ÜNİTE 8

BİLİŞİM SUÇLARI VE BİLİŞİM CEZA HUKUKU

BİLİŞİM SUÇLARI VE BİLİŞİM CEZA HUKUKU

ANAHTAR KAVRAMLAR

Ceza Hukuku
Bilişim Hukuku
Bilişim Suçları
Siber Suçlar

ÖĞRENME HEDEFLERİ

1 Bilişim hukuku ile ceza hukuku bağlantısını kurmak.

2 Bilişim alanındaki suçların neler olduğunu, unsurlarını ve bu suçlar için öngörülen cezaları öğrenmek

SEKİZİNCİ BÖLÜM

GİRİŞ

Günümüzde bilgi ve enformasyonun etkin olarak işlenmesinde belki de en önemli yere sahip olan bilişim teknolojisinin gelişimi ve özellikle modern bilgisayarın 20 yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşümün içinde şekillenerek kullanımın yaygınlaşmasıyla birlikte, toplumsal kurumları çeşitli yönleriyle etkilemeye başlamıştır. Söz konusu etkinin kapsamı ve boyutları, dönüşümün dinamikleri ve derinliğiyle bağlantılıdır. Toplumsal bir kurum olan hukuk da birçok yönüyle söz konusu gelişimden etkilenmektedir. Bu bağlamda, bilişim suçları, bilgisayar suçları gibi birçok ad altında incelenen suçlar, dönüşümün maddi ceza hukukuna etkisini oluşturmaktadır.

Bu kapsamda bilişim suçları olarak adlandırılan suçlar, tek başına ne bir bilim dalı olarak bilişim ne de bir bilişim sistemi olarak bilgisayar ya da İnternet'in kullanılmaya başlanmasıyla açıklanabilmektedir. Bilişim sistemlerinin kullanılmasının sosyo-ekonomik dönüşüm içinde ceza hukukuna etkisi olarak anlaşılması karşısında, birçok suçun bilişim suçları başlığı altında incelenmesi mümkündür. Nitekim bu gelişimin etkisiyle düzenlenen Avrupa Konseyi Sibersuç Sözleşmesi söz konusu etkinin belirli bir dönemdeki etkisi olarak önemli bir örnek oluşturmaktadır.

Farklı nitelikteki birçok suçun bilişim suçları adı altında gündeme gelmesi, bilişim suçlarının incelenmesine ilişkin belirli bir sınırlandırılmaya gidilmesi zorunluluğunu doğurmaktadır. Bu nedenle konu, daha çok 5237 Sayılı TCK'nin 243 ve 244. maddelerinde düzenlenen sınırlı tutulmuş banka ve kredi kartlarının kötüye kullanılması suçuna ve ayrıca Elektronik İmza Kanununda düzenlenen suçlara da ilgisi olduğu ölçüde kısa bir şekilde değinilmiştir. Özellikle TCK'nin 243 ve 244. maddesinde düzenlenen suçlar, ceza mevzuatlarına yeni suçların girmesi anlamında niteliksel bir etki olarak karşımıza çıkmaktadır.

Ayrıca kişisel verilerin korunmasına ilişkin TCK'nin 135 vd. maddelerinde düzenlenen suçlar da inceleme konusu yapılmıştır. Her ne kadar genel olarak bilişim suçları başlığı altında incelenmese ve Sibersuç Sözleşmesinde yer verilmemiş olsa da kişisel verilerin korunması da

sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kullanımının önemli bir etkisi olarak ortaya çıkmakta ve kişisel verilerin korunmasına ilişkin suçlar bu etkinin bir sonucu olarak ceza mevzuatlarında yer edinmektedir.

Bu suçların incelenmesi, sosyo-ekonomik dönüşüm içinde anlam kazanan ve bilişim suçları adı altında suç olarak düzenlenen fiiller yönünden, düzenleme yeri ve kapsamına ilişkin soruna ve sorunun çözümüne ilişkin 5237 Sayılı TCK'de hakim olan yaklaşımın ve yöntemin tespiti bakımından önem arz etmektedir.

Bu nedenle, bilişim sistemleri ve özellikle İnternet aracılığıyla işlenen çocuk pornografisi, ırkçılık ve yabancı düşmanlığı, hakaret gibi suçlar ile telif haklarının korunmasına ilişkin suçlar, kapsam dışı bırakılmıştır. Gerçekte, bu tür suçların bilişim suçları arasında incelenmesinin nedeni, bilişim sistemlerinin kullanılması suretiyle işlenme oranlarının artması ve yaygınlaşmasından kaynaklanmaktadır. Niceliksel etki olarak gündeme gelen bu husus farklı açılardan önem az edebilmekle birlikte bu çalışmanın kapsamı dışında bırakılmıştır.

TCK'deki ifadesiyle, "Bilişim Alanında Suçlar" hem 765 Sayılı TCK hem de 5237 Sayılı TCK'nin çeşitli yönleriyle düzenlenmiştir. 765 Sayılı TCK'nin 525a vd. maddelerinde "Bilişim Alanında Suçlar" başlığı altında düzenlenen suçlar, sosyo-ekonomik dönüşümde bilişim sistemleri ve özellikler bilgisayar sistemlerinin kullanımının bir etkisi olarak ilk defa ceza mevzuatımızda yer edinmiştir. Kişisel verilerin korunmasına ilişkin suçlar ise ilk defa 5237 sayılı TCK'de özel olarak düzenlenmiştir.

Bu haliyle ceza hukuku açısından sorunun bir yönü, bilgi ve enformasyonun, korunmasıyla ilgilidir. Sorunun diğer bir yönü, sayısallaşma olarak adlandırılan durum ile ilgilidir. Sosyo-ekonomik faaliyetlerin ağırlıklı olarak bilişim ve bilgisayar sistemleri aracılığıyla gerçekleştiriliyor olması karşısında, bilişim alt yapısının korunması da önemli hale gelmiştir. Bu tür sorunlar, bir bütün olarak, bilişim sistemlerine ve bilgi ya da enformasyonu temsil eden veriye yönelik bir kısım fiillerin suç olarak düzenlemesine ilişkin tartışmaları beraberinde getirmiştir.

Söz konusu sorunlara ilişkin olarak ceza hukukunda tartışmaların merkezini oluşturan hususlar, hangi değerin korunduğu ve bununla bağlantılı olarak bu değerlere yönelik saldırıları ifade eden hangi tür fiillerin suç olarak düzenlenmesi gerektiğidir. Nitekim, bilişim suçları olarak adlandırılan suçlarda, öncelikli olarak ceza müeyyidesiyle koruma altına alınan değerin ne olduğunun tespiti önemlidir. Bu husus, bir yandan korumanın amacını ve meşruiyetini göstermektedir. Diğer bir yandan da suçun hukuki konusunun saptanması sonucunu doğurmaktadır. Suç olarak düzenlenen fiiller ise, söz konusu değerlere yönelik ihlal yöntemlerinin ne şekilde olduğunun ya da olabileceğinin belirlenmesi suretiyle tespit edilmiştir.

Sorunun odak noktasının suçun hukuki konusunun ve bununla bağlantılı olarak özellikle suç olarak düzenlenecek fiillerin belirlenmesi olarak ortaya çıkması, söz konusu suçların incelenme yöntemini de belirlemiştir. Bu doğrultuda, tartışmanın merkezinin suçun hukuki konusu ve suç olarak düzenlenen fiiller olması, bu incelemenin ağırlıklı olarak bu iki husus etrafında yapılması tercihini de belirleyen etkenlerdendir.

Bilişim Suçları - Terim, Tanım ve Kapsam Sorunu

Bilişim ve özellikle bilgisayar sistemlerinin yaygınlaşması ile birlikte ceza hukuku alanında, bunların kötüye kullanımlarına ilişkin fiillerin cezalandırılabilirliği ve kötüye kullanımının ortaya çıkardığı sorunların çözümü ya da çözüme ilişkin yaklaşımlar sonucu, birçok tanım yapılmış ve bu tanımları ifade etmek üzere birçok terim kullanılmıştır. "Bilgisayar suçları", "bilgisayar suçluluğu", "bilişim suçları", "internet suçları" ve Sibersuç sözleşmesinde de ifade edildiği şekliyle "siber suçlar" terimler kullanılabilmektedir.

Tanım ve terim zenginliği yanında, bu alanda ortaya çıkan ihlallerin cezalandırılabilmesine ilişkin suçlar esas alınarak, bilgisayarın ya da bilişim sisteminin suçun maddi konusu ya da suçta kullanılan araç olması gibi hususlar esas alınarak birçok sınıflandırma yapılması kapsam sorunlarını da beraberinde getirmiştir.

Nitekim bu suçlarının ne olduğu üzerinde herkesin ittifakla kabul edebileceği bir tanımın yapılabilmesinin zor olduğunu ve bunun yerine bilgisayar suçlarına ilişkin genel bir kategori suçtan bahsetmenin daha doğru olduğunu ifade edilmiştir. Bu kapsamda söz konusu suçların suçları "ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller" olarak belirlenmesi yerinde olabilecektir. bilişim ve bilgisayarın farklı anlamlara sahip olduğunu ve "bilgisayar suçu" ile "bilişim suçu"nun birbirinden farklı şeyleri ifade ettiğini; pratikte ise bilgisayarın en yaygın bilişim aracı olması nedeniyle "bilişim suçları" yerine "bilgisayar suçları" teriminin kullanıldığı da bu görüş kapsamında belirtmektedir.

Bilişim ve bilgisayar terimlerinin farklı anlamlara sahip olduğu, bu kavramların birbiri yerine geçecek şekilde kullanılmasının hatalı olduğu Yenidünya ve Değirmenci tarafından da ifade edilmiştir. Yazarlara göre bilişim terimi, bilgisayara göre, daha geniş bir alanı kapsayıp bir üst kavramdır. Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetlerini, diğer bir anlatımla veri-işlemi tek başına gerçekleştirebilmektedir. Bilişim ise, hem verilerin işlenmesini hem de verilerin aktarımını kapsar. Bilişim sistemlerinin en yaygın kullanılan unsurunun bilgisayarlar olması, "bilgisayar suçu" teriminin yaygınlık kazanmasına neden olmuştur. Bu açıklama doğrultusunda yazarlar bilişim suçu terimini kullanmayı uygun bulduklarını belirtmektedirler.

Ersoy da bilişim suçu ve bilgisayar suçu ayrımını yapmakta, bilişim suçunun bilgisayarı da kapsayan ancak daha geniş olan bilişim araçlarına karşı ya da bilişim araçları ile işlenen suçları da kapsar şekilde anlaşılması gerektiğini ifade etmektedir.

Türk hukukunda, özellikle bilişim suçu ya da bilgisayar suçu terimleri tercih edilmekte ve bu iki terim arasında anlam ve kapsam farklılığı yaratılmaktadır. Söz konusu ayırım "bilişim sistemi" ve "bilgisayar" terimlerinin farklılığından hareketle dile getirilmektedir. Bunlar arasında yapılan ayırım sonucunda, bilişim suçu teriminin bilgisayar suçlarını da içeren geniş bir kapsama sahip olduğu vurgulanmaktadır. Yazarlar tarafından yapılan bu ayırım, özellikle bilişim suçları açısından suçun konusu ya da suçta kullanılan araç olarak "bilgisayar", 765 Sayılı TCK'de belirtildiği şekliyle, "bilgileri otomatik işleme tabi tutmuş sistem" ve TCK'nin 243 vd. maddelerinde yer alan "bilişim sistemi"nin kapsamının ne olduğuna ilişkin tartışmalardan kaynaklanmıştır.

765 Sayılı TCK'nin 525a vd. ve TCK'nin 243 vd. maddelerinde düzenlendiği şekliyle, suçun konusunun ya da suçta kullanılan aracın tespitinden önce bilişim suçu ile neyin anlaşılması gerektiğinin tespiti gerekmektedir. Yukarıda yapılan tanımlara dikkat edilecek olursa, Türk Hukukunda bilişim ya da bilgisayar suçları, bilişim sistemi, bilgileri otomatik işleme tabi tutan sistem ve bilgisayar terimlerinin anlam ve kapsamı belirlenmek suretiyle tanımlanmaktadır. Bu doğrultuda, bilişim ve bilgisayarın anlamlarından yola çıkılarak ve ayrıca bilişim sistemi olarak değerlendirilen araç ve aygıtlar ve de bilgisayar ara-

sındaki farklar da esas alınarak bilişim ya da bilgisayar suçu tanımları yapılmaktadır. Aynı şekilde söz konusu suçların sınıflandırılmasında da suçta kullanılan araç ya da suçun maddi konusu olan bilgisayar ya da bilişim sistemi esas alınmaktadır.

Bilindiği üzere suçların sınıflandırılmasında suçun maddi konusu ya da suçta kullanılan araç esas alınabilmekte ve suçlar bu şekilde de ayırıma tabi tutulabilmektedir. Bu ayırım ise, Toroslu'nun ifade ettiği üzere, öncelikli olarak maddi konusu olmayan suçların bulunup bulunmadığına ilişkin tartışmalar nedeniyle çeşitli sorunlara yol açabilmekte, bir yandan da farklı nitelikteki suçların bir araya toplanması sonucunu doğurarak, suçların sınıflandırılmasında beklenen yararın sağlanmasına engel olmaktadır. Suçta kullanılan araç ise bazı suçlarda özellikle suça etki eden neden olarak önem taşıyabilmektedir.

Suçların, maddi konu ya da suçta kullanılan aracın esas alınarak sınıflandırılmaya tabi tutulmasında ortaya çıkan sakınca, suçun maddi konusu ya da suçta kullanılan araç esas alınarak suçların tanımlanması durumunda da geçerliliğini korumaktadır. Bu doğrultuda, suçta kullanılan araç ve suçun maddi konusu esas alınarak bilişim ya da bilgisayar suçlarının tanımı yapılması da sosyo-ekonomik dönüşümde bilişim sistemlerinin hukuka etkisinin ve ortaya çıkardığı sorunların doğru biçimde tespitini zorlaştırmaktadır. Bilişim sistemlerinin kullanımının sorunları ne şekilde etkilediğinin saptanması bakımından maddi konu ya da kullanılan araç kapsamında bu suçların topluca incelenmesi kısmen yarar sağlamaktadır. Aynı şekilde, ceza mevzuatlarında yer alan suçların unsurlarının bu tür fiilleri kapsayıp kapsamadığının tespiti bakımından da yarar sağlayabilmektedir. Fakat bu tür fiillerle hangi değere yönelik saldırının söz konusu olduğunun tespitinde yetersiz kalmaktadır. Nitekim bilişim ve özellikle bilgisayar sistemlerinin kullanımın yaygınlaşma oranına bağlı olarak, çok çeşitli fiillerin işlenebilir hale gelmesi, bu tanımların kapsamının çok farklı amaçlara yönelik suçları da kapsayacak şekilde genişletilmesine ya da kendi içinde alt ayırımlar yapılmasına neden olmaktadır.

Bilişim sistemlerinin kullanımının yaygınlaşması, özellikle bilgisayar sistemlerinin ağırlıklı olarak kullanımı, kullanıldığı yere ve amacına göre hukuki sorunlara yol açabilmektedir. Ceza hukuku bakımından ortaya çıkan sorunlar, suçun unsurlarından kaynaklanabildiği gibi cezalandırma siyaseti açısından daha önce suç olarak düzenlenmeyen bir fiilin, suç haline getirilmesinin gerekli olup olmadığı şeklinde ortaya çıkmaktadır. Özetle, suç ve cezada kanunilik ilkesi açısından mevcut suçların unsurlarının bu tür fiilleri kapsayıp kapsamadığı ya da bu tür fiillere ilişkin yeni suçların düzenlenmesi, sorunun odak noktasını oluşturmaktadır.

Suçun hukuki konusu açısından bakıldığında bunun anlamı, ortaya çıkan yeni fiiller karşısında, halihazırda çeşitli suçlar ile korunan hukuki değerlerin, bu tür yeni fiiller karşısında korunmasına ilişkin yöntemin saptanmasıdır.

Sieber, 1998 tarihli çalışmasında, bilgisayar suçları teriminin ilk olarak 1960'lı yıllarda ortaya çıktığını ve ilk başlarda sadece ekonomik çıkar amacıyla işlenen suçlar kapsamında değerlendirilen bilgisayar suçlarının, 1980'li yıllardan itibaren daha da genişleyerek, telif haklarına ilişkin ihlalleri, daha önce kişisel verilerin korunması olarak ayrı başlık altında incelenen hususları ve İnternet'in yaygınlaşması ile birlikte, yasadışı içeriklerin dağıtımı gibi birçok konuyu da kapsamına aldığını ifade etmiştir. Bunun sonucunda "bilgisayar suçları" ve "bilgisayar ile ilgili suçlar" terimlerinin daha geniş bir şekilde her türlü kötüye kullanımları da kapsayacak şekilde genişletildiğini, sonrasında veri veya enformasyon suçu gibi çeşitli terimlerin de kullanıldığını ifade etmiştir. Yazara göre; çeşitli terim ve tanımlar bilgisayarın herhangi bir alanda kullanılması sonucu ortaya çıkan ve o alana ilişkin sorunlara işaret eden tanım ve terimlerdir. Bu nedenle yazar, belirli bir alanda ortaya çıkan sorunlara ya da amaca özgülenen veya teknik açıdan yapılan tanımların ve bunları ifade eden terimlerin, hukuki açıdan sınırlı bir değere sahip olduğunu ifade etmektedir. Bugüne kadar yapılan tanımların yerine, bilgisayar aracılığıyla gerçekleş-

tirilen fiillerin, bu fiiller nedeniyle korunmak istenen hukuki değerlere göre tanımlanması ve incelenmesi gerektiğini savunmuştur. Yazar bu açıdan, "bilgisayarların kötüye kullanımları", "bilgisayarlarla ilgili ekonomik suçlar", "bilgisayarla ilgili özel hayatın gizliliğini ihlal" ve "diğer hukuki değerlere yönelik saldırılar" başlıkları altında üç grupta toplamıştır.

