredi kartlarının kötüye kullanılması suçu koruduğu hukuksal değere göre malvarlığına karşı suçlar bölümünde yer alması gerekirken bu yapılmayarak bilişim sistemlerine karşı suçlar bölümünde düzenlenmiştir. Bu durumun düzeltilmesi ve suç tipine ilgili olduğu bölümde yer verilmesi gerekmektedir.

765 sayılı TCK'nın 525 a/1 maddesinde, verilerin ele geçirilmesi eylemi suç olarak düzenlenmiş, ancak bir bilişim sistemine yetkisiz girilerek içindeki bilgilerin ele geçirilmeden öğrenilmesi suç olarak düzenlenmemiştir. Olumlu bir eleştiri olarak söylenmelidir ki tasarının 245. maddesinde bu durum giderilmiştir. “Hacker” terimiyle tanımlanan bilişim korsanlarının eylemleri böylelikle düzenleme altına alınmıştır.

Hem 765 sayılı TCK'da ve hem de TBMM'ye sunulan hükümet tasarısında “verilerde sahtekârlık yapılması suçu” düzenleme altına alınmıştır. Ancak meclis alt komisyonunda değiştirilerek kabul edilen tasarı metninde bu suç tipine yer verilmemiştir; neticede yasa haline gelen 5237 sayılı TCK'da da bu suç tipi yer almamıştır. Suç politikası açısından bilişim sistemi aracılığıyla bu tür belgeler düzenlenip kullanılabileceği ve böylelikle kamunun güveni

⁵² Mehmet Emin Artuk/Alı Rıza Çınar, “Yeni Bir Ceza Kanunu Arayışları ve Adalet Alt Komisyonu Tasarısı Üzerine Düşünceler”, Türk Ceza Kanunu Reformu: İkinci Kitap: Makaleler, Görüşler, Raporlar, Der: Teoman ergül, Ankara, Türkiye Barolar Birliği Yayını, 2004, s.81.

ihlal edilebileceği için bu suç tipi 5237 sayılı TCK'da düzenlenmeli ve bu suç tipine kamunun güvenine karşı suçlar bölümünde yer verilmelidir. Bu suç tipi, yukarıda belirtilen ilgili bölümde ya bağımsız olarak düzenlenmeli ya da resmi ve özel belgede sahtecilik suçlarının içinde ayrı ayrı düzenlenmelidir.

Bilişim sistemlerinin organize suçlarda ve sanal terörizmde kullanılması durumları acilen düzenlenmeli ve bu konu açısından ilgili yasalarda düzenlemeler yapılmalıdır. Bunların yanı sıra ırkçılık, şiddete çağrı, halkı kin ve düşmanlığa tahrik, suça teşvik ve terör örgütlerinin propagandasının bilişim sistemleri aracılığıyla sanal alanda yapılması eylemleri hakkında da düzenlemeler yapılmalıdır⁵³.

Sanal terörizm olgusu dikkate alınarak, veri iletim ağlarından yararlanılmak yoluyla terör eylemleri gerçekleştirilmesi ağırlatıcı neden sayılmalıdır. Çünkü terör eylemi gerçekleştiren eylemciler, klasik suç tiplerinde kendi yaşamlarını dahi tehlikeye atmaktayken, eylemlerin bilişim sistemleriyle gerçekleştirilmesi hem aldıkları riski hem de tespit edilip yakalanma riskini azaltmakta ve suçun işlenişini kolaylaştırmaktadır.

Aynı şekilde organize suç örgütlerinin üyeleriyle haberleşmesi, finansal kaynaklarını kullanması ve aktarması eylemleri de ayrıca düzenlenmelidir ve ağırlatıcı neden sayılmalıdır; yukarıda bu konuda yapılan açıklamalar burası için de geçerlidir. Bu konuda 5237 sayılı TCK'da herhangi bir düzenlemenin olmaması önemli bir eksiklik olarak görülmektedir.

