

YENİ TÜRK CEZA KANUNU'NDA DÜZENLENEN BİLİŞİM SUÇLARI VE BU SUÇLARLA MÜCADELEDE ALINMASI GEREKEN ÖNLEMLER

Murat Volkan Dülger*

Bu tebliğin konusunu 5237 sayılı YTCK'da bilişim suçlarına ilişkin olarak yapılan düzenlemeler ve bu suç tipleriyle mücadelede alınması gereken önlemler oluşturmaktadır. Aslında bilişim suçları ve bunlarla mücadele yöntemleri çok geniş bir incelemeyi ve öncesinde bu konuyla ilgili çeşitli kavram ve tanım sorunlarının belirtilmesini ve bunların açıklanmasını gerektiren geniş bir konudur. Ancak bu çalışmanın bir tebliğ olması dolayısıyla, öğretilerde bu konuyla ilgili olarak yer alan tartışmalara ve ilgili suç tiplerinin ayrıntılı olarak açıklanmasına yer verilmeden, konu hakkında kısa bir bilgi edinilmesi amacıyla açıklamalar yapılacak ve böylelikle, çalışmanın geniş kapsamlı ve ayrıntılı olmasından olabildiğince kaçınılacaktır.

I. YTCK'da DÜZENLENEN BİLİŞİM SUÇLARI

A. TCK ile YTCK'da Düzenlenen Bilişim Suçlarının Karşılaştırılması

Bilişim suçları, YTCK'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. 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 veya 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” (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.114).

Bunların yanı sıra YTCK'da bilişim sistemleri aracılığıyla işlenebilecek ancak yalnızca bilişim suçu olarak nitelendirilemeyecek suç tipleri de bulunmaktadır. Bunlara örnek olarak aşağıdaki suç tipleri verilebilir (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.114).

* Avukat; İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilimdalı doktora öğrencisi.

“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 imkan sağlanması suçu”.

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

TCK m.525 a/1	YTCK m.135, m.136
TCK m.525 b/1	YTCK m.244/1-2
TCK m.525 b/2	YTCK m.244/4, 245, 158 fkr.1 b.‘f’, m.142 fkr.2 b. ‘e’.

B. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tipleri

1. Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243)

Bilişim alanında suçlar bölümünde ilk olarak 243. maddede “hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu” düzenlenmiştir. YTCK’da bu maddeye yer vermekle yasa koyucu “bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme” eylemini suç tipi haline getirmiştir (Dülger, Bilişim Suçları 2004, s.212). Bu suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. maddesinde öngörülen “hukuka aykırı erişim” düzenlemesine paralellik sağlanmaktadır(Yazıcıoğlu 2004, s.177; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115). Bu düzenlemeyle, YTCK’da veriler ele geçirilmeksizin verilere yetkisiz erişim eylemleri suç tipi haline getirilmiştir (Dülger, Bilişim Suçları 2004, s.213; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115). YTCK’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 yani bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmektedir (Akbulut 1999, s.78; Değirmenci 2002, s.153; Yazıcıoğlu 2004, s.177; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115). Bu özellikle bilişim korsanlarına karşı etkili olabilecek, son derece yerinde ve çağdaş bir düzenlemedir (Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.111; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115).

2. Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2)

YTCK'nın 244.maddesinin 1. ve 2. fıkralarında bilişim sistemine ve verilere her ne yöntemle olursa olsun zarar verme eylemleri suç tipi olarak düzenlenmiştir. 244. maddenin 1. fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması" eylemleri 2. fıkrasında ise "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" eylemleri suç tipi haline getirilmiştir(Dülger, Bilişim Suçları 2004, s.230; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115). Bu suç tipine YTCK'da yer verilmekle, Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen "verileri etkileme" ve 5. maddesinde öngörülen "sisteme etki" düzenlemelerine paralellik sağlanmaya çalışılmaktadır(Dülger, Bilişim Suçları 2004, s.212; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115; Yazıcıoğlu 2004, s.179). Bu suç tipi YTCK'da, TCK'nın 525 b/1 maddesinde düzenlenen "verilere veya veri işleme zarar vermek suçunun" yerine geçmek üzere düzenlenmiştir. Söz konusu suç tipi 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. 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 tutulmaktadır (Dülger, Bilişim Suçları 2004, s.230,231; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.115. Karşı görüşte bkz: Yazıcıoğlu 2004, s.179; Özel 2001, s.860,865; Değirmenci 2002, s.154).

3. Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4)

YTCK'nın 244. maddesinin 4. fıkrasında "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu" düzenlenmiştir. Bu suç tipi 244. maddenin 1. ve 2. fıkralarına atıf yapılarak düzenlenmiştir, her iki fıkra birlikte okunduğunda 244. maddenin 4. fıkrasında yer alan suç tipi "bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemin içerdiği 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" şeklinde olmaktadır. 5237 sayılı YTCK'da, 765 sayılı TCK'nın 525 b/2 maddesinde düzenlenen 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 haline getirilmiştir. Bu suç tipiyle de söz konusu eylemlerden "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama" eylemleri düzenlenmiştir(Dülger, Bilişim Suçları 2004, s.244; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.116). Yine 244. maddenin 4. fıkrasında bu suç tipi açısından, "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 oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir” (Dülger, Bilişim Suçları 2004, s.244; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.116).

4. Banka veya kredi kartlarının kötüye kullanılması suçu (m.245)

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 (Dülger, Bilişim Suçları 2004, s.250; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.116). Söz konusu eylemler hem öğretide hem de uygulamada TCK’nin 525 b/2 maddesinde yer alan “bilişim sistemi aracılığıyla hukuka aykırı yarar elde etme suçunun” kapsamı içinde değerlendirilmiştir; ancak 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 istenmiş (Dülger, Bilişim Suçları 2004, s.250; Yazıcıoğlu 2004, s.182) ve kredi veya banka kartıyla gerçekleştirilen her türlü hukuka aykırı yarar sağlama eylemlerinin bu suç tipini oluşturacağı maddenin gerekçesinde de belirtilmiştir (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.116,117).

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

1. Kişisel verilerin kaydedilmesi suçu (m.135)

YTCK’nın 135. maddesinin 1. fıkrasıyla, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi, aynı 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 düzenlenmiştir (Özel 2001, s.865; Değirmenci 2002, s.156,157; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117). Gelişen bilişim teknolojisiyle birlikte ülkemizde ve dünyada çok sık karşılaşılan ve aynı zamanda kişilik haklarına bir saldırı niteliği de taşıyan eylem türü, kişilerin rızaları olmaksızın kişisel verilerinin bilişim sistemlerine yerleştirilmesidir (Dülger, Bilişim Suçları 2004, s.267; (Dülger, Bilişim Suçları ve Yeni Türk Ceza

Kanunu 2005, s.117). Özellikle hastanelerin hastalarıyla ilgili, finans kurumlarının ve sigorta şirketlerinin müşterilerinin kredi olanağı ve ödeme gücüyle ilgili, ticari şirketlerin ise reklam ve pazarlama amacıyla bu tür verileri toplayıp kullandığı bilinmektedir. Bu tür bilgilerin sanal ortama veri olarak aktarılması ve bu yapılırken bu verilerin ilgisinin izninin alınmaması inceleme konusu maddeyle suç tipi haline getirilmiştir (Dülger, Bilişim Suçları 2004, s.267; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117). Böylelikle 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 (Dülger, Bilişim Suçları 2004, s.267; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117).

2. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m.136)

YTCK'nın 136. maddesiyle ise, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri bağımsız bir suç tipi olarak düzenlenmektedir. Bu düzenleme özellikle ABD ve İngiltere gibi ülkelerde çok sık karşılaşılan ve en fazla sayıda işlenen bilişim suçu olduğu ifade edilen kimlik hırsızlığı eylemlerine karşı, bu tür eylemlerin yaptırımsız kalmaması amacıyla düzenlenmiştir. Günümüzde hemen tüm kişisel bilgiler ve kimlik bilgileri özellikle internette bulunmaktadır; 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 (Dülger, Bilişim Suçları 2004, s.276; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117).