Sieber'in aktardığı şekliyle, bilişim, bilgisayar suçları, bilişim suçları gibi birçok adlar altında incelenen suçlar, spesifik bir soruna işaret etmekten çok sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kötüye kullanımlarının yarattığı sorunlara çözüm arayışlarını kapsamaktadır. Sieber'in üç grup altında topladığı etki, bilişim alanındaki gelişime paralel olarak kendi bünyesine yeni konuları da katmaktadır. Bu husus aynı zamanda, bilişim suçu veya bilgisayar suçu gibi çeşitli adlar altında incelenen suçlar arasında niteliksel farklılıklarının olduğunu ve zamanla niteliksel farklıların artacağını göstermesi açısından önemlidir.

Bünyesine yeni konuları da ekleyen söz konusu gelişim karşısında, bilişim ya da bilgisayar suçları olarak adlandırılan suçların yukarıda aktarılan, "ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller" örneğinde olduğu gibi suçun maddi konusu ya da suçta kullanılan araç olarak bilişim ya da bilgisayar sistemlerinin esas alınarak tanımlanması, farklı nitelikte ve farklı değerleri korumaya yönelik bir çok suçun bir araya toplanması ve incelenmesi sonucunu doğurur.

Bu durum niteliksel olarak farklı olan birçok suçun bir araya toplanması anlamına gelir. Bu tür tanımlar, ortak özelliği, sadece bilişim ya da bilgisayar sistemlerinin kullanılması olan suçların, bilişim suçları ya da bilgisayar suçları adı altında incelenmesi açısından etkinin yönü, boyutları ve derinliği hakkında bilgi verir. Bunun ötesinde niteliksel bir anlam taşımaz.

Özetle, bilişim suçları ya da bilgisayar suçlarına ilişkin bir tanım yerine, bilişim ya da bilgisayar suçları adı altında incelenen suçların, bilişim ya da bilgisayar sistemlerinin kullanımının belirli bir dönemde ceza hukukuna etkisi olarak nitelendirilmesi mümkündür. Sieber'in ifade ettiği şekliyle, ceza hukuku bakımından etki, farklı hukuki değerlere yönelik ihlalleri içermektedir.

İhlal edilen değere göre de ayrım yapılabilecek olan bu etki yeni suç tiplerinin ceza mevzuatı içerisine girmesi, bunun yanında hâlihazırdaki suçların işlenme kolaylığının ortaya çıkması ya da işlenme oranın artması şeklinde, ayırıma tabi tutulabilir.

Sonuç olarak, "bilişim suçu", "bilgisayar suçu", adları altında incelenen suçlar, hukuki konu açısından kategorik bir nitelik taşımamaktadır. Bunlara ilişkin tanımlar da "bir kavramın niteliklerini eksiksiz olarak belirtme veya açıklama" anlamında, tanımdan beklenen faydayı göstermekten uzaktır. Bilişim suçları, bilgisayar suçları gibi adlar altında incelenen suçlar ise, bilişim sistemlerinin ceza mevzuatlarına etkisi bakımından belirli bir dönemde ceza mevzuatlarında yer verilen suç tiplerini ifade etmektedir. Bunun yanında halihazırda ceza mevzuatlarında yer alan bazı suçların bilişim suçu vs. adlar altında incelenmesi, söz konusu suçların işlenme yoğunluğunun bilişim sistemlerinin kullanılması ile artmasında yatmaktadır.

İncelemede "bilişim suçu" teriminin kullanılması, belirli bir tanımın esas alınmasından çok, bu ad altında incelenen suçların sosyo-ekonomik dönüşümle bağlantısının daha rahat kurulabilmesine olanak sağlamasından dolayı tercih edilmiştir.

Bilişim Suçları Açısından Avrupa Konseyi Sibersuç Sözleşmesi

Bilişim sistemlerinin kullanımının ceza hukukuna etkisi, sadece ülkesel düzeyde düzenlemelerin konusu olmakla kalmamış, aynı zamanda *"Avrupa Konseyi Sibersuç Sözleşmesi"nin (Resmi Gazete'de yer alan çevirideki adıyla "Sanal Ortamda İşlenen Suçlar Sözleşmesi")* de konusunu oluşturmuştur..

Sözleşmede, bir bilişim sistemi olarak bilgisayar sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddi ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir. Sözleşmenin ikinci kısmını oluşturan maddi ceza hukukuna ve ceza yargılamasına ilişkin sorunlar iki ana bölüme ayrılmış ve birinci bölümde maddi ceza hukukuna ilişkin düzenlemelere yer verilmiştir. İkinci bölümde ise, ceza yargılamasına ilişkin sorunlar ele alınarak özellikle delillerin elde edilmesi, korunması ve saklanmasına ilişkin olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir.

Bunun yanında, bilişim suçları olarak adlandırılan suçların özellikle bilişim ağları ile işlenmesinin yaygın bir hal alması ve İnternet'in hızla yaygınlaşması, bu suçlara ilişkin sorunların ulusal bir sorun olmaktan çok uluslar arası bir sorun haline gelmesi gerçeğinden hareketle ayrıca üçüncü bir kısıma yer verilmiştir. Üçüncü kısmın konusu, Sözleşmeye taraf devletlerin birbirleri arasında adli yardımlaşmaları ve suçluların iadesidir.

Sözleşmenin amaçları, *"1.Siber suçlar alanında ülkelerin maddi ceza hukuku hükümlerini uyumlu hale getirmek, 2. Bu suçların ve bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve koğuşturulması için gerekli olan ulusal ceza muhakemesi hukuku yetkilerini belirlemek, 3. Hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak"* şeklinde sıralanmaktadır.

Sözleşmede yer ver verilen suçlarda ortak amaç, bu tür suçlara ilişkin olarak taraf devletlerin ceza mevzuatlarında uyum sağlamadır. Sözleşmede yer alan suçlar, daha önceki dönemlerde çeşitli ülkelerin ceza mevzuatında düzenlenmiş olan suçların uluslararası düzeyde ele alınması şeklindedir

Bu doğrultuda, Sözleşmenin ikinci kısmında *"Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Karşı Suçlar"* başlığı altında yetkisiz erişim (2. madde) yetkisiz müdahale (3. madde), veriye müdahale (4. madde), sisteme müdahale (5. madde) ve aygıtların kötüye kullanılması (6. madde) suçlarına yer verilmiştir.

"Yasadışı erişim", Sözleşmenin 2. maddesinde, kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girme şeklinde tanımlanmıştır. Aynı maddede, yetkisiz erişim suçunun taraf devletlerin ceza mevzuatlarında düzenlenirken, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceğine, verinin elde edilmesi ya da diğer gayri meşru bir niyetle sisteme girilmesi ya da bilgisayar ağları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceğine ilişkin ek unsurları getirebilecekleri belirtilmiştir.

"Yasadışı araya girme" ise, Sözleşmenin 3. maddesinde düzenlenmiş olup buna göre, bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, bunlara teknik yöntemler kullanılmak suretiyle müdahale edilmesinin suç haline getirilmesi öngörülmüştür. Bu maddeye göre, taraf devletlerin bu suçun oluşmasını kötüniyet ya da bilgisayar ağları aracılığıyla işlenmesi şartına bağlayabilmeleri mümkündür.

Sözleşmenin 4. maddesinde veriye müdahale, 5. maddesinde sisteme müdahale düzenlenmiştir. Sözleşmenin 4. maddesinde göre, veriye zarar verilmesi, verinin bozulması, değiştirilmesi veya ortadan kaldırılmasının suç olarak düzenlenmesi gerekmektedir. Madde incelendiğinde, verinin bilgisayar içinde bulunması ya da herhangi bir saklama aygıtında olması arasında fark yaratılmadığı görülmekte-

dir. Aynı maddenin ikinci fıkrasında, taraf devletlerin söz konusu suçun gerçekleşmesi için ciddi zararın varlığı şartına yer verebilecekleri ifade edilmiştir.

Sözleşmenin 5. maddesinde, sisteme müdahale düzenlenmiştir. Sözleşmenin beşinci maddesinde sistemin işleyişinin ciddi olarak engellenmesinin suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler, sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınarak düzenlenmiştir. Bu açıdan, fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir.

Sözleşmenin 6. maddesinde ise, birtakım hazırlık hareketlerinin suç olarak düzenlenmesi yoluna gidildiği görülmektedir. Nitekim 6. maddenin 1. fıkrasına göre, Sözleşmenin 2-5. maddelerinde düzenlenen suçların işlenmesi için öncelikli amacının söz konusu suçların işlenmesine yönelik tasarlanmış ya da uyarlanmış olan program da dahil cihazların (m. 1/,a. i); söz konusu suçların işlenmesi amacıyla, bir bilgisayarın tamamına ya da bir kısmına erişimi sağlayabilecek bir bilgisayar şifresinin, erişim kodunun ya da benzer verinin (m. 1/a.ii), üretiminin, satışının, kullanılmak için tedarikinin, ithal edilmesinin, dağıtılmasının ya da diğer şekilde erişilebilir kılınmasının taraf devletlerce suç olarak düzenlenmesi hükmüne yer verilmiştir.

Aynı maddenin "b" bendinde, Sözleşmenin 2 ila 5. maddeleri arasında düzenlenen suçların işlenmesi amacıyla, "a" bendinde sayılan hususların elde bulundurulmasının suç olarak düzenlenmesi gerektiği ifade edilmiştir. Elde bulundurmanın suç sayılabilmesi için taraf devletlerin yukarıda sayılanların belirli bir sayıda olmasına ilişkin ek şart getirebilecekleri hükmüne yer verilmiştir.

Maddenin 2. fıkrasına göre yukarıda sayılan hükümler, bu tür aygıt ya da programların, bir bilgisayarın korunması ya da test amacı gibi Sözleşmenin 2 ila 5. maddelerinde belirtilen suçların işlenmesi amacını gütmeyen meşru amaçlar için üretimi, satışı, kullanılmak için tedariki, ithal edilmesi, dağıtılması ya da diğer şekilde erişilebilir kılınmasını cezalandıracak şekilde yorumlanamaz

Aynı maddenin son fıkrasında ise, bilgisayar şifreleri, erişim kodlarının ya da benzer verilerin satışının, dağıtımının ya da diğer şekillerde erişilebilir kılınmasının cezalandırılabilmesine ilişkin hükümler saklı tutulmak kaydıyla, taraf devletlerin ceza mevzuatında birinci fıkrada düzenlenen hususları kapsam dışı bırakabileceği belirtilmiştir.

Sözleşmenin 7. ve 8. maddelerinde, bilgisayar aracılığıyla sahtekarlık ve bilgisayar aracılığıyla dolandırıcılık fiilleri düzenlenmiştir. Yedinci maddeye göre bilgisayar aracılığıyla sahtekarlık, *"verilerin açıkça okunabilir ya da anlaşılabilir olup olmadığına bakılmaksızın, bilgisayar verilerinin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi ya da hareket edilmesi amacıyla verilerin orijinalliğinin bozulması sonucunu doğuran, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme, fiillerin hukuka aykırı olarak kasten işlenmesi"* şeklinde tanımlanmıştır. 8. maddede düzenlenen bilgisayar aracılığıyla dolandırıcılık, sistemin işleyişine ekonomik bir yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması, bunların yanında sistemin işleyişine diğer herhangi bir müdahale seçimlik hareketler olarak düzenlenmiştir.

Sözleşmenin 9.maddesinde ise, içerikle ilgili suçlar başlığı altında çocuk pornografisine ilişkin hükümler yer almaktadır. Bu kapsamda yasaklanan fiiller, bilgisayar sistemleri aracılığıyla dağıtmak amacıyla çocuk pornografisinin üretilmesi (m. 9/1.a), sunulması veya temin edilebilir hale getirilmesi (m. 9/1.b) ; dağıtılması ya da iletilmesi (m. 9/1.c); kendisi ya da başkası için bilgisayar sistemi aracılığıyla elde edilmesi (m.9/1.d); son olarak, bilgisayar sistemi içerisinde ya da bilgisayar veri depolama ortamında çocuk pornografisi bulundurulmasıdır (m. 9/1.e). Maddede çocuk pornografisi, bir küçüğün cinsel içe-

rikli bir eylemde kullanılması, küçük gibi görünen bir kişinin cinsel içerikli bir eylemde kullanılması ya da bir küçüğün cinsel içerikli bir eylemde yer aldığını temsil eden gerçekçi imaj olarak tanımlanmıştır. Maddeye göre, küçük 18 yaşından küçükleri ifade etmekte, taraf devletlerin 16 yaşına kadar indirilebilmelerine imkan tanınmaktadır.

10. maddede ise, telif hakları ve bağlantılı hakların korunmasına ilişkin uluslararası düzenlemelerde yer alan hükümlerin etkin bir şekilde uygulanabilmesi ve de ihlallerin cezalandırılabilmesine ilişkin cezai hükümlere yönelik düzenlemelere yer verilmiştir.

Sözleşme incelendiğinde, bilişim suçlarının, Sözleşmedeki ifadesiyle siber suçların kapsamının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilişim sistemlerinin kullanılmasıyla ve özellikle İnternet'in yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmektedir. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşmeye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de bu grubu oluşturmaktadır. Sözleşmede bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da öngörebilecekleri belirtilmiştir.

Bilişim Suçları Açısından Türk Ceza Kanunu

Bilişim Alanında Suçlar

Bilişim Sistemine Yetkisiz Erişim (Bilişim Sistemlerine Hukuka Aykırı Girme)

Yetkisiz erişim suçuna ilişkin olarak TCK'nin 243. maddesinin birinci fıkrasında yer alan düzenleme şu şekildedir: (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

Siber Suç Sözleşmesi Madde 2 - Yasadışı Erişim

"Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir."

Sorun, veri ve veri işleme faaliyetinin yetkisiz kişilerin müdahalesinden uzak bir şekilde gerçekleştirilmesi olduğunda, özellikle, ağ üzerinden bilişim sistemleri ile iletişim kurma imkanlarının artması karşısında, bu tür faaliyetin ana unsurunu oluşturan bilişim sistemlerinin yetkisiz müdahalelerden uzak bir şekilde kullanımının sağlanmasının da önemi artmıştır. Bu açıdan, bilişim sistemlerinde yetkisiz üçüncü kişilerin işlem yapabilme yetkisini elde etme (en azından okuma yetkisi) anlamına gelen bilişim sistemlerine yetkisiz erişimin cezalandırılabilir bir fiil olarak nitelendirilmesi yoluna gidilmiştir.

Bilişim sistemleri aracılığıyla gerçekleştirilebilen diğer ihlaller esas alındığında bilişim sistemine erişim, diğer birçok suçun işlenmesinde bir araç olarak gerçekleşebilmektedir. Bu açıdan, yetkisiz erişimin ayrı bir suç olarak düzenlenmesi, suç olarak düzenlenen diğer fiilleri gerçekleştirme olanağına sahip olan kişinin, somut durumda bunları gerçekleştirip gerçekleştirmediğine bakılmaksızın cezalandırılabilmesine olanak sağlamaktadır. Yetkisiz erişim fiilinin esas alındığı düzenlemelerde ve bu doğrultuda 243. maddede de düzenlendiği şekliyle, sisteme herhangi bir zarar verip verilip verilmediğine bakılmaksızın failin cezalandırılmaktadır ve bu haliyle tehlike suçu niteliğindedir.

Suçun Hukuki Konusu

Genel Olarak

Bilişim sistemlerine yetkisiz erişim suçuyla, söz konusu sistemlerin sahibi ya da kullanıcılarının ilgili sistem üzerinde tasarruf edebilmelerine ilişkin yetkinin korunması amaçlanmıştır. Bu tasarruf yetkisi, genel olarak bir bilgisayar sistemine kimlerin erişim sağlayabileceğinin ya da diğer bir ifade ile girebileceğinin, sistem sahibi ya da sistem üzerinde hak sahibi olan diğer kişiler tarafından belirlenebilmesi anlamındadır. Bu şekliyle, dışa dönük bir nitelik taşıyan tasarruf yetkisinin görünümü, kimi düzenlemelerde kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ve dolayısıyla mameleki bir değerin korunması, kimi düzenlemelerde ise, özel hayatın gizliliğinin belirli bir yönünün korunması şeklinde ortaya çıkmıştır.

Mameleki Bir Değerin Korunması Açısından Siberalan

Malvarlığının ve dolayısıyla kişiye ait mameleki değerin korunmasına ilişkin yaklaşım, ABD'de özellikle federe devletlerde (eyalet) kendisini göstermektedir. Bu devletlerin ilgili düzenlemelerinde verinin kendisi eşya olarak kabul edilmiş ve dolayısıyla verinin ele geçirilmesi suçu da mameleki değerin korunmasına yönelik bir suç olarak düzenlenmiştir. Aynı yaklaşım, yetkisiz erişim suçu bakımından da geçerliliğini korumaktadır. Bu husus, bir yönden yetkisiz erişim suçunun özellikle Federe devletlerde ceza mevzuatları içerisinde düzenlendiği yerde etkisini göstermektedir. Diğer bir yönden, yetkisiz erişim suçunun kıyasen incelendiği ve başkasının mülküne girilmesi olarak çevrilebilecek olan "criminal trespass" suçunun niteliği göz önünde tutulduğunda, ABD ve özellikle federe devletlerde yetkisiz erişim suçu ile mameleki değerin korunmak istendiği sonucuna götürmektedir. Burada özellikle vurgulanması gereken nokta, sanal bir alanın varlığı noktasından hareket edilmiş olmasıdır.