Veri iletim ağları üzerinden gerçekleştirilen kumar oynatma eylemi mutlaka ayrı bir fıkra ve 228. maddenin nitelikli hali olarak cezayı ağırlatan hal şeklinde düzenlenmelidir. Bu konuda büyük bir yasal boşluk bulunmaktadır. 5237 sayılı TCK'da bu yönde özel bir düzenleme yoktur. Oysa herkesin ulaşamadığı somut kumarhaneler dahi ülkemizde yasaklanmışken, dileyen herkes bugün sanal kumarhanelerde kumar oynayabilmektedir. Her ne kadar 5237 sayılı TCK'nın 228. maddesinde "kumar oynanması için yer ve imkân sağlanması" denilerek geniş bir ifade kullanılıyorsa da yorum sorunlarının yaşanmaması ve uygulamada karışıklığa neden verilmemesi için "sanal alanda bilişim sistemleriyle kumar oynatılmasının" da madde metninde belirtilmesi uygun bir düzenleme olacaktır.

Başta Amerika Birleşik Devletleri'nde ve Avustralya'da olmak üzere, istenmeyen elektronik postaların (spam) gönderilmesi eylemleri suç olarak düzenlenmektedir. Bu gerçek anlamda rahatsız edici ve veri iletim ağlarındaki trafiğin yoğunluğu arttıran ve kuruluşlar ile kişilerin elektronik postalarındaki çok geniş alanları kaplayan dolayısıyla uluslararası ticareti güçleştiren bir durumdur. 5237 sayılı TCK'da bu eylemin de suç tipi olarak düzenlenmesi gerekmektedir.

Özellikle istenmeyen elektronik iletilere ilişkin diğer ülkelerde yapılan düzenlemeler dikkate alınarak bu soruna çözüm getirilmeli ve istenmeyen elektronik ileti gönderilmesi suç haline getirilmelidir. Bu bağlamda Avrupa Sınır Ötesi Yayın Sözleşmesi'nin düzenlemesiyle uyum sağlanarak, sanal alanda aldatıcı, yanıltıcı, istismar edici, mal ve can güvenliğini tehlikeye atıcı reklâmlara karşı düzenlemeler getirilmeli⁵⁴ özellikle kasten can ve mal güvenliğini tehlikeye atıcı reklâmların üretilmesi ve internet üzerinden yayınlaması suç haline getirilmelidir⁵⁵.

⁵³Ünver, Ceza Kanununun Değerlendirilmesi, s.106,107.

⁵⁴Geniş açıklama için bkz: **Emrehan İnal**, Reklam Hukuku ve Aldatıcı Reklamlar, İstanbul, Beta Yayıncılık, 2000, s.102-119.

⁵⁵Ünver, Ceza Kanununun Değerlendirilmesi, s.135, 136.

Bugün için adam öldürme suçu gibi klasik suç tiplerinin dahi birçoğu bilişim sistemi aracılığıyla veri iletim ağları üzerinden gerçekleştirilebilmektedir (örneğin hastanenin bilişim ağına girilerek sisteme bağlı yaşam destek ünitesinin durdurulmasıyla hastanın öldürülmesi gibi). Bu eylemlerde bilişim sistemlerinin ve veri iletim ağlarının kullanılması hem suçun hem failin tespitini zorlaştırmakta buna karşın fail açısından suçun işlenmesini son derece kolaylaştırdığı gibi, aldığı riskleri ve yakalanma ihtimalini azaltmaktadır. Bu nedenle bilişim sistemleriyle gerçekleştirilmesi olanaklı olan suç tipleri açısından bu sistemlerin kullanılması, ilgili suç tipleri açısından ağırlatıcı neden olarak öngörülmelidir.

Sanal alanda yer alan kişilerin cezai sorumluluklarına ilişkin olarak mutlaka düzenleme yapılmalıdır. Bugün için ülkemizde bu konuda tam anlamıyla yasal bir boşluk bulunmakta suç ve failer ortaya çıkarılsa dahi yasal boşluk nedeniyle bu kişilere ceza verilememektedir. Bu düzenlemeler Alman Teleservisler Yasası'nda olduğu gibi ayrı bir yasal düzenlemede olabileceği gibi, konuyla ilgili yasalarda da düzenleme yapılabilecektir; öğretide de bu konuda farklı görüşler bulunmaktadır⁵⁶. Ancak bu düzenlemeler yapılırken düşünce özgürlüğüne ilişkin evrensel ilkeler göz önünde bulundurulmalı, özellikle AİHS'nin 10. maddesinde yer alan "ifade özgürlüğü hakkı" ve aynı maddenin 2. fıkrasında yer alan bu hakkın sınırlanabildiği haller çerçevesinde düzenleme yapılmalıdır⁵⁷. Sanal alanda yer alan kişilerin cezai sorumluluklarının belirlenmesi düşünce özgürlüğüne ket vurulması anlamını taşımamalıdır⁵⁸.