3. Verilerin yok edilmemesi suçu (m.138)

YTCK'nın 138. maddesiyle de, yasal süresi dolmasına rağmen kişisel verileri sistem içinden yok etmekle görevli olan kişilerin bu görevlerini yerine getirmemeleri durumu suç haline getirilmektedir (Özel 2001, s.865; Değirmenci 2002, s.157; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117). YTCK'da yer verilen bu suç tipiyle 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. 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. Söz konusu bu suç tipiyle bunun önüne geçilmek istenmektedir (Dülger, Bilişim Suçları 2004, s.281). Bu suç tipi ilk kez 5237 sayılı YTCK ile düzenlenmektedir (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.117,118).

D. Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri

Yukarıda açıklanan suç tipleri dışında, YTCK'da farklı bölümlerde düzenlenen ve bilişim sistemleri aracılığıyla işlenebilecek başka suç tipleri de bulunmaktadır. Bu suç tipleri şunlardır: YTCK'nın 124. maddesinde düzenlenen "haberleşmenin engellenmesi suçu", 125. maddesinde yer alan "hakaret suçu", 132. maddesinde düzenlenen "haberleşmenin gizliliğini ihlal suçu", 142. maddesinin 2. fıkrasının 'e' bendinde yer alan "nitelikli hırsızlık suçu", 158. maddenin 1. fıkrasının 'f' bendinde yer alan "nitelikli dolandırıcılık suçu", 226. maddesinde düzenlenen "müstehcenlik suçu" ve 228. maddesinde düzenlenen "kumar oynanması için yer ve imkan sağlanması suçu" (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.118).

E. YTCK'da Bilişim Suçlarıyla İlgili Olarak Getirilen Eleştiriler

Bilişim suçları olarak değerlendirilen ve yukarıda kısaca belirtilen suç tipleri, YTCK'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 (Dülger, Bilişim Suçları 2004, s.332; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.109; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.118).

765 sayılı TCK'nın 525 a/1 maddesinde, verilerin ele geçirilmesi eylemi suç olarak düzenlenirken aslında daha sık karşılaşılan bir eylem türü olan bilişim sistemine yetkisiz girilerek içindeki bilgilerin ele geçirilmeden öğrenilmesi suç tipi olarak düzenlenmemiştir. Olumlu bir eleştiri olarak söylenmelidir ki YTCK'nın 243. maddesinde bu eksiklik giderilmiş ve böylelikle "hacker" terimiyle tanımlanan bilişim korsanlarının eylemleri karşı ceza hukuku aracılığıyla bir önlem alınmaya çalışılmıştır (Dülger, Bilişim Suçları 2004, s.332; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.118).

Burada değinilmesi gereken önemli bir eksiklik, hem 765 sayılı TCK'da ve hem de TBMM'ye sunulan hükümet tasarısında düzenlenen "verilerde sahtekarlık yapılması suçu" ile ilgilidir. Bu suç tipine meclis alt komisyonunda değiştirilerek kabul edilen tasarı metninde yer verilmemiştir; neticede yasa haline gelen YTCK'da da bu suç tipi yer almamıştır. Suç politikası açısından bilişim sistemi aracılığıyla bu tür belgeler düzenlenip kullanılacağı ve böylelikle kamunun güveni ihlal edilebileceği için bu suç tipi YTCK'da açık bir biçimde 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 bir düzenlenme şeklinde bu suçların ağırlatıcı nedeni olarak

öngörülmalıdır (Dülger, Bilişim Suçları 2004, s.332,333; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.109; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.118).

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 yapılmalıdır (Ünver 2001, s.106,107; Dülger, Bilişim Suçları 2004, s.333; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.118,119).

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 (Dülger, Bilişim Suçları 2004, s.333; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.111; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.119).

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 YTCK'da herhangi bir düzenlemenin olmaması önemli bir eksiklik olarak görülmektedir(Dülger, Bilişim Suçları 2004, s.333; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.111; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.119).