Gerçek ve sanal alan ayırımı Avrupa Konseyi Sibersuç Sözleşmesinde de yer almıştır. Sözleşmenin açıklayıcı raporunda da (gerekçesi) siber alan ya da sanal alan *"Enformasyon teknoloji alanındaki hızlı gelişmenin modern toplumun her bölümünde doğrudan etkiler doğurduğu, dünyanın herhangi bir yerinden herhangi bir kişinin erişim sağlayabileceği internet de dahil olmak üzere enformasyon super-otoyollarının ve ağlarının ortaya çıkışının bu gelişmeyi hızlandırdığı. Enformasyon ve iletişim servislerine bağlanılması suretiyle kullanıcıların bir çeşit ortak alan yarattıkları ve bunun siber alan olarak adlandırıldığı..."* şeklinde ifade edilmektedir.

Bu durumda, gerçek alan ve sanal alan ayırımında, Sözleşmenin açıklayıcı raporunda belirtilen ortak alan içinde, kişiye ait ya da kişinin tasarrufu altında olan bir alanın yetkisiz üçüncü kişilerin müdahalesinden korunması söz konusu olmaktadır. Bu yaklaşım ise genel olarak gerçek alan ve sanal alan ya da siber alan şeklinde ikili bir ayırıma dayanmaktadır.

Özel Hayatın Gizliliğinin Korunması Kapsamında Siberalan

Sanal alan gerçek alan ayırımı, İtalyan Ceza Kanununda düzenlenen yetkisiz erişim suçunda da, suçun hukuki konusu bakımından etkisini göstermiştir. Sisteme yetkisiz erişim suçu, Kanunun *"kişilere karşı suçlar"* düzenleyen 12. bölümünde bireysel özgürlüklere karşı suçlar kapsamında, *"konut dokunulmazlığına karşı suçlar"* arasında 615 ter maddesinde düzenlenmiştir. İtalyan Ceza Kanunun 615 ter maddesinde, *"bilişim"* veya *"telematik"* sistemlerine hukuka aykırı girme veya hak sahibinin açık veya zımni rızası hilafına sistemde kalmaya devam etme fiilleri cezalandırılmaktadır.

Konut dokunulmazlığına karşı suçlar arasında düzenlenen yetkisiz erişim suçu ile ilgili olarak madde gerekçesinde, *"bilişim"* ve *"telematik"* sistemleri ile İtalyan Anayasasının 14. maddesince güvence altına alınan ve daha önemli hallerde İtalyan Ceza Kanunun 614. ve 615. maddeleri ile korunan ilgili kişiye ait saygı alanı kapsamında olan konutun düşünsel olarak genişlediği ifade edilmiştir.

Bu gerekçe incelendiğinde, özel hayatın gizliliği kapsamında fiziksel bir alan olarak korunan konut yanında bilgisayar sistemlerinin kullanılmaya başlanması ile birlikte konutun düşünsel olarak genişlediği ifade edilmekle, düşünsel bir alanın varlığı da vurgulanmaktadır. Bu ikili ayırım doğrultusunda sanal alan içinde kişinin tasarrufunda bulunan alan, ABD'de genel olarak malvarlığına ilişkin bir değerin korunması olarak karşımıza çıkmakta iken, İtalya'da, özel hayatın gizliliğinin korunması kapsamında, konutun bir uzantısı olarak algılanmış ve yetkisiz erişim suçu, konut dokunulmazlığının elektronik ihlali olarak ifade edilmiştir.

Sırrın Korunması Açısından Verinin Gizliliğinin Dolaylı Olarak Korunması

Yetkisiz erişim suçunun hukuki konusunun belirli bir alan –siber alan- açısından malvarlığının ve kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ya da özel hayatın gizliliği kapsamında konut dokunulmazlığının korunması ile aynı yönde olduğu görüşleri yanında, bu suçun hukuki konusu ile ilgili olarak ileri sürülen diğer bir görüş, yetkisiz erişim suçunun sırrın korunmasına yönelik olduğudur.

İtalyan Ceza Kanununda yetkisiz erişim suçunun düzenlendiği yer ve hukuki konusuna ilişkin ileri sürülen eleştirilere göre, bilişim sistemleri yukarıda aktarıldığı üzere konut ve konutun devamı olan bir sanal alan yaratmamaktadır. Bu açıdan, bilişim sistemlerine yetkisiz erişim suçu ile korunmak istenen husus, bilişim sistemleri içerisinde bulunan veri hakkında yetkisiz üçüncü kişilerin bilgi sahibi edinememesi olup, bu husus konut dokunulmazlığının da dâhil olduğu özel hayatın gizliliğinin korunması bakımından başka bir yönü gündeme getirmektedir. Bu da özel hayatın gizliliğin korunmasının bir yönü olarak sırrın korunmasıdır. Bilişim sistemleri açısından, sırrın korunması, bilişim sistemleri içerisindeki verilere erişimin korunması olarak ortaya çıkmakta ve söz konusu durum verinin gizliliğinin korunmasını gündeme getirmektedir.

Söz konusu yaklaşım, sırrın korunması esasından hareketle düzenlenen verinin ele geçirilmesine ilişkin suçlarla hukuki konu bakımından paralellik arz etmektedir. Verinin ele geçirilmesine ilişkin suçlarda verinin gizliliğine yönelik doğrudan bir koruma sağlanırken, bilişim sistemlerine yetkisiz erişime ilişkin düzenlemelerde bilişim sistemlerinin gizliliğinin korunması dolayısıyla bilişim sistemleri içerisindeki verinin gizliliği korunmakta; verinin gizliliği bakımından, sırrın korunması anlamında, dolaylı bir koruma sağlanmaktadır.

Türk Ceza Kanunda Düzenlenen Yetkisiz Erişim Suçunun Hukuki Konusu

243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu ile ilgili olarak çeşitli görüşler ileri sürülmüştür. Bu görüşlerden bir kısmında, 244. maddede düzenlenen suçun hukuki konusunun özel hayatın gizliliğinin korunması olduğu ifade edilmiştir. Kurt, bilişim sistemine yetkisiz erişim suçu ile sistem sahibinin kişisel alanına girildiğini ifade etmiştir. Yazara göre; *"Bilişim sistemine girme ve orada kalmaya devam etme suçunda korunan hukuki yarar, özel hayatın gizliliği ve sırların masuniyeti olarak belirlenebilir. Bilişim sistemi ve içinde bulunan veriler, programlar sistem sahibinin özel alanı da bulunmaktadır. Bu suç ile bu alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır. Bilişim sistemi sahibinin kişisel alanına girilmektedir. Hak sahibi izin vermedikçe bu alana girilmesi mümkün değildir. Anayasanın 20. maddesindeki 'özel hayatın gizliliği'ne ilişkin maddesine paralel bir hüküm olarak karşımıza çıkmaktadır."* Yazarın bu görüşü incelendiğinde, bilişim sistemlerinin kullanılması ile birlikte, ABD'de federe devletlerde başkasının mülküne girme ile aynı yönde gelişen, İtalyan Ceza Kanununda konut dokunulmazlığının elektronik ihlali şeklinde somutlaştırılmak istenen, gerçek alanın yanında bir siber alanın var olduğu görüşü ile paralellik arz etmektedir.

Biçkin ise, 243. maddede düzenlenen suçun hukuki konusunun karma bir nitelik gösterdiğini ve devamında *Kurt* ile aynı yönde ilk olarak *"bireyin özel hayatının korunduğunu"* belirtmektedir. Yazar, özellikle 2. fıkrada yer alan düzenlemeyi esas alarak, *"malvarlığının"* da korunan hukuki menfaatler arasında olduğunu, çünkü bu fıkrada bedeli karşılığında yararlanılabilen sistemler hakkında ilgili suçun işlenmesi halinin düzenlendiğini vurgulamaktadır.

TCK'nin 243 maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun karma bir nitelik taşıdığı, başka bir açıdan, *Dülger* tarafından da ifade edilmiştir. Yazar, yetkisiz erişimin engellenmesiyle sistemin malik ya da kullanıcıları olarak sistemden faydalanan kişilerin birçok sayıdaki farklı türden çıkarları koruma altına alındığını belirtmektedir. Bu kişilerin çıkarlarının, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabildiğini ifade etmiştir. Yazar, farklı türden çıkarlar olarak ifade ettiği bu değerlerin üstünde ve bu değerleri kapsayacak şekilde *"bilişim sisteminin güveliği"*nin korunmasının asıl hukuki konuyu oluşturduğunu belirtmiştir. Aktarılan bu görüş ise, yukarıda belirtildiği üzere, Siber Suç sözleşmesinin 2. maddesinde düzenlenen yetkisiz erişim suçu ile ilgili olarak Sözleşmenin açıklayıcı raporundaki gerekçe ile paralellik arz etmektedir.

Bu kapsamda TCK'nin 243. maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun saptanmasında TBMM Genel Kurul görüşmelerinde 244. maddeye ilişkin değişiklik teklifi ve bu teklif hakkındaki görüşlerin bilinmesi önemlidir. Söz konusu değişiklik teklifine ilişkin görüşler maddenin hangi hukuki konuya yönelik olarak düzenlenmek istediğini göstermesi bakımından önemlidir.

Nitekim, 243. maddeye ilişkin TBMM Genel Kurulunda yapılan görüşmelerde suçun unsurlarına ilişkin bir değişiklik teklif edilmiş ve bu teklif kabul edilerek madde son şeklini almıştır. Suçun unsurlarında yapılması istenen değişikliğe ilişkin "Biliyorsunuz bir de bilgisayar sistemin bozan hackerlar var, onlar size bir şey gönderdi, üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz. Burada da -hazırladığımız taslakta- girme ve orada kalma şerhini koyduk; çünkü, bu bir kasttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama girdiniz kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte biz tasarıda, buraya açıklık getirdik. Bağlantılı olarak 244'te de bir açıklık getiriyoruz." gerekçesi ileri sürülmüştür.

Aynı değişiklik teklifinde 243. maddenin son fıkrasında düzenlenen ağırlatıcı nedenin varlığı halinde öngörülen cezanın miktarına ilişkin olarak şu görüş dile getirilmiştir: *"Çocuğunuz 16 yaşında; geldi, bilişim sistemine girdi ve istemeden bir değişikliğe ya da veri kaybına neden oldu. Biz, şu andaki tasarıda diyoruz*

ki, bu kişiyi iki yıldan dört yıla kadar mahkûm edelim; ama, bir sonraki maddede diyoruz ki, bozma niyeti olana, bozma amacıyla, veriyi değiştirme amacıyla, sistemin tamamına zarar verme amacıyla bu eylemi işleyene de bir yıldan üç yıla kadar ceza verelim; hazırlanan metin bu şekilde. Şimdi, bir şey düşünün; suçu işleyen kişi, hâkimin karşısına geçecek, bu işi bilmeyerek yaptıysa, daha az ceza almak için "hâkim bey, benim kastım vardı, bu işi bilerek, isteyerek yaptım" diyecek ve bunun karşılığında daha az bir ceza alıp kurtulacaktı. Fiilde dengesizlik var."

Her iki görüş incelendiğinde, 243. maddenin hukuki konusu ile ilgili olarak özel hayatın gizliliğinin ya da bu kapsamda sırrın korunmasına ilişkin tercihin esas alınmadığı görülmektedir. Bunun yerine, bilişim sisteminin işleyişinin korunması açısından bilişim alanında işlenen suçların konusunu oluşturan hareketler arasında önem dercesine göre bir ayırım yapılmıştır. Bu açıdan, söz konusu fiiller içinde en hafifi sisteme girilmesi olarak kabul edilmektedir. Her ne kadar hatalı olarak suçun manevi unsuru kapsamında sadece girmenin suç sayılması çeşitli sakıncalara yol açacağı belirtilmişse de gerekçenin devamı incelendiğinde girmenin önem derecesi bakımından en alt sırada olduğu ve en önemli hususun sistemin bozulması olarak ifade edildiği görülmektedir.

Bu kapsamda söz konusu suçla korunan hukuki değere yönelik olarak farklı görüşler ileri sürülmektedir.

Yetkisiz Erişim Suçunun Maddi Unsuru-Sisteme Girme ve ya Orada Kalmaya Devam Etme

Yaygın olarak *"illegal access" "yetkisiz veya hukuka aykırı erişim"* olarak adlandırılan bu suçun maddi unsurunu oluşturan ilk hareket sisteme erişim (access) olarak düzenlenmektedir. Avrupa Konseyi Sibersuç Sözleşmesi'nin İngilizce metninde de bu suç *"illegal access"* (yetkisiz/hukuka aykırı erişim) olarak adlandırılmaktadır. Aynı şekilde ABD ve İngiltere'de bu suç yetkisiz erişim olarak adlandırılmakta ve bu suça ilişkin düzenlemelerde suçun maddi unsuru, sisteme erişim (access) olarak düzenlenmektedir.

Parker, Türkçeye erişim olarak çevrilen *"access"* teriminin ceza hukuku alanında karışıklıklara yol açabileceğini, bu terimin fiziksel bir alana erişilmesini ya da girilmesini çağrıştırdığını, fakat bilgisayara girişin bu açıdan imkânsız olduğunu belirtmektedir. Bilgisayar sistemlerinin işleyişinde, bilgisayara sinyal gönderilmesi ve bunun sonucunda, bilgisayarın, bu sinyale belirli bir programın çalışması ve sıklıklı bir programın başlaması şeklinde cevap vermesinin söz konusu olduğunu ifade etmektedir. Bu nedenle, kullanılması gereken doğru terimlerin, *"bilgisayara yaklaşılma (approach) ya da enformasyona girilmesi"* ve bilgisayarın *"kullanılması"* olduğunu vurgulamaktadır.

Günümüzde yaygın olarak kullanılan Windows ve Unix tabanlı işletim sistemleri açısından değinilecek olursa, en az bir yönetici hesabı ve bunun yanında sistemin teknik olarak elverdiği sayıda oluşturulabilecek kullanıcı hesabı bulunmaktadır. Kullanıcılar kimi zamanlarda yönetici yetkilerine de sahip olabilmesine rağmen, özellikle çok kullanıcılı sistemler açısından genel olarak sınırlı yetkiye sahip olabilmektedir. Sistem içerisinde kullanıcıların yetkilerinin belirlenmesi genel olarak sistem içerisinde yer alan yönetici tarafından gerçekleştirilmektedir. Bu açıdan yönetici, sistem içerisindeki kullanıcıları belirli dizin, klasör ya da dosyalara erişim yani genel olarak verilere erişim bakımından sınırlandırabileceği gibi bununla birlikte belirli işlemlerin yapılması bakımından da sınırlandırabilir. Özellikle, çok kullanıcılı sistemlerde kullanıcıların yetkilerinin belirlenmesi sistem kaynaklarına kimlerin ne şekilde erişebileceğinin önceden tespit edilmesi bakımından önem arz etmektedir.

Yönetici (administrator ya da root), bir bilgisayar sisteminde, sistemin teknik olarak elverdiği ölçüde her türlü yetkileri kullanabilir. Yönetici dışındaki kullanıcılar ise, yönetici ile aynı yetkilere sahip olabileceği gibi bunun yanında daha sınırlı bir yetkilendirme söz konusu olabilir. Bu durum genel olarak yönetici ve diğer kullanıcıların ilgili sistem üzerindeki yetkileri olarak karşımıza çıkmaktadır. Bu yetkiler ise genel olarak iki grupta toplanabilir. Bunlardan birincisi genel olarak sisteme *"log on (oturum açma)"* yetkisi diğeri ise kullanıcıların sistem içerisinde işlem yapma (okuma-yazma-çalıştırma) yetkisidir.

Bu ayrım içerisinde, oturum açma "log on" yetkisi, kimlerin sistemi kullanma yetkisi olduğunu göstermektedir. Bu açıdan bir sistemde kimlerin oturum açma yetkisinin olduğunun belirlenmesi kimlerin sistemde işlem yapabileceğinin tespiti anlamına gelmektedir. Bu yetki aynı zamanda diğer yetkilerin kullanılmasına ilişkin bir ön koşul olarak ortaya çıkar.

Söz konusu yetkiye sahip olan kullanıcının sistemde oturum açmasından sonraki konumu ise, sistem içerisindeki işlem yapma yetkileri gündeme getirir. Bu ise, genel olarak sistem aracılığıyla ya da içerisinde var olan veri ve programlar üzerinde ya da bunlar aracılığıyla işlem yapılabilmesi yetkisi anlamına gelmektedir. Sistemde oturum açma yetkisi olan kullanıcıların sistemde hangi işlemleri yapabileceği, kullanıcı hesabına ya da kullanıcı hesabının bağlı bulunduğu gruba göre sınırlandırılabilir. Bu nedenle, bir bilgisayar sisteminde işletim sisteminin elverdiği ölçüde değişik düzeyde işlem yapabilme yetkisine sahip olan kullanıcı hesaplarının oluşturulması mümkündür.