Yukarıda belirtildiği üzere ülkemizde yürürlükteki mevzuatta kişilerin internetteki eylemlerinden kaynaklanan ceza sorumluluğunu belirten bir düzenleme bulunmamaktadır⁵⁹. Bu nedenle ayrı bir yasada internet kişileri olan internet servis sağlayıcıların, erişim sağlayıcıların ve içerik sağlayıcıların ceza hukuku açısından sorumlulukları ayrı ayrı düzenlenmelidir⁶⁰. Ancak özellikle içerik sağlayıcılar, basın kuruluşları ya da sanal gazetecilik alanında faaliyet gösteren kuruluşlar olabileceği için bunların sorumlulukları bireylerin haber alma hakkı engellenmeyecek şekilde düzenleme yoluna gidilmelidir.

Ayrıca burada belirtilmelidir ki, 15.07.1950 tarihli ve 5680 sayılı eski Bas. K.ya, 15.05.2002 tarihinde 4756 yasanın 26. maddesiyle getirilen Ek 9. maddeyle, internette yayın yapanlar için söz konusu yasanın düzenlemelerinin yalan haber, hakaret ve benzeri eylemler açısından ortaya çıkacak maddi ve manevi zararlarla ilgili uygulanmasını içeren düzenleme sanal alanın ve internetin doğal yapısıyla uyumlu değildi. Ayrıca sanal alanda yapılan yayınlı basılı yayın arasında her açıdan büyük farklılıklar var olduğu için yasa uygun bir düzenleme olmamıştı. Bugün için tekelleşmeye doğru giden ve neredeyse tek sesli olan yazılı basın karşısında internet aracılığıyla gerçekleştirilen sanal basının özgürlüğünü ve çok sesliliğini korumak gerekirken söz konusu yasa maddesiyle bu engellenir bir duruma getirilmekteydi⁶¹.

⁵⁶Kayihan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul, C.LIX, S.1-2, s.10; Ünver, Ceza Kanununun Değerlendirilmesi, s.81, 82.

⁵⁷AİHS'nin bu maddesi ve sınırlanabildiği haller için bkz: Mehmet Şükrü Alpaslan, "Avrupa İnsan Hakları Sözleşmesi Uygulamasında Düşünce ve Basın Özgürlüğü", Prof. Dr. Sahir Erman'a Armağan, İstanbul, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, 1999, s.27-31; Murat Volkan Dülger, "Avrupa İnsan Hakları Sözleşmesi'nde Düşünce Özgürlüğü", Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s.283-298.

⁵⁸Ünver, Ceza Kanununun Değerlendirilmesi, s.82.

⁵⁹Selman Dursun, "İnternette Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", MHB Prof. Dr. Gülören Tekinalp'a Armağan, Y.23, S.1-2, 2003, s.285.

⁶⁰Hasan Sınar, "İnternet'in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", MHB Prof. Dr. Yılmaz Altuğ'a Armağan, Y: 17-18, S:1-2, 1997-1998, s.365-370; Cevat Özel/M. Gökhan Ahi, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", Güncel Hukuk, S:6, İstanbul, Haziran 2004, s.21.

⁶¹"Basın, sadece siyasi konuları özel bir vurguyla işlemesi yönünden değil, ayrıca bu konuları bir dinleyici kitleye sunması ve bu yolla, demokratik toplumun ideali olan geniş çaplı bir kamusal tartışmaya önayak olması bakımından da diğer haberleşme türlerinden ayrılır. Bundan başka, kamunun görüşü iktidarın gücü önünde bir engel görevi üstlendiğine göre, kamuyu ilgilendiren ve harekete geçiren bir aracı (medium), büyük bir öneme sahip demektir."Frederick Schauer, İfade Özgürlüğü:

Yasanın bu maddesi, hem söz konusu yayınların verdiği zararlardan korunmak açısından hem de failin belirlenmesi açısından amacı karşılamaya uygun değildi ve kaldırılması gerektiği defalarca belirtilmişti. İşte bu yoğun eleştirileri dikkate alan yasa koyucu 09.06.2004 tarihli ve 5187 sayılı yeni Basın Kanunu ile internete ilişkin bu düzenlemelere yerinde olarak hiç yer vermemiş ve internet yayıncılığı ile basılı yayıncılık arasındaki önemli farkı göz önünde tutmuştur.