Veri iletim ağları üzerinden gerçekleştirilen kumar oynatma ve oynama eylemi mutlaka ayrı bir suç tipi olarak düzenlenmelidir. Bu konuda büyük bir yasal boşluk bulunmaktadır. YTCK'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 YTCK'nın 228. maddesinde "kumar oynanması için yer ve imkan sağlanması" denilerek geniş bir ifade kullanılıyor ve bu maddenin internet üzerinden gerçekleştirilecek eylemler açısından da uygulanabileceği mümkün görülüyorsa da yorum sorunlarının yaşanmaması ve uygulamada karışıklığa neden verilmemesi için "sanal alanda bilişim sistemleriyle kumar oynatılmasının" da madde metninde belirtilmesi uygun bir düzenleme olacaktır (Dülger, Bilişim Suçları 2004, s.333; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.112; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.119).

Başta ABD'de 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. YTCK'da bu eylemin de suç tipi olarak düzenlenmesi gerekmektedir (Dülger, Bilişim Suçları 2004, s.333,334; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.112; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.119).

Bilişim suçlarıyla ilgili olarak yapılması gereken önemli bir düzenleme de çocukların sanal alanda ticari amaçla cinsel istismarının bağımsız bir suç tipi haline getirilmesidir (Ünver 2001, s.99). 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 getirilmelidir (Ünver 2001, s.101). Ayrıca her türlü çocuk pornografisi içeren materyalin bilişim sistemlerinde bulundurulması, bunların paylaşımına açılması, iletilmesi ve kullanılması suç tipi olarak düzenlenmelidir (Dülger, Bilişim Suçları 2004, s.336,337; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.119).

Özellikle internet üzerinden gerçekleştirilen "çocuk pornografisine ilişkin her türlü eylem" suç haline getirilmelidir. Bu eylemlerin neler olduğu Avrupa Siber Suç Sözleşmesinde tek tek gösterilmiştir. Günümüzde neredeyse kanayan bir yara haline gelen ve internetin ortaya çıkmasından beri bu çok yararlı ağ sisteminin en zararlı yanı olarak kabul edilen (Raman 2004; Sokulu Akıncı 2001, s.37; Çeken 2003, s.56) bilişim sistemleri aracılığıyla çocuk pornografisi içerikli verilerin üretimi, dağıtılması ve bulundurulması eylemlerinin bu sözleşme ile ayrıntılı olarak tarif edilmesi ve söz konusu eylemlerin sanal dahi olsa her türlü gerçekleştirilme şeklinin suç olarak düzenlenmesi bu sözleşmenin dikkati çeken en önemli düzenlemelerinden birisidir (Dülger, AK ve AB Düzenlemelerinde Çocuk Pornografisi 2004, s.1485,1486). Söz konusu sözleşmede de ayrıntılı olarak belirtilen bu eylemlerin suç haline getirilmesinin çok acil şekilde yapılması gerekmesine rağmen YTCK'da buna konuyla ilgili düzenleme olan 226. madde bu açıdan son derece yetersizdir (Dülger, Bilişim Suçları 2004, s.337; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.111). Bu yetersizliğin konunun önemini farkına varılarak en kısa zamanda giderilmesi gerekmektedir (Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.120).

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 (Dülger, Bilişim Suçları 2004, s.337; Dülger, Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi 2004, s.113; Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu 2005, s.120).

II. BİLİŞİM SUÇLARI İLE MÜCADELEDE ALINMASI GEREKEN ÖNLEMLER

Bilişim suçlarının çok ciddi bireysel ve toplumsal sonuçları bulunduğu bugün artık yadsınamayan bir gerçektir (Özdilek 2004), dolayısıyla bu suç tipleriyle yürütülecek mücadelenin de çok boyutlu olması gerekmektedir. Ancak ceza hukuku normlarıyla sağlanmaya çalışılan koruma, bilişim suçlarıyla mücadelenin yalnızca bir boyutudur (Dülger, Bilişim Suçları 2004, s.319,320). Bu mücadelenin diğer bir boyutu da bilişim sistemi kullanan kişi, kurum ve hatta devletlerin bu konuda almaları gereken önlemler ve ceza hukuku dışında özellikle sanal alanın hukuksal bir alan haline getirilmesi için yapmaları gereken düzenlemelerdir (Dülger, Bilişim Suçları 2004, s320; Özdemir 2000, s.20).