Bu doğrultuda, yetkisiz erişim fiilinde failin amacı kullanma yetkisi olmadığı bir sistem üzerinde hukuka aykırı olarak kullanma yetkisini sağlaması yani sistemde oturum açması suretiyle en azından okuma yetkisinin elde edilmesi olarak özetlenebilir. Bu durum sistem içindeki yetkilerin elde edilmesi bakımından yönetici düzeyinde ya da kullanıcı düzeyinde erişim olarak adlandırılabilmektedir. Yetkisiz erişim, sistemi kullanmaya yetkili kullanıcılara ait erişim kodlarının (kullanıcı adı, sifre vb.) ele geçirilmesi suretiyle gerçekleştirilebileceği gibi sistem açıklarından faydalanılması ya da sistemde açık yaratılması suretiyle de gerçekleştirilebilir. Ayrıca, sisteme yetkisiz erişim, başka bir bilgisayarın kullanılması suretiyle hedef bilgisayara iletişim araçları aracılığıyla erişilmesi suretiyle gerçekleştirilebileceği gibi, hedef bilgisayarın doğrudan kullanılması yoluyla da gerçekleştirilebilir.

Özetle teknik olarak oturum açma (log on) yetkisi olarak da adlandırılan ve kimlerin sistemde oturum açabileceğini belirleyen yetkinin ihlal edilerek sistemde oturum açma, TCK'nin 243. maddesinde belirtilen hukuka aykırı girmeyi oluşturur. Bu madde kapsamında, sisteme hukuka aykırı olarak elde edilen erişim kodlarından yararlanılması suretiyle girilmesi, sistemdeki açıklardan faydalanılarak ya da sistemde açıklar yaratılarak girilmesi arasında bir fark yoktur. Aynı şekilde sistemin tamamına ya da bir kısmına girilmesi bakımından bir farklılık yoktur.

Yukarıda sistemi kullanma ya da daha teknik bir ifade ile sistemde oturum açma yetkisi olmayan bir kişinin sisteme girmesi olasılığı incelenmiştir. Burada incelenmesi gereken diğer husus, genel olarak bilişim sisteminin bütününe ya da bir kısmına girmeye yetkili olan bir kişinin sisteme kendisine ait oturum açma yetkisinin ilişkilendirildiği kullanıcı hesabından başka bir hesap ile sisteme girmesi olasılığıdır.

Burada özellikle iki olasılık açısından değerlendirme yapılması gerekir Bunlardan birincisi, sistem içerisinde işlem yapma yetkisinin kapsamı diğeri ise, maddede açıkça vurgulandığı üzere, bilişim sistemi içerisinde sistemin belirli kısımlarına girişe ilişkin yetkilendirme olarak karşımıza çıkmaktadır.

Sistem içerisinde işlem yapma yetkisinin kapsamı bakımından incelendiğinde, sistem içerisinde işlem yapma için farklı yetkilendirme söz konusu ise, kural olarak sisteme girme yetkisine sahip bir kişinin başka bir kullanıcı hesabı kullanarak sisteme girmesi durumunda yetkisiz erişim gerçekleşir. Bu durumda, sistem içerisinde sınırlı işlem yapma yetkisine sahip bir kullanıcının daha üst düzeyde işlem yapma yetkisine sahip bir kullanıcı hesabı aracılığıyla sisteme girmesi halinde hukuka aykırı bir girişten bahsedilir. Aynı düzeydeki kullanıcılar bakımından ise, işlem yapma yetkisi bakımından bir farklılaştırma yapılıp yapılmadığı sisteme girmenin hukuka aykırılığın tespitinde ölçüt teşkil eder.

Madde metni incelendiğinde sadece sistemin bütününe girişten bahsedilmemekte bunun yanında sistemin bir kısmına girilmesi hali de suç olarak öngörülmektedir. Belirli bir kısma girilmesinin sınırlandırılması, yukarıda belirtildiği üzere, tek bir sistem içerisindeki yetkiler bakımından okuma,

yazma ve çalıştırma yetkileri içerisinde en azından okuma yetkisinin de verilmemiş olması anlamına gelmektedir. Bu ise, yukarı da belirtildiği üzere, oturum açma yetkisi kapsamında düşünülebilir, çünkü olan oturum açma yetkisi sistemde işlem yapma yetkisinin önkoşuludur. Sistem içerisindeki kısım ve bu kapsamda düşünülebilecek veri bakımından işlem yapma yetkilerinin kullanımı konusunda bunlar üzerinde en azından okuma yetkisinin bulunması şarttır.

Bunun dışında, başkasına ait herhangi bir kullanıcı hesabını kullanmadan sistem açıklarında yararlanılması gibi diğer yollarla sistem içerisinde girişin sınırlandırılmış olduğu bir bölüme girilmesi, yetkisiz erişimi oluşturur.

243. maddede düzenlenen suçun gerçekleşmesi için sistemin bütününe ya da bir kısmına hukuka aykırı olarak girilmesi ya da hukuka aykırı olarak, sistemde kalınmaya devam edilmesi yani var olan yetkinin sonlandırılmış olmasına rağmen sisteme erişimi gerekmektedir. Sisteme girme veya orada kalmaya devam etme, , 243. maddede düzenlenen yetkisiz erişim suçunun maddi unsurunu oluşturmakta olup bu haliyle son değişikle birlikte seçimlik hareketli suç haline getirilmiştir.

Suça Etki Eden Nedenler

Yetkisiz erişim suçunun düzenlendiği 243. maddenin 2. fıkrasında, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, cezada indirim sebebi olarak öngörülmüş bunun yanında son fıkrada sistemin içerdiği verilerin değişmesi ve de yok olması hali ise ağırlatıcı neden olarak düzenlenmiştir.

- Yetkisiz Erişim Suçunun Bedeli Karşılığı Yararlanılabilen Sistemler Hakkında İşlenmesi

243. maddenin 2. fıkrasında yetkisiz erişim suçunun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi cezada indirim sebebi olarak düzenlenmiştir. Kanunun madde gerekçelerinde bedeli karşılığı yararlanabilen sistemlerin ne olduğu ve neden bu şekilde bir cezada indirim sebebinin öngörüldüğü hakkında herhangi bir gerekçeye yer verilmemiştir.

Karagülmez, maddede yer alan bu ifadenin yoruma açık olduğunu, belirli bir ücret karşılığında hizmet veren web sayfalarının bu kapsamda düşünülebileceğini belirtmektedir. Yazar, internet kafe ve benzeri yerlerde bedeli karşılığında sistemin kullanılmasının bu kapsamda düşünülemeyeceğini ifade ederek maddede sistemin kullanıldığı mekanın değil sistem içerisindeki elektronik yapıda sunulan ücretli hizmetleri vurguladığını savunmaktadır. Yazara göre, belirli bir süre İnternet bağlantı servisinin sağlanması da bu fıkra kapsamında değildir.

Yazıcıoğlu ise, bu fıkrada düzenlenen hafifletici sebebi, ücreti karşılığı hizmet veren sistemlere girilmesi şeklinde yorumlamakta ve devamında ve bu düzenlemenin yetkisiz erişim suçunun uygulanmasının genişliğinden doğacak sakıncaları gidermesi bakımından isabetli olduğunu ifade etmektedir.

- Yetkisiz Erişim Fiili Sonucunda Sistemin İçerdiği Verinin Değişmesi ya da Yok Olması

243. maddenin 3. fıkrasında sisteme yetkisiz erişim sonucunda sistemin içerdiği verinin değişmesi veya yok olması ağırlatıcı neden olarak düzenlenmiştir. Bu fıkrada, TCK'nin 23. maddesinde düzenlendiği şekliyle, neticesi sebebiyle ağırlaşan bir suç söz konusu olup ağırlatıcı nedenin uygulanabilmesi için failde verinin değiştirilmesi ya da yok edilmesi yönünde bir kastının olmaması gerekmektedir. Bu fiilin kasıtlı olarak işlenmesi halinde, 244. maddenin 2. fıkrasında yer alan hüküm gündeme gelecektir.

Bilişim sistemlerinde yer alan ve bunların işleyişini sağlayan ana yazılımlar olarak karşımıza çıkan işletim sistemleri açısından değerlendirildiğinde, genellikle bu tür işletim sistemlerinin her açılışında ya da bu sistemlere girilmesinde günlük kayıtları içeren veriler gibi birçok veri sistemin işleyişine bağlı

olarak değişebilmektedir. Bu tür değişiklikler sistemin olağan çalışması için zorunlu ya da işlevsel olup bunlardaki değişiklik bu fıkra kapsamına girmemektedir.

Bu fıkrada öngörülen ağırlatıcı nedenlerin uygulanması açısından birinci ya da ikinci fıkrada düzenlenen sistemler bakımından maddede özellikle cezanın miktarı bakımından bir fark yaratılmamıştır. Fıkrada belirtilen durumun gerçekleşmesi halinde verilecek ceza, yetkisiz erişimin konusunun bedeli karşılığı sistemler olup olmamasına bakılmaksızın altı aydan iki yıla kadar hapis cezasıdır.

Araya Girme

243. maddenin son fıkrasına 6698 sayılı Kanun ile *" Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."* hükmü eklenmiştir. Sonradan eklenen bu düzenleme Siber Suç Sözleşmesinde yetkisiz erişim suçundan bağımsız bir suç olarak düzenlenmesi öngörülen *"Yasadışı Araya Girme"* suçuna ilişkin düzenlemenin TCK'deki karşılığı olarak yer almaktadır.

Siber Suç Sözleşmesi Madde 2 - Yasadışı Araya Girme

"Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi içi hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasam tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun sahtekârlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir."

Diğer nitelikli hallerden farklı olarak bu düzenlemenin yetkisiz erişim suçunu ağırlaştıran bir neden olmaktan çok farklı unsurları içeren bir suça yönelik olduğu görülmektedir. Nitekim düzenlemede fiilin sisteme girmeksizin yapılması gerekliliği getirilmiştir. Aslında bu haliyle bu düzenleme kişiler arasındaki haberleşmenin gizliliğini ihlal suçunun tamamlayıcısı olarak da görülebilir. TCK'nin 132. maddesinde düzenlenen suçun oluşması için kişiler arasında bir haberleşmenin varlığı aranmakla birlikte bilişim sistemleri aracılığıyla yapılan iletişimde taraflar her zaman için hazırda bulunmamakta iletişim kimi zamanlar insan-insan, kimi zamanlar insan-sistem ya da sadece sistem- sistem arasında gerçekleşebilmektedir. Söz konusu düzenleme ile bu hususa ilişkin kişiler arasındaki haberleşmenin gizliliği ihlal suçlarının unsurlarında ortaya çıkan eksiklik tamamlanmaktadır.

Bilişim Sistemine ve Veriye Müdahale

Genel Olarak

Sosyo-ekonomik yapı içerisinde faaliyetlerin ağırlıklı olarak bilgisayar sistemleri aracılığıyla veri işleme şeklinde gerçekleştirilmeye başlanması ve bu kapsamda sayısallaşmanın yoğunluğundaki artış, verinin gizliliğine ve içeriğine ilişkin koruma yanında veri ve bilişim sistemlerinin bütünlüğünün ve erişilebilirliğinin de korunmasını gündeme getirmiştir.

Verinin işlenmesi faaliyeti bilgisayar ortamında genel olarak bir veri grubunu oluşturan ve sistemin nasıl çalışması gerektiğine ve sistem içerisindeki verinin işlenmesine ilişkin komutları içeren programlar aracılığıyla gerçekleştirilebilmektedir. Programın kendisi genel olarak verinin düzenli ve öngörülen şekilde işlenmesini sağlayan bir veri grubunu oluşturmaktadır Veri işleme süreci içerisinde merkezi bir işleve sahip programlara müdahale edilmesi ise, her zaman için sistemin tamamen zarar görmesine yol açmamakla birlikte, veri işleme faaliyetinde aksamalara neden olabilmektedir. Bu açıdan veri işleme faaliyeti içerisinde, bunların da müdahalelerden korunması önem arz etmektedir.

Verinin işlenmesi faaliyetinin ana unsurunu oluşturan bilgisayar sistemlerinin işleyişinin ve bütünlüğünün korunmasının önemi de bu sistemlerin kullanımının yaygınlaşması ve faaliyetlerin bilişim sistemlerine bağlı olarak yapılmasına paralel bir şekilde artmaktadır[1].

Günümüzde bilgisayar sistemlerinin işleyişine, veri ve programlara müdahale genel olarak bunlara doğrudan erişim yoluyla gerçekleştirilebileceği gibi bu amacı güden kötü amaçlı programların kullanılması da yaygın bir yöntemdir. *"Virüs", "Solucan", "Mantık Bombaları", "DOS saldırıları[2]", "Truva Atı[3]"* yöntemleri günümüzde yaygın olarak kullanılan yöntemlere örnek gösterilebilir.

Bu gelişim sonucunda, veri ve programlara ve ayrıca bilgisayar sistemlerinin işleyişine müdahalenin engellenmesi zorunluluğu gündeme getirilmiş ve bunlara yönelik müdahaleler ceza mevzuatlarında düzenlenmeye başlanmıştır. Bu düzenlemelerde yeni ve önemli olan nokta, müdahalenin konusunun fiziki varlığı olmayan veri, program ya da genel olarak bilişim sistemlerinin yazılım unsuru olması ve sisteme yönelik müdahalelerin yazılım unsuruna yönelik olarak gerçekleştirilmesidir.

Sibersuç Sözleşmesinde bu husus veri ve programa müdahale esas alınarak, veriye müdahale 4. maddede, sisteme müdahale ise 5. maddede düzenlenmiştir. Sözleşmenin 4. maddesine göre *"veriye müdahale"*, bilgisayar verilerinin haksız bir şekilde kasten tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilmez kılınmasıdır. *"Bilgisayar sistemlerine müdahale"* ise Sözleşmenin 5. maddesinde bilgisayar verisi girişi yapmak, bilgisayar verisi göndermek, bilgisayar verilerini tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak suretiyle bilgisayar sistemlerinin işleyişini ciddi bir şekilde haksız ve kasten engellemek olarak tanımlanmıştır.

Sözleşmenin 4. maddesinde düzenlenmiş olan veriye müdahale fiilinin gerçekleşebilmesi için verinin bilgisayar sistemi içerisinde veya herhangi bir veri taşıyıcısında bulunması arasında fark yaratılmamıştır[4]. Sisteme müdahalede ise, bilgisayar sisteminin fiziki bir zarar görmesi aranmamış işleyişinin

---

[1]HEYMANN, s. 378

[2]İngilizce "denial of service" teriminin kısaltması olan "DOS" saldırılarında sistemin işleyemez hale gelmesi ya da sisteme erişimin engellenmesini amaçlayan hareketlere verilen genel bir ad olarak tanımlanması mümkündür. YILMAZ, s. 319 vd.

[3]Truva atı ise adını Truva efsanesinden almış olup genel olarak başka bir programın içine yerleştirilmiş olan kötü amaçlı kod ya da program olarak tanımlanabilmektedir. Bu haliyle bilgisayar program ve verilerine zarar verme gibi birçok amaçla kullanılabilmektedir. PARKER, s. 89,

[4]Bkz. Sözleşme açıklayıcı rapor, parag., 60, http://conventions.coe.int/Treaty/en/Reports/ Html/185.htm..

ciddi bir şekilde engellenmesi esas alınmıştır. Sisteme müdahalede genel olarak sistemdeki verilere müdahale edilmesi ya da sisteme veri iletilmesi suretiyle müdahale esas alınmış ve bu haliyle bilişim sisteminin fiziki varlığını oluşturan donanımına yönelik fiziksel müdahale kapsam dışı bırakılmıştır.

Sözleşmenin 4. maddesinde düzenlenen veriye müdahale ile ilgili olarak Sözleşmenin açıklayıcı raporunda, maddi varlığı olan şeylere yönelik zarar verme girişimlerine korumaya benzer bir şekilde bilgisayar veri ve programlarına yönelik fiillerin korunmak istendiği, bu açıdan verinin bütünlüğü ve düzgün bir şekilde çalışması ve kullanımın korunmasının amaçlandığı belirtilmektedir[5]. Veriye müdahale bakımından ilgili kişinin veri üzerinde, veriye yönelik olarak üçüncü kişiler tarafından gerçekleştirilecek müdahalelerden uzak bir şekilde tasarrufta bulunabilmesi sağlanmak istenmektedir. İlgili kişinin tasarruf yetkisi, verinin elde edilmesinde, üçüncü kişilerin verinin içeriğini öğrenmesinin ya da veriyi kullanmasının önüne geçilmesi şeklinde, dışa dönük olarak korunmakta iken; veriye müdahalede, veriyi elinde bulunduran kişinin veri üzerinde tasarruf yetkisinin, veriye müdahale edilerek ve bu şekilde zarar verilerek hukuka aykırı bir biçimde sınırlandırılması ya da ortadan kaldırılması anlamında içe dönük olarak korunmaktadır.

Türk Ceza Kanununda da söz konusu gelişimin etkisiyle 244. maddenin 1. fıkrasında sisteme müdahale, 2. fıkrasında ise veriye müdahaleye ilişkin düzenlemelere yer verilmiştir. Buna göre "(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

Suçun Hukuki Konusu Açısından Mala Zarar Verme Suçu Karşısında Sisteme ve Veriye Müdahale

Bilişim sistemine yönelik müdahaleler genel olarak veri ya da programlara müdahale açısından ele alınmakta, bu haliyle ilgili kişinin sistem üzerinde sistemin işleyişi bakımından tasarruf yetkisinin korunması veriye paralel bir şekilde ortaya çıkmaktadır. Nitekim Sözleşmenin açıklayıcı raporunda bu husus, sistemi kullanan kişilerin ya da sistem operatörlerinin sistemin sorunsuz bir şekilde işlemesindeki çıkarlarının korunduğu şeklinde ifade edilmiştir[6].