İnternet kişilerinin hukuksal sorumlulukları düzenlenirken veri iletim ağlarıyla sanal basın olarak hareket eden sitelerle kişilerin oluşturduğu ve sanal yayın yapma amacı gütmeyen siteler arasında ayırım yapılmalıdır. Örneğin bir forum odasını yöneten site sahibinin bu siteye gelen yazıları denetlemek ve hepsini okumak gibi bir görevi yoktur, böyle bir görev yasayla da yaratılmamalıdır; bu nedenle site sahibi siteye gönderilen yazıların suç içermesi halinde söz konusu yazılardan dolayı sorumlu tutulmamalıdır. Bu ayırım gözetilerek bir düzenleme yapılmalıdır.

Bilişim suçlarıyla mücadelede maddi ceza hukukunun ve ceza muhakemesi hukukunun birlikte ele alınmasıyla bir sonuç elde edilmesi mümkündür. Bilişim suçlarının özelliği dolayısıyla uluslararası nitelikte olması, suçun işlendiği yer bakımından sorunların çıkmasına bu da suçun kovuşturmasının nerede yapılacağı sorununa yol açmaktadır. Bu sorunların aşılması ancak uluslararası işbirliğine işlerlik kazandırılmasıyla mümkün olacaktır. Avrupa Siber Suç Sözleşmesi'nde bu konuda ayrıntılı düzenlemeler bulunmaktadır. Bu sözleşmeye ülkemiz tarafından da taraf olunması ve 5237 sayılı TCK'nın suçun işlendiği yer konusuna ilişkin maddelerinde bu sözleşmeye paralel gerekli düzenlemelerin yapılmasıyla bu sorunun aşılması mümkün olabilecektir⁶².

Bilişim sistemleri kullanılarak veri iletim ağları üzerinden kişilik haklarına saldırıda bulunulması durumunda özellikle internet aracılığıyla hakaret etme ve sövme cürümleri akla gelmektedir⁶³. Bu eylemlerin internet aracılığıyla yapılması çok kısa zamanda çok fazla sayıda kişinin bilgisine ulaşmasını sağlamaktadır, ayrıca özellikle haber siteleri ya da forum alanlarında bu eylemlerin gerçekleştirilmesi halinde bu eylemin sonuçlarını giderici önlemler Basın Kanunu'nda basılı eserlerde olduğu gibi internet açısından bulunmamaktadır. Bu nedenlerle hem bu alana ilişkin önlemler düzenlenmeli hem de sanal alanda, özellikle de internette hakaret, sövme, tehdit ve haberleşme özgürlüğünün ihlali gibi suçların işlenmesinde bu alanının kullanılması ağırlatıcı bir neden olarak kabul edilmeli ve bu düzenlemeler ile mevcut bilişim suçları arasında ortaya çıkabilecek suçların içtimai sorunları açık düzenlemelerle çözülmelidir⁶⁴.

Bilişim suçlarıyla ilgili olarak yapılması gereken önemli bir düzenleme de çocukların sanal alanda ticari amaçla cinsel istismarının bağımsız bir suç tipi haline getirilmesidir⁶⁵. Çocukların anne-babaları, veli-vasi gibi kişilerce zorlanarak pornografik resim, film gibi materyallere konu edilmesi ve bunların internet üzerinden pazarlanması ve alınması suç tipi haline getirilmelidir⁶⁶. Ayrıca her türlü çocuk pornografisi içeren materyalin bilişim

Felsefi Bir İnceleme, Çev: M. Bahattin Seçilmişoğlu, Ankara, Liberal Düşünce Topluluğu Yayını, 2002, s.152. Yukarıdaki açıklamalar ışığında bu görüş özellikle bugün için sanal basın açısından daha da geçerli olmaktadır.