Bilişim suçlarıyla mücadelede alınması gereken önlemler olarak ceza hukuku normlarıyla bu konuyla ilgili kamu düzeninin ihlali olarak görülen eylemlerin suç tipi olarak tanımlanmasının yanında ve öncesinde aşağıda kısaca ve genel olarak üç başlık halinde incelenecek önlemlerin alınması gerekmektedir. Bunlar; “kişilerin ve/veya kurumların alması gereken önlemler”, “devletlerin alması gereken önlemler” ve” sanal alanın düzenlenmesidir”.

A. Kişilerin ve/veya Kurumların Alması Gereken Önlemler

Bilişim suçlarıyla mücadelede alınması gereken önlemlerin ilki, kişilerin ve kurumların kullandıkları bilişim sistemlerinin güvenliğini sağlamalarıdır. Bununla kastedilen; sistemde bulunan verilerin ve sistemin kendisinin, gizliliği, bütünlüğü ve kullanıma yönelik her türlü tehlikelere karşı güvenliğinin sağlanmasıdır (Dülger, Bilişim Suçları 2004, s.320).

Buna göre, bilişim istemlerinin güvenliğinin yedi ana konudan oluştuğu belirtilmektedir (Dülger, Bilişim Suçları 2004, s.320,321; Yenidünya/Değirmenci 2003, s.113; Değirmenci 2002, s.106-108), bunlar; 1. idari ve kurumsal güvenlik, 2. personel güvenliği, 3. fiziksel güvenlik, 4. iletişim ve elektronik güvenliği, 5. donanım güvenliği, 6. yazılım güvenliği; 7. işlem güvenliğidir (Bu konuda farklı ayırım yapanlar da bulunmaktadır, bkz: Uzunay, 2003, s.138).

Bu güvenlik önlemleriyle, hem bilişim sistemleri için öngörülen güvenlik, hem sistemde bulunan verilerin gizliliği ve yetkisiz erişimlerin önlenmesi, hem de sistemin kesintisiz olarak çalışması sağlanmalıdır(Akbulut 1999, s.245). Bugün için özel sektöre devredilmiş bir çok kamu hizmeti tamamen bilişim sistemlerinin kontrolünde çalışmaktadır, bu sistemlerin çalışmasının kesintiye uğratılması toplumda büyük zararların doğmasına sebebiyet verebilecektir(Dülger, Bilişim Suçları 2004, s.321).

Bugün için en yaygın olan, uygulamada en çok başvurulan ve etkili olan önlemler ise; bilişim sistemlerinde “fire wall” adı verilen güvenlik duvarı yazılımlarının bulundurulması yetkisiz erişimlerin önüne geçilmesi ve bilişim

sistemlerine anti-virüs yazılımları yüklenerek ve bu yazılımlar internet üzerinden sürekli güncellenerek yeni virüslerin bilişim sistemine girmesinin önlenmesine, girenlerin ise temizlenmesine çalışılmasıdır (Uzunay, 2003, s.139,140). Bir de özellikle büyük kurumların bilgi işlem merkezlerinde ancak yetkisi olan ve güvenilir personelin çalıştırılmasının sağlanmasıdır(Dülger, Bilişim Suçları 2004, s.321).

B. Devletlerin Alması Gereken Önlemler

Yukarıda belirtilen bilişim sistemlerinin ve içerdiği verilerin güvenilirliğinin sağlanması kamu kurum ve kuruluşları tarafından kullanılan bilişim sistemleri ve sahip olunan veriler açısından da geçerlidir. Bu başlık altında değinilen konu ise devletin bu suç tiplerinin işlenmesi önlemek için alacağı ve üçüncü kişileri de etkileyen önlemlerdir. Bu önlemler, “bilişim suçlarını kovuşturan birimlerin eğitilmesi”, “sanal terörizm olgusuna karşı alınan önlemler”, “devletlerin sanal alanı denetlemesi” ve “uluslararası işbirliği yapılması” şeklinde dört başlık altında toplanabilir.