Bilişim sistemine ve veriye müdahale suçları yukarıda belirtildiği üzere genel olarak malvarlığına karşı suçlar arasında düzenlenmekte, hukuki konu esas alınarak yapılan düzenlemelerde ise mala zarar verme suçu ile aynı bölümde yer almaktadır. Özellikle hukuki konu bakımından esas alınan bu düzenleme tarzı, bu suçların hukuki konusunun tespitinde önem arz etmekte aynı zamanda bu suçların düzenlenmesinde klasik mala zarar verme suçunun kapsamı bakımından tartışmaları da beraberinde getirmektedir.

Bu kapsamda, klasik mala zarar verme suçunun düzenlenmesinde tarihsel süreç esas alındığında taşınır ya da taşınmaz malın fiziki yapısı ya da diğer bir ifade ile maddi varlığı esas alınarak bunlara yönelik zarar verici fiillerin engellenmesi amaçlandığı görülür. Mala zarar verme suçunun ceza kanunları

[5]Bkz. Sözleşme açıklayıcı rapor, parag. 60 http://conventions.coe.int/Treaty/en/ Reports/Html/185.htm
[6]Bkz. Sözleşme açıklayıcı rapor parag. 65 http://conventions.coe.int/Treaty/en/ Reports/Html/185.htm

içerisinde düzenlenmesinde ise, genel olarak bu suçun seçimlik hareketli bir suç olarak ele alınması yoluna gidilmiş ve bu yönde mala zarar verme suçunun maddi unsuru belirlenmiştir. Bu açıdan, TCK'de mala zarar verme suçu, Kanunun 152. maddesinde düzenlenmiş olup suçun maddi unsurunu oluşturan hareketler taşınır ya da taşınmaz malın kısmen ya da tamamen yıkılması, tahrip edilmesi, yok edilmesi, bozulması, kullanılmaz hale getirilmesi ve de kirletilmesi olarak karşımıza çıkmaktadır.

Bilişim sistemlerinin yaygınlaşması bu kapsamda veri işleme faaliyetinin artması ile birlikte, veri ya da programları hedef alan müdahalelerin önlenmesi ve bu tür fiillerin cezalandırılabilirliği sorununu ortaya çıkmıştır. Geleneksel mala zarar verme suçunda genel olarak taşınır ya da taşınmaz malda genel olarak fiziksel bir zarar arandığı ifade edilmekte, bilişim sistemlerine yönelik sistemin yazılım unsuruna müdahale bilişim sistemi bakımından her zaman için fiziksel bir değişikliğe yol açmamaktadır.

Sisteme müdahale bakımından ortaya çıkan sorun, sistemin yazılım ve donanım unsurlarından oluşması karşısında, sistemin fiziki yapısı yani donanımına yönelik olmayan yani yazılım unsuruna yönelik müdahaleler sonucunda sistemin fonksiyonlarını yerine getirememesinin mala zarar verme suçu kapsamında değerlendirilip değerlendirilemeyeceğidir. Bu durumda, suçun unsurlarını oluşturan hareketler ve bu hareketler sonucunda sistemin fiziki yapısında bir değişiklik olmadan sistemin işleyişine müdahale edilmiş olması bakımından soruna yaklaşmak gereklidir.

Bilişim sistemine yönelik müdahalelerde genel olarak sorun, sisteme müdahale teşkil edebilecek fiillerin mala zarar verme suçunu oluşturup oluşturmadığıdır. Bu tür müdahalelerde sistemin maddi varlığı ya da fiziki yapısında bir değişiklik olmamasına karşın sistemin fonksiyonlarını yerine getirememesi söz konusu olmaktadır. Bu haliyle mala zarar verme suçu açısından çözümlenmesi gereken husus, mala zarar verme suçunun unsurlarının bu tür fiilleri kapsayıp kapsamadığı noktasında toplanmaktadır. Sorunun bu noktada toplanması ise, diğer bir husus hakkında, yani bu tür fiillerin cezalandırılması ise korunmak istenen değerin yani bu suçun hukuki konusu bakımından bir çözüme ulaştırabilmektedir. Sorunun suçun maddi unsuru bakımından ortaya çıkması ve bunun çözümü için yeni bir suça yer verilmesi, mala zarar verme suçunun hukuki konusu ile bu suçun hukuki konusunun aynı olduğunu göstermektedir.

Nitekim sisteme müdahale bakımından yukarıda örnek olarak verilen ceza kanunlarında hukuki konu açısından bu yaklaşımın sergilendiği ve sisteme müdahaleye ilişkin ya veriye müdahale ile birlikte ya da veriye müdahaleden bağımsız bir suç şeklinde malvarlığının korunması merkezinde özel düzenlemelerin yapıldığı görülmektedir.

Verinin bütünlüğüne yönelik müdahalelerde ise sorun, yukarıda belirtildiği şekliyle mala zarar verme suçunun unsurları bakımından ortaya çıkmakla birlikte sorunun diğer bir yönü maddi varlığı olmayan verinin, genel olarak maddi varlığı olan taşınır ve taşınmaz malın esas alınarak düzenlendiği mala zarar verme suçunun konusunu oluşturup oluşturmadığıdır[7].

Verinin mal/eşya olarak kabul edilip edilemeyeceğine ilişkin sorun ise, veriye müdahaleye yönelik fiillerin cezalandırılmasında iki farklı yaklaşımın esas alınmasına yol açmıştır. Birinci yaklaşım, genel olarak ekonomik değer taşıyan verinin mal / eşya olarak kabul edilmesi şeklinde olup bu haliyle genel olarak kıta Avrupasında ve Türk Ceza Hukukunda mala zarar verme suçunun konusunun maddi varlığı olan taşınır veya taşınmaz mal olması şartından uzaklaşılmaktadır[8]. Diğer yaklaşım ise, veriye müda-

[7]SIEBER, s. 77.

[8]Enformasyonun bilişim sistemleri içerisinde temsil edici işlevi olan veriye müdahale özellikle verinin müdahalelerden korunması isteği ise öncelikli olarak, yukarıda ifade edildiği üzere günümüzde yaygın olarak enformasyon ya da bilişim toplumu olarak ifade edilen dönüşüm içerisinde verinin içerdiği enformasyonun başlı başına bir ekonomik değer olarak ortaya çıktığı görüşüne işaret etmekte ve ekonomik değere sahip veri saklandığı aygıtın işlevinden bağımsız olarak bir değer ifade etmektedir.

halenin verinin saklandığı diğer bir ifade ile bulunduğu mala yönelik bir zarar verme fiili olduğudur. Burada verinin saklandığı maddi mal esas alınarak, veriye müdahale ile verinin saklandığı malın işlevine müdahale edilmiş olduğu vurgulanmaktadır.

Bu doğrultuda ABD'de özellikle federe devletlerin (eyaletlerin) ceza mevzuatlarında genel olarak ekonomik değeri olan veri, mal olarak kabul edilmiş ve veriye müdahale de verinin mal olarak kabul edilmesi merkezinde düzenlenmiştir. Bu doğrultuda, sisteme ve veriye müdahale mala zarar verme kapsamında ele alınmış bunlara müdahale malvarlığına karşı suçlar olarak düzenlenmiştir.

İkinci yaklaşımda ise, verinin kendisi mala zarar verme suçu kapsamında suçun konusunu oluşturabilecek bir mal olarak kabul edilmemektedir. Burada, veriye yönelik müdahale, doğrudan mala zarar verme olarak kabul edilmemiş, sorun verinin saklandığı mal esas alınarak ele alınmıştır. Söz konusu yaklaşıma göre, veriye müdahale, verinin saklandığı mal, içerdiği veri ile birlikte bir işleve sahip olup veriye müdahale sonucunda bu işleve zarar verilmekte bu haliyle mala zarar verme söz konusu olmaktadır. Bu durumda, veriye müdahaleye ilişkin özel düzenleme yapılması bu duruma ilişkin bir açıklık getirilmesi amacını taşımaktadır[9]. Aynı yaklaşım, sisteme müdahale bakımından geçerli olup, her ne kadar sistemin yazılım unsuruna yönelik müdahale söz konusu olsa da, burada, sistemin işlevini yerine getirememesi söz konusu olduğundan, mala zarar verme suçunun oluştuğu söylenebilir.

Yukarıda aktarılan hususlar topluca değerlendirildiğinde, sistem ve veriye müdahaleye ilişkin suç ya da suçların, genel olarak mala zarar verme suçuna ilişkin hükümlerin özellikle sistemin yazılım yönüne ve veriye müdahale bakımından uygulanabilir olup olmadığı noktasında ortaya çıkan tartışmalar ve söz konusu soruna açıklık getirme isteği noktasından hareketle ortaya çıktığı görülmektedir. Bu haliyle de sisteme ve veriye müdahale genel olarak mala zarar verme kapsamında değerlendirilmektedir. Söz konusu fiillerin mala zarar verme kapsamında değerlendirilmiş olması, bu yöndeki fiillerin esas alındığı suçların hukuki konusu bakımından da bir işleve sahiptir.

Bu açıdan değerlendirildiğinde, ister ABD de federe devletlerde kabul edildiği şekliyle veri mal olarak kabul edilsin isterse verinin saklandığı malın işlevi ya da sistemin işleyişi esas alınarak soruna yaklaşılsın, mala zarar verme kapsamındaki fiiller söz konusu olmakta bu haliyle de malvarlığının korunması amaçlanmaktadır. Sisteme ve veriye müdahale fiillerine ilişkin suç, mala zarar verme suçu ile aynı hukuki konuya sahiptir.

Türk Ceza Kanununda Düzenlenen Bilişim Sistemine ve Veriye Müdahale Suçunun Hukuki Konusu

Yukarıda sisteme ve veriye müdahalenin hukuki konusu tartışılırken, bu fiillerin ayrıca suç olarak düzenlenmesinin nedenlerinden hareket edilmiş, bu kapsamda mala zarar verme suçunun unsurunda ve kapsamında ortaya çıkan tartışmalar bu suçun hukuki konusunun saptanmasında esas alındığı belirtilmişti.

TCK'nin gerekçesi incelendiğinde de sisteme ve veriye yönelik müdahale fiillerinin mala zarar verme suçuna göre özel bir düzenlemeye tabi tutulduğunun belirtildiği görülmektedir. Sisteme ve veriye müdahale ile ilgili olarak madde gerekçesinde *"...sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir."* denmektedir.

[9] Aktaran, SIEBER, s. 91–92

TCK'nin 244. maddesinin 1. ve ikinci fıkralarında düzenlenen *"sistem ve veriye müdahale"* suçunun da mala zarar verme suçu ile bağlantılı olarak incelendiği ve sisteme ve veriye zarar verme fiillerinin ayrıca özel olarak düzenlendiği yazarlarca da kabul edilmektedir . Bu doğrultuda 5237 Sayılı TCK ve 765 Sayılı TCK bakımından da sistem ve veriye müdahalenin genel olarak mala zarar verme suçu kapsamında değerlendirildiği ve 765 Sayılı Kanunun 525/b 1. fıkrasında ve TCK'nin 244 1 ve 2. fıkralarında düzenlenen sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olarak genel kabul gördüğü görülmektedir.

Sisteme ve veriye müdahalenin mala zarar verme suçunun özel şekli olduğu kabulü, aynı zamanda Türk Ceza Hukukunda da sisteme ve veriye müdahalenin hukuki konusu ile mala zarar vermenin hukuki konusunun birbirine paralel olduğu sonucuna götürebilmektedir.

Suçun Maddi Unsuru

Sistemin İşleyişini Engelleme ve Bozma

Genel Olarak

Sistemin işleyişini engelleme ve bozma TCK'nin 244. maddesinin 1. fıkrasında, *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* şeklinde düzenlenmiştir. 244. maddenin birinci fıkrasında suçun unsurunu oluşturan seçimlik hareketler *"bilişim sisteminin işleyişinin engellenmesi"* ve *"sistemin işleyişinin bozulması"*dır. Maddede yer aldığı şekliyle, bilişim sisteminin işleyişi genel olarak veri işleme faaliyeti anlamına gelmekte olup bu haliyle fıkrada veri işleme faaliyetinin engellenmesi ya da bozulması düzenlenmiştir.

Kanunda, engellemenin ve bozmanın tanımına yer verilmemiştir. Türk Dil Kurumu Sözlüğünde *"engellemek", "bir şeyin gerçekleşmesini veya yapılmasını önlemek"; "bozmak"* ise, *"bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek"* olarak tanımlanmaktadır. Bu kapsamda bilişim sisteminin işleyişinin engellenmesi sistem aracılığıyla veri işleme faaliyetinin gerçekleştirilmesinin engellenmesi, bilişim sisteminin bozulması ise sistemin veri işleme faaliyetini yapamayacak hale getirilmesi olarak tanımlanabilir.

Nitekim, yazarlar tarafından sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiği ifade edilmiştir[11]. Sistemin tamamen çalışamaz hale gelmesi[12], sistemin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması[13], haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılmasının[14] sistemin işleyişini bozma anlamına geleceği ifade edilmiştir[15].

---

[10]TCK'nin 244. maddesinde düzenlenen sisteme ve veriye zarar verme suçunun mala zarar verme suçunun özel bir şekli olduğu hakkında ayrıca bkz, İnci BİÇKİN, Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları, Yargıtay Dergisi, C.32, Ocak – Nisan 2006, Sayı 1-2, s. 153. KARAGÜLMEZ, s. 187, KURT, s. 161.

[11]MERAN, s. 371; Aynı yönde DÜLGER, s. 234, KARAGÜLMEZ, s. 188.
Kurt, bilişim sisteminin engellenmesi halinde sistemin bozulmasının söz konusu olmayıp normalde yerine getirdiği fonksiyonları ifa etmesinin engellendiğini ifade etmektedir. KURT, s. 164.

[12]KURT, s. 164.

[13]MERAN, s. 371.

[14]KARAGÜLMEZ, s. 188..

[15]Sistemin işleyişinin engellenmesi açısından kimi yazarlarca sistemin elektriğinin kesilmesi durumunda da sistemin işleyişinin engel olma kapsamında değerlendirilebileceği ifade edilmiştir. Bkz. YAZICIOĞLU, Bilgisayar Suçları, s. 263. MERAN, s. 371.Mala zarar verme suçunda belirtildiği şekliyle mala zarar verilmiş olması nedeniyle başkasına zarar verme söz konusu olmakta, bu açıdan elektriğin kesilmesi suretiyle makinelerin işlemesinin engellenmesi örneğinde olduğu gibi doğrudan mala yönelik olmayan fiiller mala zarar verme kapsamında değerlendirilmemektedir. Bkz. TOROSLU, Ceza Hukuku Özel Kısım, s. 156.

Mala Zarar Verme Suçu Açısından Sistemin İşleyişinin Engellenmesi ve Bozulması

244. maddenin 1. fıkrası incelendiğinde, Sibersuç sözleşmesinden farklı olarak, sisteme müdahalenin sistemin yazılımına yönelik olarak sisteme veri gönderilmesi, yerleştirilmesi gibi hareketlerle gerçekleştirileceğine ilişkin bir düzenlemeye yer verilmediği görülmektedir. Burada tespit edilmesi gereken, sistemin yazılımına veri aracılığıyla müdahale halinin mi yoksa her türlü müdahalenin mi bu kapsamda değerlendirilmesi gerektiğidir.

Bu hususun tespiti, 244. maddenin 1. fıkrasının yazılıma yönelik fiiller yanında, maddi varlığı yani donanımına yönelik, mala zarar verme suçunun konusunu oluşturabilecek fiilleri de kapsayan özel bir suç mu olduğu; yoksa bu fıkranın sadece sistemin yazılım unsuruna yönelik fiillerin esas alınarak mala zarar verme suçunu tamamlayan bir suç olarak düzenlendiğinin tespiti bakımından önem arz etmektedir.

Yukarıda belirtildiği üzere, sisteme müdahale, sistemin özellikle yazılım kısmına müdahale teşkil eden fiillerin cezalandırılabilmesine ilişkin mala zarar verme suçunun unsurlarına açıklık getirilmesi amacıyla çeşitli ülke kanunlarında düzenlenmeye başlanmıştır. Sisteme müdahalenin bu kapsamda düzenlenmesi ise, öncelikli olarak yazılıma müdahalenin esas alınması suretiyle sisteme müdahale fiillerinin düzenlenmesi sonucuna götürmüş olup Sibersuç Sözleşmesinin 5. maddesinde de bu husus somutlaştırılmıştır.

244. maddede ise, sadece sistemin işleyişinin engellenmesi veya bozulmasından bahsedilmiş olup bunun sistemin yazılımına veri aracılığıyla müdahale edilerek gerçekleştirileceğine ilişkin açık bir hükme yer verilmemiştir. Madde ile ilgili yaygın kabul, sisteme veri yoluyla müdahale yanında sistemin işleyişini engelleyen ya da bozan her türlü müdahalenin de bu madde kapsamında değerlendirilmesi yönündedir. Bunun yanında, 244. maddenin 1. fıkrasının sadece donanıma yönelik müdahaleleri kapsadığı görüşü de ileri sürülmüştür.