⁶² Aynı görüşte bkz: **Hasan Sınar**, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s.785; **Özel/Ahi**, a.g.y., s.22.

⁶³ **Erol Karaoğlu**, "İnternet Ortamından Gerçekleştirilebilecek Bir İhlal Türü Olarak Asılsız İsnat", (Çevrimiçi) <http://www.bilisimhukuku.net/index.php?option=content&task=view&id=337&Itemid=40> 20.04.2004.

⁶⁴ **Karaoğlu**, a.g.y., s.87.

⁶⁵ **Ünver**, Ceza Kanununun Değerlendirilmesi, s.99.

⁶⁶ **Ünver**, Ceza Kanununun Değerlendirilmesi, s.101.

sistemlerinde bulundurulması, bunların paylaşıma açılması, iletilmesi ve kullanılması suç tipi olarak düzenlenmelidir.

Özellikle internet üzerinden gerçekleştirilen “çocuk pornografisine ilişkin her türlü eylem” suç haline getirilmelidir. Bu eylemlerin neler olduğu Avrupa Siber Suç Sözleşmesinde tek tek gösterilmiştir. Bu eylemlerin suç haline getirilmesinin çok acil şekilde yapılması gerekmesine rağmen YTCK’da buna ilişkin düzenleme olan 226. madde bu açıdan son derece yetersizdir.

Son olarak belirtilmelidir ki; yapılacak tüm düzenlemeler pozitif ve yapıcı bir yaklaşımla; özgürlük esas, kısıtlama istisna olacak şekilde yapılmalı; hukuk devleti ilkesi, suç ve cezada yasallık prensibi ve Anayasamızda belirtilen temel hak ve özgürlüklerin özü ilkesiyle, AİHS’de ve AİHM kararlarında belirtilen demokratik toplumda gereklilik kıstasından ödün verilmemelidir.

KAYNAKÇA

- Alpaslan**, Mehmet Şükrü, “Avrupa İnsan Hakları Sözleşmesi Uygulamasında Düşünce ve Basın Özgürlüğü”, Prof. Dr. Sahir Erman’a Armağan, İstanbul, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, 1999, s.27-35.
- Akbulut**, Berrin, “Türk Ceza Hukukunda Bilişim Suçları”, Yayınlanmamış Doktora Tezi (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı), Konya, 1999.
- Artuk**, Mehmet Emin/Alı Rıza Çınar, “Yeni Bir Ceza Kanunu Arayışları ve Adalet Alt Komisyonu Tasarısı Üzerine Düşünceler”, Türk Ceza Kanunu Reformu: İkinci Kitap: Makaleler, Görüşler, Raporlar, Der: Teoman ergül, Ankara, Türkiye Barolar Birliği Yayını, 2004, s.37-84.
- Başalp**, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, 2004.
- Başalp**, Nilgün, “Kişisel Verilerin Korunması ve İnternet”, İnternet ve Hukuk, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.5-36.
- Cerrah**, İbrahim, “Bilişim Teknolojileri ve Etik: Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının ‘Etik Boyutu’ ve ‘Sosyal Sonuçları’”, Polis Bilimleri Dergisi, Ankara, C:4, S:1-2, Ocak-Haziran 2002, s.137-155.
- Dede**, Şeref, “Topluma Karşı Suçlar”, Türk Ceza Kanunu Tasarısı: Türk Ceza Hukuku Derneği Toplantısı (10 Temmuz 2004): İstanbul Barosu-Türk Ceza Hukuku Derneği Toplantısı (10 Eylül 2004): Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul, İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını, 2004, s.59-68.
- Değirmenci**, Olgun, “Bilişim Suçları”, Yayınlanmamış Yüksek Lisans Tezi (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı), İstanbul, 2002.
- Dursun**, Selman, “İnternette Kaynaklanan Ceza Sorumluluğundaki Gelişmeler”, MHB Prof. Dr. Gülören Tekinalp’a Armağan, Y.23, S.1-2, 2003, s.256-290.
- Dülger**, Murat Volkan, “Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu”, Güncel Hukuk Dergisi, İstanbul, S:23, Kasım 2005, s.28-30.
- Dülger**, Murat Volkan, “Yeni Türk Ceza Kanunu’nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler”, 2. Polis Bilişim Sempozyumu, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s.201-207.
- Dülger**, Murat Volkan, “Bilişim Suçları ve Yeni Türk Ceza Kanunu”, Kazancı Hukuk, İşletme ve Maliye Bilimleri Dergisi, S.5, Ocak 2005, s.114-120.
- Dülger**, Murat Volkan, Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2004.