Bu önlemlerin ayrıntılı olarak açıklanması uzun sayfaları gerektirmektedir; buna ise bu çalışmanın sınırları izin vermemektedir. Söz konusu önlemlere kısaca değinilecek olursa, “bilişim suçlarını kovuşturan birimlerin eğitilmesi” kavramıyla özellikle polisin ve savcılarının bu suçların niteliği ve delillerin elde edilmesi açısından acele ve etkin bir biçimde eğitilmesi kastedilmektedir. Özellikle polisler açısından, bu alanda “ya bir polisi alıp bilişim uzmanı yapacaksınız ya da bir bilişim uzmanını polis yapacaksınız” ifadesi kullanılmaktadır (Dülger, Bilişim Suçları 2004, s.322; Yenidünya/Değirmenci 2003, s.110,111). Bu alanda polis açısından önemli gelişmeler olduğu ve bunların somut ürünlerinin uygulamaya geçirildiği söylenebilirse de (bu somut örnekler açısından bkz: Yamaç/Dokurer/Özcan 2004) savcılık kurumu açısından aynı ifadeleri kullanmak mümkün görülmemektedir. Aynı şekilde bu konuda karar verecek yargıçların ve savunma yapacak avukatların da benzer eğitimleri alması gerekmektedir (Dülger, Bilişim Suçları 2004, s.323).

“Sanal terörizm olgusuna karşı alınan önlemler” başlığı altında ise şu değerlendirmeler yapılabilir. Sanal terörizm, belirli bir siyasal ve sosyal amaca ulaşabilmek için bilişim sistemleri kullanılarak bireylere, mallara ve toplumsal yaşayış düzenine zarar verilerek, toplumu ve yöneticileri yıldırma, baskı altında tutma çalışmaları olarak tanımlanmaktadır (Özcan 2004, s.308,309). Terörist örgütlerin sanal terörizmle gerçekleştirebilecekleri ve toplum üzerinde çok büyük zararlara neden olabilecek ve acil önlem alınması gereken eylemlerine örnek olarak; istenilen kentin bütün trafik ışıklarının durdurulması, telefonları hatlarının felç edilmesi, elektriğin ve doğalgazın kapatılması, bilişim sistemlerinin işletim dışı bırakılması, ulaşım ve su sistemlerinin işleyişinin bozulması, bankacılık ve finans sektörünün çökertilmesi, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engellenmesi verilmektedir (Salıcı/Güneş 2004; Yamaç/Dokurer/Özcan 2004). Özellikle 11 Eylül 2001’de ABD’nin New York kentinde bulunan ve ikiz kuleler olarak anılan Dünya Ticaret Merkezi’ni yıkan

terörist saldırılar için gerekli örgütlenme, destek ve eğitim için internetin çok geniş ve denetlenemeyen olanaklar sunduğu belirtilmektedir (Tanyol 2002). Bu eylemden ve ABD’li yetkililerin bu eylemin hazırlanması için teröristlerin internet üzerinden iletişime geçtiklerini açıklamasından sonra bir çok ülkede sanal terörizme karşı önlemler alınması yönünde çalışmalar başlatılmıştır (Murphy 2004). Ülkemizde ise, uzun yıllar terörizmle mücadele edilmiş ve edilmekte olmasına, bu konuda çok zarar görülmüş ve çok acıya katlanılmış olmasına rağmen ciddi bir tehdit olan sanal terörizme ve gerçekleşebilecek terörist eylemlere karşı ceza hukuku açısından hiçbir düzenleme yapılmadığı görülmektedir (Dülger, Bilişim Suçları 2004, s.325).

Bilişim suçlarıyla mücadelede devletlerin alabileceği etkin önlemlerden birisi olarak da sanal alanın özellikle de internetin denetlenmesi ve bu alan üzerindeki iletişimin kontrol altında tutulmasının gerektiği gösterilmektedir. Ancak sanal alanın denetlenmesindeki temel sorunun; kişi mahremiyeti ve iletişim özgürlüğü gibi, demokratik toplumların olmazsa olmaz ilkelerinin zedelenmeden, bir denetim mekanizmasının kurulup kurulamayacağı olduğu ifade edilebilir (Dülger, Bilişim Suçları 2004, s.325). Bu konuda yaşanan ikilem; özgürlük alanı olarak tanımlanan özellikle internet aracılığıyla gerçekleştirilen bilişim suçlarıyla mücadelenin, bireyin evrensel temel hak ve özgürlüklerinin özüne dokunulmadan gerçekleştirilmesindeki güçlüktür (Salıcı/Güneş 2004). Ancak bu çekincelere rağmen halkın bilgisine açık, bağımsız yargıların denetiminde olan bir kurumun temel halk ve özgürlükleri kısıtlamaksızın, belli başlı suçlara ve özellikle çocuk pornografisine ilişkin filtreleme yapması ve böylelikle olası suç ve suçluları belirlemesi şeklinde bir yöntem geliştirilebilir (Dülger, Bilişim Suçları 2004, s.327).