Bu fıkra kapsamında hangi tür fiillerin düzenlendiğinin belirlenmesi, TCK'de sisteme müdahalenin mala zarar verme suçu karşısındaki konumunun saptanması bakımından önemlidir. Eğer bu fıkranın yazılıma yönelik veri aracılığıyla gerçekleştirilen fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçu bakımından 244. maddenin birinci fıkrasında, suçun konusunun sistemin yazılım yönünün esas alındığı sonucuna varılabilecektir. Fakat bu fıkranın donanıma ve yazılıma yönelik fiilleri bir bütün olarak kapsadığı ya da donanıma yönelik fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçuna göre bilişim sistemini bir bütün olarak konu edinen özel hüküm olduğu sonucuna varılabilecektir.

244. maddenin 1. fıkrasında yer alan düzenlemenin mala zarar verme suçunu tamamlayıcı nitelikte bir düzenleme olduğu kabul edilecek olursa, geleneksel olarak taşınır ya da taşınmaz malın maddi varlığına yönelik hareketleri kapsayan mala zarar verme suçu ile sisteme müdahale bir bütün halinde uygulanabilecektir. Bu kapsamda, yazılıma yönelik hareketler sonucunda sistemin işleyişinin engellenmesi ya da bozulması halinde 244. maddenin 1. fıkrası, sistemin tahrip edilmesi, yok edilmesi gibi donanıma yönelik fiilleri kapsayan maddi varlığına yönelik fiillerde ise, TCK. nun 151. maddesi uygulama alanı bulacaktır. Bu durumda, sorun, cezaların miktarında ve 3. fıkrada düzenlenen ağırlatıcı nedenlerin uygulanmasında ortaya çıkmaktadır.

244. maddenin 1. fıkrasının 151. maddeye göre, hem donanıma hem de yazılıma ya da sadece donanıma yönelik fiilleri düzenleyen, özel bir suç olduğu kabul edilecek olursa, bu durumda mala zarar verme suçunun maddi unsurunu oluşturan hareketlerin bilişim sisteminin maddi unsurunu oluşturan donanıma yönelik gerçekleştirilmesi durumunda nasıl bir çözüme varılması gerektiği sorun olarak karşımıza çıkmaktadır. Bu durumda, sorun, mala zarar verme suçunun düzenlendiği 151. maddenin bilişim sistemleri bakımından uygulanıp uygulanamayacağıdır.

Bilişim sistemleri ve özellikle bilgisayar sistemleri esas alındığında bunların karakteristik özelliklerini donanım yani fiziksel yapıdan çok yazılım unsuru belirlemektedir. Bu açıdan, bir aygıt olarak bilgisayar sistemlerini diğer aygıtlardan ayıran unsur yazılım kapsamında belirli komutlar aracılığıyla veri işleme faaliyetini yapabilmesi ya da daha genel bir ifade ile işlem yapabilmesidir. Programlar aracılığıyla verinin işlenmesi ve de saklanması yani yazılım unsuru, sadece donanıma bağlı çalışan aygıtlardan farkını ortaya koymaktadır. Veri işleme faaliyeti olarak adlandırılan bu süreç ise kanunda bilişim sisteminin işleyişi olarak formüle edilmiştir.

Bilişim suçları arasında sisteme müdahalenin ayrı olarak düzenlenmesinin nedeni ise, veriye müdahale edilmesi suretiyle sistemin işleyişine müdahale edilebilmesidir. Bilişim sisteminin işleyişinden, yazılıma bağlı veri işleme faaliyeti olarak anlaşıldığına göre 244. maddenin birinci fıkrasında bilişim sisteminin işleyişine müdahale edilmesi düzenlenmesinin, bilişim sisteminin yazılım yönüne yani veri işleme faaliyetine işaret ettiği sonucuna götürebilmektedir. Bu kapsamda, sisteme yönelik fiziki müdahaleler yoluyla değil, sistemin yazılımına ve veriye müdahale ya da yazılımda değişiklik yapılması nedeniyle işleyişinin engellenmesi ya da bozulması halinin bu fıkrada düzenlenmek istendiği söylenebilir.

Bu açıdan incelendiğinde, bilişim sistemi açısından, sistemin işleyişinin engellenmesi, bilişim sistemi olarak bilgisayarın çalışma yöntemi esas alınarak, çalışma yöntemine yani veri işleme faaliyetine müdahale edilmesi yoluyla sistemin çalışmasının engellenmesi olarak karşımıza çıkmaktadır. Nitekim, bir bilgisayar sistemi, işlemleri kapasitesine göre sıraya koyarak gerçekleştirir. Bir bilgisayar sisteminin işlem yapabilme sonuçlandırma hızı onun donanımsal yapısı ile bağlantılıdır. Bir sistemin belirli bir sürede yapabileceği işlem miktarını, yani sistemin işlem kapasitesinin zorlanması ise, bir süre sonra sistemin işlem yapamaz hale gelmesi ile sonuçlanır. Bu durumda, sistemin donanım ya da yazılımında bir bozukluk meydana gelmemesine rağmen kapasitesi üzerinde işlem talep edilmesi nedeniyle çalışamaz hale gelmektedir. Yani sistemin donanım ve yazılımı ile birlikte bütünlüğü ve gördüğü işlev bakımından bir bozukluk meydana gelmemekte fakat sistem belirli bir süre çalışamamaktadır.

Bu kapsamda değerlendirilebilecek müdahale yöntemleri birbirinden farklı olmalarına rağmen, şu örnekle konuyu açıklamak mümkündür. Bir web sayfasına erişim, genel olarak o web sayfasının barındırıldığı sunucu bilgisayara bağlantı kurulması ve sunucuda bulunan web sayfasının içeriğinin yer aldığı verinin kopyalanması anlamına gelmektedir. Web sayfasının yer aldığı sunucunun ise, belirli bir zaman diliminde ancak belirli sayıda bağlantıyı sağlayabilecek ve veri kopyalamasına izin verebilecek bir kapasiteye sahiptir. Birim zamandaki işlem kapasitesinin aşılmasını sağlayacak şekilde sisteme bağlantı kurulması ve veri kopyalanmasına ilişkin bilgisayar aracılığıyla gönderilen talep, yani veri iletilmesi, sistemin gönderilen taleplere cevap verememesi sonucunu doğurabilmektedir. Bu durum ise, belirli bir zaman diliminde sistemin öngörülen hizmeti verememesi, (örn. web sitesine erişilememesi) sonucunu doğurmaktadır.

Yukarıda verilen örnek dışında, sistem içerisindeki veriye müdahale edilmesi, veri yerleştirilmesi yoluyla da bu sistemin işleyişinin engellenmesi mümkün olmakla birlikte bu örnekte olduğu şekliyle sistem içerisindeki verinin ya da genel olarak yazılımın değiştirilmesi, yok edilmesi gibi durumlar gerçekleşmeden ya da sistem bozulmadan da sistemin çalışamaması söz konusu olabilmektedir. Nitekim, bu hususu da kapsaması amacıyla Sibersuç Sözleşmesinde diğer hareketler yanında sistemin veri iletilmesi (transmitting) yoluyla işleyişinin engellenmesi de sisteme müdahalenin düzenlendiği 5. maddede yer almıştır.

Bilişim sisteminin işleyişinin bozulması ise, bu kapsamda sistemin yazılımını oluşturan işletim sistemi ya da diğer programlar gibi sistem içerisinde veri işleme faaliyetini ya da genel olarak işlem yapabilmesini sağlayan unsurlarına müdahale edilmesi sonucu, bunların işlem yapabilme kabiliyetinin tamamen ya da kısmen ortadan kaldırılması anlamındadır.

Bilindiği üzere, bir aygıtın fonksiyonunu yerine getirememesi bozulma kapsamında değerlendirilmekte ve bu haliyle bu tür bir fiil mala zarar verme suçunu oluşturabilmektedir. Bir bilişim sistemi ele alındığında sistemin iki farklı şekilde bozulması söz konusu olabilmektedir. Bu açıdan bir bilgisayarın işlemcisine, anakartına, sabit diski gibi donanımına ait unsurlara zarar verilmesi sonucu sistemin kullanılmasının önüne geçilebilmesi mümkündür. Bütün bu fiiller ise mala zarar verme suçu kapsamındadır.

Bunun yanında, bilişim sisteminin ve bu kapsamda ortaya çıkan bilgisayar sistemlerinin donanım ve yazılım unsuru ile birlikte çalışması bunlara yönelik fiiller ile de sistemin bozulması, yani tamamen ya da kısmen kullanılmasının önüne geçilmesi mümkün hale gelmiştir. Bu durumda, sistemin donanımında herhangi bir değişiklik meydana gelmemekle birlikte yazılım unsurunun bozulması nedeniyle sistem çalışmamaktadır.

Aslında burada, sistemin işleyişinin bozulmasına ilişkin bir hükmün yer almamış olması durumunda da sistemin işleyişinin bozulmasının mala zarar verme suçu kapsamında bozma olarak değerlendirilmesi mümkün olabilecektir. Çünkü bozma, sistemin fonksiyonu yerine getirememesi olarak anlaşıldığında bunun fiziksel bir müdahale ya da yazılıma müdahale yoluyla gerçekleştirilmesi arasında bir fark yoktur. Her ikisinde de özgülendiği amaç için kullanılamaması hali ortaya çıkmaktadır.

Bu durumda, sistemin donanımında, diğer bir ifadeyle maddi varlığında ve bütünlüğünde bir değişiklik olmasından ve bozulmasından bağımsız olarak sistemin çalışamaması durumunda, sistemin bozulmuş sayılıp sayılmayacağına ilişkin ortaya çıkabilecek tereddüdün giderilmesi amacıyla bu hükme yer verildiğini söylemek mümkündür. Bunun sonucunda, maddede ayrıca bilişim sisteminin işleyişinin bozulmasına yer verilmesi, bu madde ile fiziksel müdahalelerden çok yazılım ve veriye müdahale yoluyla sistemin bozulmasına ilişkin bir düzenleme yapıldığı sonucuna götürmektedir.

244. maddenin birinci fıkrasında düzenlenen fiillerin, yazılım unsuruna yönelik müdahalelerin veri aracılığıyla gerçekleştirilmesi şeklinde olduğunun kabulü, 2. fıkrada düzenlenen veriye müdahale ile sisteme müdahale arasındaki ilişkinin ise genel olarak geçitli suç şeklinde olması sonucunu doğurmaktadır. Aynı gerekçe söz konusu suçun mala zarar verme suçuna göre, sadece yazılım unsurunu kapsayan, özel bir norm olması sonucuna götürdüğü kanaatindeyiz.

Bilişim Sistemindeki Verileri Bozma, Yok Etme, Değiştirme, Verileri Başka Bir Yere Gönderme

Bu suç, TCK'nin 244. maddesinin ikinci fıkrasında ayrıca düzenlenmiş ve sisteme müdahaleye göre daha az ceza öngörülmüştür. 244. maddenin 2. fıkrasında, "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gön¬deren kişi, altı aydan üç yıla kadar hapis cezası ile cezalan-dırılır." hükmüne yer verilmiştir.

Maddede yer alan seçimlik hareketlerden ilki, bilişim sistemi içerisindeki "verinin yok edilmesi"dir. Bilişim sistemi içerisindeki verinin yok edilmesi, verinin varlığına son verilmesi, ortadan kaldırılması, hak sahibinin tekrar elde edemeyeceği ya da büyük güçlükler sonucu elde edebileceği şekilde tasarrufundan çıkarılması verinin yok edilmesi olarak tanımlanabilir.

Maddede yer alan diğer bir seçimlik hareket bilişim sisteminin içindeki "verinin bozulması"dır. Verinin bozulması verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılamayacak hale gelmesi olarak tanımlanabilir. Burada özellikle verinin içeriğine müdahalenin var olan verinin içerdiği bilgi ya da enformasyona olumsuz müdahaleyi kapsadığını belirtmek gerekir.

Sistem içerisindeki veriye ve veri grubunu oluşturan programa virüs vb kötü amaçlı kodların sadece eklenmesi, bu anlamda veriyi bozma değil, verinin değiştirilmesi ya da sisteme veri yerleştirme olarak değerlendirilmelidir. Çünkü bu halde virüs gibi kötü amaçlı kodların öngörülen şekilde çalışmasından önceki bir aşamada var olan bir veriye eklenmesi söz konusu olup bu aşamada veri tamamen ya da kısmen kullanılamaz hale gelmemiştir.

Bu açıklama doğrultusunda, madde metninde yer alan verinin değiştirilmesi ise var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinalliğini ortadan kaldıran her türlü değişiklik olarak tanımlanabilir. Bu açıdan kötü amaçlı kodların veriye yerleştirilmesi bu kapsamda değerlendirilebilmektedir.

"Verinin erişilmez kılınması" ise, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup veri, içerik bakımından bütünlüğünü korumaktadır. Veri, ne yok edilmekte ne de bozulmakta, fakat verilere ulaşım için gereken işlem bağı koparılmaktadır. Veriye erişilmesi bakımından erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur.

Yargıtay 8. Ceza Dairesi 2019/3839 E., 2020/5418K.

Sanığın, mağdura ait MSN adresinin internet şifresini, onun bilgisi ve rızası dışında değiştirerek, mağdurun bilişim sistemindeki hesabına erişimini engellemesi biçiminde sübutu kabul edilen eyleminin, TCK'nın 244 /2. madde ve fıkrasında tanımı yapılan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede yanılgıya düşülerek, yasal ve yeterli olmayan yazılı gerekçelerle sanık hakkında TCK'nın 243 /3. madde ve fıkrasındaki bilişim sistemine girme suçundan mahkumiyet hükmü kurulması,

244. maddenin 2. fıkrasında düzenlenen hareketlerin sonuncusu ise, "sistem içerisindeki verinin başka bir yere gönderilmesi"dir. Verinin başka bir yere gönderilmesinin, verinin transferi, verinin kopyalanması olduğu ve kopyalandığı yerin önemsiz olduğu, ifade edilmiştir.

Yargıtay 8. Ceza Dairesi 2015/1581 E., 2016/9981 K.

Sanıkların, katılana ait bilgisayarlara uzaktan erişim yoluyla bağlanıp katılana ait sunuculara izinsiz olarak girilerek şifrelerinin değiştirildiği, kullanılmaz hale getirildiği ve katılana ait ROP programının tüm datalarının silindiği iddiası üzerine açılan davada; soruşturma aşamasında alınan 23.11.2009 tarihli inceleme raporuna göre katılanın bilgisayarlarında bulunan 4 adet klasörün silindiğinin tespit edildiği ancak uzaktan bağlantı yaptığı tespit edilen IP numarasının kime ait olduğuna, bu IP numarası ile bağlantı yapan bilgisayarın kim tarafından kullanıldığına, sanıkların, bilirkişi raporunda server ve client olarak belirlenen numaralara göre suç tarih ve saatinde katılana ait bilgisayarlardan kendi bilgisayarlarına bağlantı gerçekleştirildiğinin anlaşıldığını beyan etmeleri karşısında, bilirkişi raporunda belirlenen bağlantı IP lerine göre hangi yöne doğru bağlantı yapıldığına, klasörlerin bu bağlantı sırasında silinip silinmediğine, klasörlerin mahiyetine, katılanın sisteme girişinin engellenip engellenmediğine, şifrelerin değiştirilip değiştirilmediğine dair dosya içerisinde bir tespitin bulunmadığı anlaşılmakla; öncelikle katılanın bilgisayarlarına bağlantı yaptığı tespit edilen IP numarasının kime ait olduğunun tespiti ve gerektiğinde bağlantı yapan bilgisayar üzerinde inceleme yaptırılarak belirtilen hususlarda bilirkişi raporu alınması ile tüm deliller birlikte değerlendirilip sonucuna göre sanıkların hukuki durumlarının takdir ve tayini gerektiği gözetilmeden eksik araştırmayla yazılı şekilde hükümler kurulması,

Bu suça ilişkin özel bir düzenleme de Elektronik İmza Kanununda yer almaktadır. Özü itibariyle veriye müdahale teşkil eden fiiller elektronik imza ve sertifikaya ilişkin özel düzenleme yapma gereği olarak ayrıca düzenlenmiştir. Bu kapsamda Elektronik İmza Kanunun 16. maddesinde ***"İmza oluşturma verilerinin izinsiz kullanımı"*** suçu *"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."* hükmüne yer verilmiştir. Aynı Kanunun **Elektronik sertifikalarda**[16] **sahtekârlık** başlıklı 17. maddesinde ise *"Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."* hükmüne yer verilmiştir.

Her iki düzenleme de incelendiğinde özü itibariyle veriye müdahaleye ilişkin hareketlerin elektronik imza ve sertifika açısından önemli görülen yönlerinin düzenlenmesi şeklinde olduğu görülür. Bu haliyle veriye müdahale açısından özel hüküm niteliğinde olup elektronik imza ya da sertifika verilerine müdahale durumunda maddelerde sayılan hareketlerin (kopyalama, yeniden oluşturma, elde etme vs, taklit tahrif vs.) gerçekleştirilmesi durumunda Elektronik imza Kanununda düzenlenen bu suçlar uygulanma alanı bulur.

Suça Etki Eden Nedenler

244. maddenin 3. ve 4. fıkralarında suça etki eden nedenler açısından iki ağırlatıcı nedene yer verildiği görülmektedir. Bunlardan birincisi, 244. maddenin 1. ve 2 fıkrasında düzenlenen fiillerin bir kamu kurum ya da kuruluşuna ya da banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmesidir.