- Dülger**, Murat Volkan, “Avrupa İnsan Hakları Sözleşmesi’nde Düşünce Özgürlüğü”, Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s.283-298.
- Dülger**, Murat Volkan, “Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla yayılmasına Karşı Yapılan Düzenlemeler”, İstanbul Barosu Dergisi, İstanbul, S.4, 2004, s.1485-1496.
- Dülger**, Murat Volkan, “Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi”, Türk Ceza Kanunu Tasarısı: Türk Ceza Hukuku Derneği Toplantısı (10 Temmuz 2004): İstanbul Barosu-Türk Ceza Hukuku Derneği Toplantısı (10 Eylül 2004): Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul, İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını, 2004, s.109-113.
- Ippolito**, Carlo Sarzana di S., “Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalya’daki Durum” Çev: Vesile Sonay Daragenli, İÜHFM Prof. Dr. Türkan Rado’ya Armağan Sayısı, İstanbul, C:LV, S:3, 1997, s.389-405.
- İçel**, Kayıhan, “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul, C.LIX, S.1-2, s.3-10.
- İlkiz**, Fikret, “İkinci Bilişim Şurası 2004”, Güncel Hukuk, S:6, İstanbul, Haziran 2004, s.13, 14.
- İnal**, Emrehan, Reklam Hukuku ve Aldatıcı Reklamlar, İstanbul, Beta Yayıncılık, 2000.
- Karagülmez**, Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara, Seçkin Yayıncılık, 2005.
- Karaoğlu**, Erol, “İnternet Ortamından Gerçekleştirilebilecek Bir İhlal Türü Olarak Asılsız İsnat”, (Çevrimiçi) <http://www.bilisimhukuku.net/index.php?option=content&task=view&id=337&Itemid=40> 20.04.2004.
- Kurt**, Levent, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, 2005.
- Meran**, Necati, Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara, Seçkin Yayıncılık, 2005.
- Orwell**, George, Bin Dokuz Yüz Seksen Dört, Çev: Nuran Akgören, İstanbul, Can Yayınları, 1999.
- Özel**, Cevat/M. Gökhan Ahi, “Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler”, Güncel Hukuk, S:6, İstanbul, Haziran 2004, s.21.
- Özel**, Cevat, “Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı”, İstanbul Barosu Dergisi, İstanbul, C.LXXV, S.7-8-9, Eylül 2001, s.858-872.
- Özel**, Sibel, Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması, Ankara, Seçkin Yayıncılık, 2004.

- Schauer**, Frederick, İfade Özgürlüğü: Felsefi Bir İnceleme, Çev: M. Bahattin Seçilmişoğlu, Ankara, Liberal Düşünce Topluluğu Yayını, 2002.
- Schjolberg**, Stein, “The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries” (Çevrimiçi) <http://www.mosstingrett.no/info/legal.html#37>, 08.02.2004.
- Sınar**, Hasan, “Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme”, Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s.765-800.
- Sınar**, Hasan, “İnternet’in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, MHB Prof. Dr. Yılmaz Altuğ’a Armağan, Y: 17-18, S:1-2, 1997-1998, s.355-372.
- Ünver**, Yener, “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.LIX, S.1-2, İstanbul 2001, s.51-153.
- Ünver**, Yener, “Federal Almanya’da Terör ve Organize Suçluluk ile İlgili Düzenlemeler”, Prof. Dr. Nurullah Kunter’e Armağan, İstanbul, İÜHF Eğitim Öğretim ve Yardımlaşma Vakfı Yayını, 1998, s.385-464.
- Yarsuvat**, Duygun, “Müstehcenliğin Neresindeyiz”, Güncel Hukuk, S:9, İstanbul, Eylül 2004, s.49.
- Yazıcıoğlu**, Yılmaz, “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Y:1, S:1, Ocak-Mart 2004, s.172-185.