Devletin alması gereken önlemler başlığı altında değinilecek olan son konu devletlerin bilişim suçlarıyla mücadelede uluslar arası işbirliğine yönelmelerinin kaçınılmazlığıdır. Bu suç tipleri doğaları gereği ve genellikle görüldüğü üzere bir çok ülke sınırlarını geçen veri iletim ağları üzerinde gerçekleştirilmektedir. Bu nedenle benzer eylemler tüm ülkelerde birbirine benzer şekillerde suç tipi haline getirilmeli ve de özellikle suç ve suçlunun kovuşturması esnasında ilgili kurumların yetki ve görevleri yeknesak kurullarla belirlenmelidir. Nitekim bu konudaki en somut ve güncel örnek Avrupa Siber Suç Sözleşmesidir (Dülger, Bilişim Suçları 2004, s.327,328).

C. Sanal Alanın Düzenlenmesi

Bilişim suçlarıyla mücadele açısından alınması gereken bir diğer önlem de sanal alanın, özellikle de bugün için en yaygın veri iletim ağı olan internetin düzenlenmesidir. Temel olarak sanal alanı düzenlemek için dört seçenek birbiriyle yarışmaktadır, bunlardan ilk üçü klasik olarak bilinen modellerdir, dördüncüsü klasik ve merkezi olmayan bir modeldir. Dördüncü seçenek sanal alanı kullananların etik davranışları dikkate alınarak önerilen bir düzenlemedir (Dülger, Bilişim Suçları 2004, s.328). Bu nedenle dördüncü modelin bir diğer adı da “kendi kendine düzenleme” modelidir (Çeken 2003, s.10).

Sanal alanın düzenlenmesi yöntemleri şunlardır; “ulusal alanda yapılan düzenleme”, uluslararası anlaşmalarla yapılan düzenleme”, uluslar arası kuruluşlar oluşturularak yapılan düzenleme” ve “kendi kendine yapılan düzenlemedir” (Dülger, Bilişim Suçları 2004, s.329).

Bunlardan özellikle sonuncusu yeni bir kavram olması nedeniyle çok dikkat çekmektedir. Buna örnek olarak “öz-düzenleme” (self-regulation) ve “işbirliğine dayalı düzenleme” (co-regulation) yöntemleri gösterilebilir (Akdeniz 2003, s.51-57; Akdeniz 2004, s.24). Bu düzenleme modelinde kendiliğinden ortaya çıkan kurallardan sanal alana uygulanacakların seçimi, filtrelemelerin yapılama yöntemi, sanal alana girecek kullanıcıların ve sistemi yöneteceklerin seçimi vb. düzenlemeler kendi kendine yapılacaktır (Johnson/Post 2004). Sanal alan için uygulanacak bu düzenlemeler için yine sanal alanda kendiliğinden oluşturulan bu kurallara kısaca “netiket” denilmektedir (Memiş 2001).

Yukarıda kısaca belirtilen bu önlemler alınmadan da yukarıda açıklanan yasal tanımda yer alan eylemlerin gerçekleştirilmesi halinde suç işlenmiş olacak ve failer cezalandırılacaktır; ancak unutulmamalıdır ki ceza hukuku ikincil nitelikte olan bir hukuk disiplinidir. Bu önlemlerin alınmasıyla ise suç işlenmesinin önüne geçilebilecek bu önlemlere takılmadan geçebilen sınırlı sayıdaki olay yargılama konusu olacaktır. Bundan da önemlisi, bugün için yaşamsal önem taşıyan bilişim sistemlerinin ve bunların oluşturduğu ağ sisteminin güvenilirliği ve sürekli çalışır durumda olması sağlanabilecek ve bu tür suçlar neticesinde gerçekleşebilecek zararlar en alt düzeyde tutulabilecektir.