Son fıkrada yer alan hüküm ise, genel olarak bilişim ya da bilgisayar sistemleri aracılığıyla yarar sağlama fiillerinin cezalandırılmasına yönelik bir düzenlemedir. Bu düzenleme Bilgisayar dolandırıcılığı adı altında halihazırda bir çok ülke mevzuatında yer alan suça paralel bir hüküm içermektedir. Bu açıdan sorun bilgisayar sistemleri aracılığıyla, veriye ya da sisteme müdahale yoluyla yarar sağlanması halinde veri ya da program manipülasyonunun yani hileli bir takım hareketlerin söz konusu olması, lakin dolandırıcılık suçunun unsuru açısından bunun gerçek kişiye yönelik bir hile olmaması ve bu şekilde yarar sağlanması nedeniyle dolandırıcılık suçu kapsamında değerlendirilememesidir. Bu sorunu gidermek amacıyla da Sibersuç Sözleşmesinde de öngörüldüğü şekliyle özel bir düzenleme yapılması yoluna gidilmesi tercih edilmiştir.

Siber Suç Sözleşmesi Madde 8 - Bilgisayar ile Bağlantılı Dolandırıcılık

Taraflardan her bir, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, ir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

[16] Söz konusu Kanuna göre elektronik sertifika, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder.

Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

a. bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;

b. bir bilgisayar sistemini işleyişine herhangi bir müdahalede bulunma.

Uygulamada söz konusu hüküm ilk başlarda internet bankacılığını kullanmak suretiyle başkalarının hesaplarından hukuka aykırı olarak para transferi yapılması fiillerinde uygulanmış iken sonrasında Yargıtay Ceza Genel Kurulu'nun 2009/11-193 E., 2009/ 268 K. sayılı kararı ile söz konusu fiiller hırsızlık suçu kapsamında değerlendirilmeye başlanmıştır. Hali hazırda bu son fıkradaki düzenlemeye örnek olarak başkasının Bitcoin hesabından hukuka aykırı olarak Bitcoin transfer etme fiilleri gösterilebilir.

Bu hükmün yürürlükten kalkmış olan 765 sayılı TCK'de karşılığı olarak düzenlendiği ifade edilen 525b/1. maddesi söz konusu hükmün yürürlükte olduğu dönemlerde başkalarına ait banka ya da kredi kartlarının söz konusu kartları kullanılması fiillerine bilgileri otomatik işleme tabi tutan ATM cihazları ya da birer terminal niteliği taşıyan POS cihazlarının kullanılması nedeniyle uygulanmıştır. Bu fiillere yönelik olarak 5237 TCK'de özel düzenleme yapılması yoluna gidilmiş ve söz konusu fiiller 245. maddede özel olarak düzenlenmiştir.

Yasak Cihaz veya Programlar

Siber Suç Sözleşmesine uyum sürecinde TCK bağımsız bir suç olarak 245/A maddesinde düzenlenene bir suç olup söz konusu maddeye göre *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."*

Bu hüküm incelendiğinde korunan hukuki konu ya da hukuki değer açısından birçok suçun işlenmesine yönelik hazırlık hareketi olarak nitelendirilebilecek davranışların cezalandırılması yoluna gidilmesi ve bu kapsamda soyut tehlike suçu olarak düzenlenmesi nedeniyle belirsizliğin söz konusu olduğu ifade edilebilir. Nitekim TCK'nın 245/A maddesinde, bilgisayar programı, şifre veya güvenlik kodunun ya münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesi için yapılması ya da farklı bir amaçla yapılmış olmakla birlikte söz konusu suçları işlemeye yönelik sonradan uyarlanmış olması gerekmektedir.

Bu haliyle suçun oluşumu açısından özel kast, yani münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesi için maddede sayılan hareketlerden bir ya da birkaçının gerçekleşmesi gerekmektedir. Haliyle örneğin test ya da bilimsel bir faaliyet kapsamında bu maddede sayılan hareketlerin yapılması manevi unsurunun oluşmamasından dolayı suç olmayacaktır.

Banka veya Kredi Kartlarının Kötüye Kullanılması

Genel Olarak

765 sayılı TCK döneminde başkasına ait banka ya da kredi kartlarının kullanılması ATM ya POS cihazlarının bilgileri işleme tabi tutan sistem olarak kabul edilmesi ve bu tür fiillerde bilgileri işleme tab tutan sistem aracılığıyla yarar sağlandığı sonucuna varılmasına binaen adı 765 sayılı TCK'nin 525b/2. maddesinin uygulanması yoluna gidilmişti (YARGITAY CGK E. 2000/6–62 K. 2000/72 T. 11.4.2000). Söz konusu uygulama sonrasında 5237 Sayılı Türk Ceza Kanununda banka ve kredi kartlarının kötüye kullanılmasına ilişkin 245. maddede özel düzenleme yapılması yoluna gidilmiştir. Bunun yanında 5464 sayı Banka ve Kredi Kartları Kanununda da 5237 sayılı TCK'ye ek yeni suçlar düzenlenmiştir.

Özellikle kredi kartlarının bilişim sistemlerinin kullanılmasından çok daha önce kullanılmaya başlanması karşısında kredi kartlarının bilişim alanında suçlar arasında değerlendirilmesine yol açan husus söz konusu kartlar açısından bir niteliksel etki olmaktan çok TCK açısından adı geçen maddenin uygulanmasından kaynaklanan bir sorun olarak gündeme gelmiştir. Bunun yanında, bu tür kartların elektronik ticaret alanında en yaygın ödeme aracı olarak kullanılıyor olması, bunların kötüye kullanılmasının bilişim suçları arasında anılmasının diğer bir sebebidir. Bu nedenle bu suçların bilişim suçları arasında değerlendirilmesi çok da yerinde olmamakla birlikte hem genel olarak elektronik ticarette yaygın olarak kullanıyor olması hem de eski TCK'de uygulanacak normun tespiti açısından gündeme gelmesi ve nihayetinde 5237 sayılı TCK'de bilişim alanında suçlar arasında özel düzenleme yapılması nedeniyle aşağıda TCK'de düzenlenen suçlara kısaca değinilecektir.

Başkasına Ait Kartın Hukuka Aykırı Olarak Kullanılması

TCK'nin 245. maddesinin birinci fıkrasında *"Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır."* hükmüne yer verilmiştir.

5464 sayılı Kanunun 3. maddesinde banka ve kredi kartı tanımlanmıştır. Buna göre, "banka kartı," *"Mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kartı"* ifade eder. "Kredi kartı" ise *"Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını,"* ifade eder.

TCK 245/2. maddesinin uygulanması açısından failin kartı ne şekilde ele geçirdiğinin önemi olmamaktadır. Bu kapsamda kartın hukuka uygun olarak ele geçirilmesi veya elde bulundurulması neticesinde kartın rıza dışı olarak kasten kullanılması durumunda suç oluşabilecektir. Bu nedenle kartın örneğin hırsızlık sonucu ele geçirilmesi, teslim edilen kuryenin kartı kullanması, kartın bulunması sonrasında rıza dışı kullanımı arasında fark bulunmamaktadır. Burada önemli olan husus kartın hukuka aykırı olarak kullanılması olup ele geçirme ya da elde bulundurma ayrı bir su teşkil ettiği durumda ayrıca söz konusu suçlardan dolayı da cezalandırılır.

Yargıtay CGK, 30.04.2019 tarihli ve 172-361 Sayılı Karar

"Ayrıntılarına Ceza Genel Kurulunun 30.03.2010 tarihli ve 17-65 sayılı kararında da yer verildiği gibi; 5237 sayılı TCK'nın 245/1. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun kanundaki düzenleniş şekli göz önüne alındığında bileşik suç olarak düzenlenmediği görülmektedir. Banka veya kredi kartının kötüye kullanılması suçu ile birlikte oluşabilecek diğer suçlara kanunda öngörülen ceza miktarları da, bu suçun bileşik suç olarak düzenlenmediğini açıkça ortaya koymaktadır. Bu nedenle, banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma, dolandırıcılık gibi suçlar ile banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralı uygulanarak fail her bir suçtan ayrı ayrı cezalandırılmalıdır. Banka veya kredi kartının kanunlarda suç olarak düzenlenen eylemlerle ele geçirilmesi ve şartların varlığı hâlinde, TCK'nın 245. maddesinin birinci fıkrasındaki suçun yanında ayrıca hırsızlık, dolandırıcılık ya da yağma gibi suç oluşabileceği kabul edilmelidir..."

Suçun oluşumu için kart hamilinin rızasının bulunmaması gerekir. Bu kapsamda kart hamilinin kartın çalınması ya kayıp başvurusunda bulunması sonrasında rızaen kullanması ya da başkalarına kullandırtması durumunda ise 5464 sayılı Banka ve Kredi Kartları Kanunun 37/1. maddesinde düzenlenen suç kapsamında değerlendirilmesi gerekir. Söz konusu hükme göre, *"Banka kartı veya kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve ikibin güne kadar adlî para cezası ile cezalandırılırlar."*

TCK' nin 245. maddesinin 1. fırkasında yer alan düzenleme açısından aynı Kanunda şahsi cezasızlık sebepleri ve etkin pişmanlık hali düzenlenmiştir. TCK'nin 245/1. maddesine göre, *"Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz. (5) (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."*

Söz konusu hükmün maddeye konularak malvarlığına karşı suçlar ile ilişkinin de kurulması karşısında bu suçun esasen malvarlığına karşı suç olarak kabul edilerek korunan hukuki değerin kişinin malvarlığı üzerindeki hakları olduğu sonucuna ulaşılabilir.

Sahte Banka veya Kredi Kartı Üretme, Satma, Devretme, Satın Alma veya Kabul Etme

TCK'nin 245/2. maddesinde *"Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır."* hükmüne yer verilerek sahte kredi kartı ya da banka kartlarına yönelik olarak zararın oluşmasını esas almayan tehlike suçu niteliğinde bir düzenlemeye yer verilmiştir.

Söz konusu suçun oluşabilmesi açısından öncelikli olarak başkalarının banka hesaplarıyla ilişkilendirilmiş bir banka ya da kredi kartının sahte olarak oluşturulması gerekmektedir. Bu kapsamda kart başvurusunda sözleşme ve eki belgelerde sahtecilik yapılmış olması durumunda 5464 sayılı Banka ve Kredi Kartları Kanunun 37/2. maddesi uygulanır. Söz konusu hükme göre *"Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler."* Yargıtay kararlarında bu iki hükmün uygulanması açısından sahte belge ibraz suretiyle başvurulma aşamasında 37/2'nin uygulama alanı bulacağını kartın üretilmiş olması durumunda TCK'nin 245/2. maddesinin uygulanma alanı bulacağı sonucuna ulaşılmıştır (Örnek karar için bkz. Yargıtay 8. Ceza Dairesi 2019/19765 E., 2020/578 K.).

245/2. maddesinde suç olarak düzenlenen hareketler sahte kartın üretilmesi (oluşturma, yaratma, kopyalayarak oluşturma), devredilmesi (bir malın mülkiyetini, ya da mal üzerindeki hakkı başkasına geçirmek), satın alma, (belirlenen fiyatın ödenerek mal edinme), kabul etme (sunulan bir şeyi alma) olarak tanımlanmıştır. Bu haliyle kartın kullanılması suretiyle yarar sağlanması ya da zarar verilmesi şartı aranmamakla bir tehlike suçu olarak düzenlenmiştir. Bu hükümle korunan değerin sahtecilik suçlarıyla aynı yönde banka ve kredi kartlarına duyulan güven ilişkisi olduğu söylenebilir.

Sahte Banka veya Kredi Kartının Kullanılması Suretiyle Yarar Sağlanması

TCK 245/2 maddesinde tehlike suçu olarak düzenlenen suça ilişkin olarak sahte kartın kullanılması şartını aramamaktaydı. Bu düzenleme ile sahte olarak oluşturulmuş olan kartın ayrıca kullanılarak yarar sağlanması hali düzenlenmiştir. Burada yararın ekonomik bir yarar olacağı söylenebilir.

Yargıtay kararlarına göre, bu husus tartışmalı olmakla, 245/2 madde kapsamında kartta sahtecilik fiilinin gerçekleştirilmesine binaen kartların kullanılmış olması durumunda fail hem 245/2 hem de 245/3'ten cezalandırılması gerektiği sonucuna ulaşılmaktadır (Örnek karar için bkz. Yargıtay 8. Ceza Dairesi 2013/7794 E., 2014 / 13790 K.; Yargıtay 11. Ceza Dairesi 2012/2110 E., 2013/9973 K.).

Kişisel Verilerin Korunmasına İlişkin Suçlar

Genel Olarak

Bilindiği üzere, özel hayatın korunması kimi yönleri açısından cezai düzenlemelerin konusunu da oluşturmuştur. Nitekim, 765 Sayılı TCK'de özel hayatın gizliliği kapsamında değerlendirilen konut dokunulmazlığı ile haberleşmenin gizliliğine ilişkin suçlar yer almaktaydı. 765 Sayılı TCK'nin 193. vd. maddelerinde yer alan *"mesken masuniyeti aleyhine cürümler"*, 195. vd. maddelerinde yer alan genel olarak haberleşmenin gizliliğini korumaya yönelik olarak karşımıza çıkan *"Sırrın Masuniyeti Aleyhine Cürümler"* 765 Sayılı TCK'de özel hayatın gizliliğinin korunmasına ilişkin suçlar olarak düzenlenmekteydi.

5237 Sayılı TCK'de ise, hem özel hayatın gizliliği genel olarak, hem de özel hayatın gizliliğinin çeşitli yönleri ayrıca özel olarak düzenlenmiştir. 5237 Sayılı TCK'de özel hayatın gizliliğine ilişkin suçlar, genel olarak, *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* başlıklı 9. bölümünde 132. vd. maddelerinde düzenlenmiştir. Kanunun 132. maddesinde *"haberleşmenin gizliliğini ihlal"*, 133. maddesinde *"kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması"*, 134. maddesinde *"özel hayatın gizliliğini ihlal"*, suçlarına yer verilmiştir.

765 Sayılı TCK'den faklı olarak, TCK'de, ayrıca kişisel verilerin korunmasına ilişkin kimi suçlara yer verilmiştir. Kanunun 135. maddesinde, *"kişisel verilerin kaydedilmesi"* 136. maddesinde, *"verileri hukuka aykırı olarak verme veya ele geçirme"*, 138. maddesinde ise, *"verileri yok etmeme"* suçları düzenlenmiştir. Kişisel verilerin korunmasına ilişkin suçlara ilişkin olarak 137. maddede, kişisel verilerin korunmasına ilişkin 135 ve 136. maddelerde düzenlenen suçların *"kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle"* ve "*Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle"* işlenmesi halinde verilecek cezanın yarı oranında arttırılacağı öngörülmüştür.

Bu hususlar doğrultusunda, öncelikli olarak TCK'nin 135 vd. maddelerinde düzenlenen suçların hukuki konusu olarak ortaya çıkan özel hayatın gizliliği esas alınırken bu hususu Anayasanın özel hayatın gizliliğine ilişkin 20. maddesinde 2010 yılında yapılan değişiklikle açık bir hükme bağlanmıştır. Bu haliyle bu düzenlemelerde yer alan suçlarla korunan hukuki değer genel olarak özel hayatın gizliliği kapsamında değerlendirilen kişisel verilerin korunması hakkı olup Anayasanın 20 maddesinin son fıkrasına göre, *"(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hak-*

kına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." Bu düzenleme ile bağlantılı olarak 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilerek hükümleri Kanunda belirtilen tarihlerde yürürlüğe girmiştir.

Söz konusu Kanun incelendiğinde kişisel verilerin işlenmesine ilişkin genel olarak usul ve esasların belirlendiği görülür. Kanunda *"kişisel veri", "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. Kanuna göre *"kişisel verilerin işlenmesi," "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifade eder

Kişisel verilerin işlenmesi açısından genel olarak uyulması gereken ilkeler ise Kanunun 4. maddesinde genel olarak düzenlenmiştir. Buna göre kişisel veriler işlenmesinde *"a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."* ilkelerine uyulması zorunludur.

Kanunda belirtilen sorumluluk ve yükümlülüklerin yerine getirilmemesi açısından ise ikili bir yaptırım yoluna gidilmiş olup bir kısım fiiller açısından Kanunun 18. maddesinde idari yaptırım içeren kabahatler olarak düzenlenmiştir. Söz konusu maddede Kanunda düzenlenmiş bulunan *aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülükleri yerine getirilmemesi, Kurul tarafından verilen kararları yerine getirilmemesi, ve veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi* fiilleri kabahat olarak düzenlenmiştir.

Ceza hukuku anlamında suç oluşturan fiiller açısından ise Kanunun 17. maddesinde *"(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır. (2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."* hükmüne yer verilerek TCK'nin ilgili maddelerinin uygulanacağı belirtilmiştir.

Türk Ceza Kanunun 135 vd. maddelerindeki suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin ilkeler olarak ifade edilen, hem ulusal hem de uluslararası düzenlemelerde çeşitli şekillerde yer verilen kişisel verilerin işlenmesine ilişkin usul ve esasları esas alındığı görülmektedir. Bu açıdan, TCK'nin 135 vd. maddelerinde, dürüst ve hukuka uygun toplama ve işleme, amaçla bağlılık ilkeleri başlığı altında incelenen kişisel verilerin işlenmesine ilişkin usul ve esasların belirli yönleriyle konu edinildiği görülmektedir. Nitekim, 135. maddede suçun maddi unsuru olarak kişisel verinin kaydedilmesi, 136. maddede düzenlenen suçun seçimlik hareketlerini oluşturan, kişisel verinin ele geçirilmesi, verinin başkasına verilmesi ve yayılması, dürüst ve hukuka uygun toplama ve işleme ayrıca amaçla bağlılık ilkesinin bir görünümü olarak karşımıza çıkmaktadır. 138. maddede düzenlenen verinin yok edilmemesi ise özellikle amaçla bağlılık ilkesi ile ilişkisi bulunmaktadır.