KAYNAKÇA

- 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.
- Akdeniz**, Yaman, “Çağdaş İnternet Yönetimi”, Güncel Hukuk, S:6, İstanbul, Haziran 2004, s.24, 25.
- Akdeniz**, Yaman, Internet Governance: Towards the Modernization of Policy Making Process in Turkey, İstanbul, Ankara, İzmir, Adana, TBV Series:1, Papatya Publication Education, 2003.
- Çeken**, Hüseyin, Council of Europe’s Convention 2001 on Cybercrimes and Turkey, Unpublished Master of Science Thesis (University of Marmara European Community Institute Law of European Union), İstanbul, 2003.
- Değirmenci**, Olgun, “Bilişim Suçları”, Yayınlanmamış Yüksek Lisans Tezi (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı), İstanbul, 2002.
- Dülger**, Murat Volkan, “Bilişim Suçları ve Yeni Türk Ceza Kanunu”, Kazancı Hukuk, İşletme ve Maliye Bilimleri Dergisi, İstanbul, S:5, Ocak 2005, s.114-120.
- Dülger**, Murat Volkan, Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2004.
- Dülger**, Murat Volkan, “Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler”, İBD, 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.
- Johnson**, David R./David G. Post, “And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law”, (Çevrimiçi) <http://www.cli.org/emdraft.html>, 19.04.2004.
- Memiş**, Tekin, “İki Uluslararası Sempozyum ve Bir Özet”, AÜEHFD, Erzincan, C:V, S:1-4, 2001, s.445-451.

- Murphy**, Jonn F., "Computer Network Attacks by Terrorists: Some Legal Dimensions" SSRNEL, (Çevrimiçi) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=208671, 02.05.2004.
- Özcan**, Mehmet, "Siber Terörizm ve Ulusal Güvenlik", İnternet ve Hukuk, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.301-340.
- Özdemir**, Muammer, "Suç ve Ceza", PC Magazine Türkiye, S:78, Mayıs 2000, s.20.
- Özdilek, Ali Osman**, "Bilgisayar Suçları Ne Kadar Ciddi?", (Çevrimiçi) http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm, 20.04.2004.
- Özel**, Cevat, "Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İBD, İstanbul, C: LXXV, S: 7-8-9, Eylül 2001, s.858-872.
- Raman**, Jari, "Computer Crime" (Çevrimiçi) http://www.urova.fi/home/oiffi/enlist/commentary/computer_crime.html, 21.12.2004.
- Salıcı**, Berfu/İsmail Güneş, "İnternette Güvenlik ve Denetim: Masumiyet Yitiriliyor Mu?" (Çevrimiçi) http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=243, 14.04.2004.
- Sokullu Akıncı**, Füsün, "Avrupa Konseyi Siber Suç Sözleşmesi'nde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve İnternette Çocuk Pornografisi" İÜHFM, İstanbul, C:LIX S:1-2, 2001, s.11-38.
- Tanyol**, Tuğrul, "Anarşizm ve İnternet", Cogito İnternet: Üçüncü Devrim, Yapı Kredi Yayınları, S:30, Kış 2002, s.204-210.
- Uzunay**, Yusuf, "Dijital Saldırıları, Emniyet Güçleri Açısından Önemi ve Korunma Yolları", PBD, Ankara, C:5, S:2, 2003, s.131-146.
- Ünver**, Yener, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", İÜHFM, C:LIX S:1-2, İstanbul, 2001, s.51-153.
- Yamaç**, Fatih/Semih Dokurer, Mehmet Özcan, "Bilişim Suçları", (Çevrimiçi) <http://inet-tr.org.tr/inetconf7/bildiriler/86.doc>, 11.04.2004.
- 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.
- Yenidünya**, Caner/Olgun Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, Legal Yayıncılık, 2003.