Kişisel Verilerin Kaydedilmesi Suçu

TCK'nin kişisel verilerin korunmasına ilişkin ilk suç kişisel verilerin hukuka aykırı olarak kaydedilmesi suçudur. TCK'nin 135. maddesinde, *"(1) Hukuka aykırı olarak kişi¬sel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir... Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."* hükmüne yer verilmiştir.

135. maddede düzenlenen suçun maddi unsuru, kişisel verilerin kaydedilmesidir. Kanunda kaydetmenin ne anlama geldiğine ilişkin bir tanıma yer verilmemiştir. TDK sözlüğüne göre *"kaydetme"* genel olarak yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; sesi veya resmi manyetik bant üzerine geçirmek; bilişim açısından ise, elektronik veya sayısal araçlarda bilgiyi korumaya almak anlamlarını taşımaktadır. Bu kapsamda, genel olarak, her türlü kişisel verinin hukuka aykırı olarak kaydı, 135. maddede düzenlenen suçu oluşturmaktadır. Bunun yanında 135. maddenin ikinci fıkrasında ikili bir ayırıma gidilmiş *"kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine", "hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına"* ilişkin bilgilerin kişisel veri olarak kaydedilmesi durumunda düzenlemenin son haliyle ceza daha da arttırılmaktadır.

Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu

Kişisel verilerin korunmasına ilişkin olarak TCK'nin 136. maddesinde yer alan diğer bir suç, şu şekilde düzenlenmiştir: *"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır... (2) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.*

Maddede kişinin kendisi hakkındaki verileri kontrol edebilmesi bakımından, ilgili kişi hakkındaki verinin, sadece rıza gösterdiği ya da hukuken kişisel veri işlemeye yetkili kişilerin elinde bulunması ve yetkisiz üçüncü kişilerin eline geçmesinin önlenebilmesi için kişisel verinin başkasına verilmesi, yayılması ve ele geçirilmesi şeklinde seçimlik hareketli bir suç olarak düzenlenmiştir. TCK'nin 136. maddesinde düzenlenen suç, genel olarak hangi tür verilerin, kimler tarafından ne şekilde kaydedilebileceğine ilişkin bir koruma sağlarken, bu maddede düzenlenen suç, kişisel verinin yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi ya da kişisel verinin içeriğinin genel olarak öğrenilmesinin engellenmesi açısından, kişisel verilerin işlenmesi süreci içerisinde, kişi bakımından bir koruma getirmektedir. Aynı şekilde,

> Yargıtay 19. Ceza Dairesi 2019/28161 E., 2020/13552 K.,
>
> *"...TCK'nun 135 ve 136 . maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir."*

kişisel verilerin korunması genel olarak kişinin kendisi hakkındaki verileri kontrol hakkı olarak tanımlandığında, ilgili kişinin kendisi ile ilgili verileri kimlerin işlediğini bilebilmesi veya öngörebilmesi bakımından 136. maddede düzenlenen suç önem taşımaktadır.

Maddede yer alan seçimlik hareketlerden, kişisel verinin başkasına verilmesi ve yayılması, bir yönüyle kişisel veri işlemeye yetkili olan kişilere yönelik verinin işlenmesine ilişkin bir iç sınırı oluşturmaktadır. Kişisel veri işlemeye yetkisi olan kişilerin hukuka uygun olarak kişisel verileri kaydetmesi halinde de söz konusu veriler üzerindeki tasarrufu, verinin üçüncü kişilere verilmesi ya da verilerin içeriğinin birçok kişi tarafından öğrenebilecek şekilde başkalarının bilgisine sunması yani yayması bakımından sınırlandırılmaktadır. Bu haliyle, kişisel verilerin kullanımının sınırlandırılması ve istenmeyen ya da yetkili olmayan ifşalardan korunması istenmektedir.

Maddede düzenlenen suçun maddi unsurunu oluşturan seçimlik hareketlerden bir diğeri, verinin yetkisiz üçüncü kişiler tarafından ele geçirilmesidir. Bu hüküm bakımından, kişisel verilerin yetkisiz üçüncü kişiler tarafından elde edilmesinin engellenmesine yönelik bir işleve sahiptir. 135. maddede genel olarak kişisel verilerin toplanmasından bahsedilmesi karşısında, bu maddede düzenlenen kişisel verinin ele geçirilmesi, kaydedilmiş olan kişisel verinin hukuka aykırı olarak elde edilmesi anlamına gelmektedir.

Yargıtay 8. Ceza Dairesi 2019 / 23499 E., 2020 / 17559 K.

"...Bölge Müdürlüğü önündeki ... Bankası ATM'sine kart kopyalama düzeneği yerleştirilmesinden sökülmesi anına kadar her hangi bir kart hamiline ait banka kartı veya kredi kartı bilgilerini kopyalama suretiyle elde edip etmediği konusunda Bankalararası Kart Merkezi tarafından rapor aldırılıp sonucuna göre; kart hamillerine ait kart bilgileri kopyalanarak bir kart oluşturulmaması halinde ele geçirilen kopyalama cihazında bilgi bulunması halinde eyleminin mağdur sayısınca TCK.nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı ve suçun mağdurunun kart bilgilerinin sahibi olan banka müşterileri olacağı cihetle; manyetik şerit bilgilerinin kopyalanarak sahte bir banka veya kredi kartı üretilmesi halinde kartları gerçeğe aykırı olarak üretilen banka sayısınca TCK.nın 245/2. maddesi ile aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda 43. maddesinin, sanığın bankanın ATM cihazlarına yerleştirdiği düzenekle, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışması halinde ise eyleminin TCK. nın 136, 35. ve 43/2. maddelerinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırmayla yazılı şekilde hüküm kurulması..."

Verileri Yok Etmeme Suçu

Kişisel verilerin korunmasına ilişkin olarak TCK'de yer alan üçüncü suç kişisel verilerin yok edilmemesidir. Verileri yok etmeme başlığını taşıyan 138. maddeye göre *"(1)Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir... (2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."* Kişisel Verilen Korunması Kanunun 17/2. maddesi de söz konusu Kanuna tabi kişisel veri işleme faaliyetleri açısından suçun unsurlarını genişletmiştir. Buna göre: *"2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır."* Kanunun 7. maddesinde ise *"MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir."* hükmüne yer verilmiştir.

Kişisel verilerin kaydedilmesinin ve işlenmesinin kişisel verilerin korunmasına ilişkin hükümlerle ayrıntılı olarak düzenlenmesi ve bu açıdan kişisel verilerin işlenmesi, kişisel verilerin korunması hakkı kapsamında istisnai bir durum olması, beraberinde kişisel veriye ihtiyaç duyulmadığı durumlarda verinin yok edilmesi ya da ilgili kişiyle olan doğrudan ya da dolaylı bağlantısının ortadan kaldırılmasını gündeme getirmektedir.

Kişisel verinin yok edilmesi yukarıda belirtildiği üzere, verinin tamamen ortadan kaldırılması anlamına gelebileceği gibi bunun yanında verinin içerdiği bilgi ya da enformasyon ile ilgili kişinin arasındaki bağlantının ortadan kaldırılması şeklinde de gerçekleştirilebilir. Bu ikinci husus, özellikle bilimsel ve istatistikî amaçlarla kişisel verinin işlenmesinde önem arz etmektedir. Saklama zorunluluğunun ortadan kalkması sonrasında, bu tür faaliyetler için verinin gerekli olduğunda kullanılabilmesi açısından verinin yok edilmesi tamamen ortadan kaldırma yanında ilgili kişi ile bağlantısının kurulamayacak hale getirilmesi olarak anlaşılmalıdır. Bu son durumda, verinin ilgili kişi ile doğrudan ya da dolaylı bir biçimde irtibat sağlanamayacak hale getirilmesi sonucunda kişisel verilerin korunmasına ilişkin düzenlemelerin amacını oluşturan veri/enformasyon mahremiyeti kapsamında özel hayatın gizliliğinin korunmasına ilişkin bir beklenti söz konusu olmamaktadır. Bu durumda, verinin içerdiği bilgi ya da veri herhangi bir konu hakkında genel bir bilgi olarak kalmakta ve ancak istatistiki ya da bilimsel bir anlam taşıyabilmektedir.

TCK'nin 138. maddesinde, amacın ortadan kalkması ya da amacın gerçeklemesi sonucunda kişisel verilerin yok edilmesi hususuna yer verilmemiş, bunun yerine kanunların belirlediği sürelerin geçmiş olması sonucunda verinin yok edilmemesi esas alınmış ve ihmali bir suç olarak düzenlenmiştir. Bu son husus Kişisel Verilerin Korunması Hakkında Kanunun 17. maddesinde düzenlenerek adı geçen Kanun kapsamında kalan kişisel veri işleme faaliyeti açısından suç kapsamına alınmıştır.

BÖLÜM ÖZETİ

Günümüzde bilgi ve enformasyonun etkin olarak işlenmesinde teknik açıdan belki de en önemli yere sahip olan bilişim teknolojisinin gelişimidir. Bilişim teknolojisi, özellikle modern bilgisayarın 20. yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşümünün içinde şekillenerek toplumsal ilişki ve kurumları çeşitli yönleriyle etkilemeye başlamıştır. Toplumsal bir kurum olan hukuk da birçok yönüyle söz konusu gelişimden etkilenmiştir. Bu bağlamda bilişim suçları, bilgisayar suçları gibi birçok ad altında incelenen suçlar, dönüşümün ceza hukukuna niceliksel ve niteliksel etkisini oluşturmaktadır.

Ceza hukuku açısından sorunun bir yönü bilgi ve enformasyonun, korunmasıyla ilgilidir. Sorunun diğer bir yönü ise sayısallaşma olarak adlandırılan durum ile ilgilidir. Söz konusu sorunlara ilişkin olarak ceza hukukunda tartışmaların merkezini oluşturan hususlar, hangi değerin korunduğu ve bununla bağlantılı olarak bu değerlere yönelik saldırıları ifade eden hangi tür fiillerin suç olarak düzenlenmesi gerektiğidir. Bilişim suçları olarak adlandırılan suçlarda, öncelikli olarak ceza müeyyidesiyle koruma altına alınan değerin ne olduğunun tespiti önemlidir. Bu husus, bir yandan da korumanın amacını ve meşruiyetini göstermektedir. Hâliyle bu da suçun hukuki konusunun ve bununla bağlantılı olarak özellikle suç olarak düzenlenecek fiillerin belirlenmesine yönelmeyi gerekli kılmaktadır.

Farklı nitelikteki birçok suçun bilişim suçları adı altında gündeme gelmesi, bilişim suçlarının incelenmesine ilişkin belirli bir sınırlandırılmaya gidilmesi zorunluluğunu doğurmaktadır. Bu nedenle bu bölümde 5237 Sayılı Türk Ceza Kanunu'nun 243. ve 244. maddelerinde düzenlenen suçlar ağırlıklı olarak incelenmiştir. Banka ve kredi kartlarının kötüye kullanılması suçu ile Elektronik İmza Kanununda düzenlenen suçlar da ilgisi olduğu ölçüde ele alınmıştır. Sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kullanımının diğer önemli bir etkisi olarak ortaya çıkan kişisel verilerin korunmasına ilişkin Türk Ceza Kanunu'nun 135 ve diğer maddelerinde düzenlenen suçlar da yine niteliksel bir etki olarak inceleme konusu yapılmıştır.

GÖZDEN GEÇİRELİM

Yetkisiz erişim suçundan bahsedilebilmesi için sisteme erişim açısından en azından .... yetkisinin elde edilmiş olması gerekir.

Veriye müdahale suçunda sistem üzerine .....yetkisinin kullanılmış olması esastır.

Cihazların kötüye kullanma suçunun gerçekleşebilmesi için maddede belirtilen suçların işlenmesine yönelik olarak ..... kastın bulunması gerekir.

Bilişim sistemleri aracılığıyla dolandırıcılık suçu özü itibariyle dolandırıcılık suçunda .... unsurunun bulunmaması nedeniyle klasik dolandırıcılık suçunun unsurlarında ortaya çıkan eksikliği gidermek amacıyla düzenlenmiştir.

Yargıtay kararlarına göre sahte kredi kartını devralan ve sonrasında kullanarak yarar sağlayan fail, ... göre cezalandırılır.

CEVAP ANAHTARI

1. okuma
2. yazma
3. özel
4. hile
5. hem 243/2 hem de 243/3. maddelere

KAYNAKÇA

(Bu bölüm ağırlıklı olarak Muammer Ketizmen, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi Ankara 2008, adlı eserden özetlenerek hazırlanmış olup aşağıda doğrudan yararlanılan kaynaklar gösterilmiştir. Kaynakçanın tamamı için söz konusu eser esas alınmalıdır.)

Akıncı, Hatice/*Alıç*, A. Emre/*Er,* Cüneyd: Türk Ceza Kanunu ve Bilişim Suçları, İnternet ve Hukuk, Der. Yeşim M. Atamer, Baskı, İstanbul 2004, s. 157-275.

Biçkin, İnci: Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları, Yargıtay Dergisi, C. 32, Ocak-Nisan 2006, s. 145-168.

Carter, David L.: Computer Crime Categories: How Techno-Criminals Operate, http://www.lectlaw.com/files/cri14.htm. (E.T. 20.11.2022)

Danışman, Ahmet: Ceza Hukuku Açısından Özel Hayatın Korunması, Konya 1991.

Dönmezer, Sulhi/*Erman*, Sahir: Nazari ve Tatbıki Ceza Hukuku, Genel Kısım, C. I, 12. B., İstanbul 1997.

Dülger, Murat Volkan: Bilişim Suçları, 1. Baskı, Ankara 2004.

Erem, Faruk/*Toroslu,* Nevzat: Türk Ceza Hukuku Özel Hükümler, Savaş Yayınevi, 9. Baskı, Ankara 2003.

Ersoy, Yüksel: Genel Hukuki Koruma Çerçevesinde Bilgisayar Suçları, Prof. Dr. Yılmaz Günal'a Armağan, Ank. Ün. SBFD, C. 49, Haziran-Aralık 1994, No. 3-4, Ankara 1995, s. 149-183.

Falzetti, Valerio I.: Computer Crimes, 83 vd. http://www.unicam.it/ ssdici/falzetti.pdf. (E.T. 13.10.2005)

Gülşen, Recep: İnternet ve Suç, İnternet ve Toplum, Editör: Ahmet Tarcan, Ankara 2005, s. 200-256.

Güney, Niyazi/*Özdemir,* Kenan/*Balo,* Yusuf S.: Yeni Türk Ceza Kanunu, 1. Baskı, 2004.

Heymann, Stephen P.: Legislating Computer Crime, 34. Harv. J. on Legis. (1997), pp. 373 - 391. (Heinonline)

Ippolito, Carlo Sarzana di S.: Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalyadaki Durum, İHFM, C: LV, S. 3, 1997, Çev. Vesile Sonay Daragenli. s. 389-405.

İçel, Kayıhan: Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İHFM, C. LIX, S. 1-2, 2001, s. 3- 9.

Karagülmez, Ali: Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 1. Baskı, Ankara 2005.

Karakurt, Eren, A.: "Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre Ya Da Güvenlik Kodlarının Üretilmesi, Yayılması Veya Bulundurulması Suçu". Türkiye Adalet Akademisi Dergisi (2020), s. 219-246

Keskin, Serap: Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İHFM, C. LIX, S. 1-2, s. 155 – 180.

Koca, Mahmut: Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, C. III, s. 785-816.

La Greca, Federico Tavassi: Hacking e Criminalità Informatica, http://www.dvara.net/hk/hacking_e_criminalita_informatica.doc (E. T. 20.11.2022)

Meran, Necati: Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında İşlenen Suçlar, Seçkin Yayımevi, 1. Baskı, Ankara 2005.

Nicholson, Laura J./*Shebar,* Tom F./*Weinberg,* Meredith R.: Computer Crimes, 27 Am. Crim. L. Rev. (2000), pp. 207-259.

Özbek, Veli/*Doğan,* Koray/*Bacaksız,* Pınar: Türk Ceza Hukuku Özel Hükümler. 17. Baskı, Seçkin Yayıncılık, Ankara 2022.

Rasch, Mark D.: 11. Criminal Law and The Internet, http://cla.org/ RuhBook/chp11.htm. (E.T. 03.04.2006)

Sieber, Ulrich, Legal Aspects of Computer - Related Crime, in the Information Society, - COMCRİME - Study, 1998, https://www.law.tuwien.ac.at/sieber.pdf (E.T. 20.11.2022)

Sinrod, Eric J./*Reilly,* William P.: Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer & High. Tech. L. J. (2000), pp. 177-232.

Sokullu-Akıncı, Füsun: Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi, İHFM, C. LIX, S. 1-2, 2001, s. 11-38.

Soyaslan, Doğan: Ceza Hukuku Özel Hükümler, 5. Baskı, Ankara 2005.

Toroslu, Nevzat: Ceza Hukuku Özel Kısım, 1. Baskı, Ankara 2005.

Wallace, Wang: Steal This Computer Book 3: What They Won't Tell You About the Internet, San Francisco, 2003. (Ebrary)

Yazıcıoğlu, Yılmaz: Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, Yeditepe Hukuk Fakültesi Dergisi, C. 2, S. 2, 2005, s. 393-412.

Yazıcıoğlu, Yılmaz: Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle, 1. Baskı 1997.

Yenidünya, A. Caner/*Değirmenci,* Olgun: Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 1. Baskı, 2003.

Yılmaz, Davut: Hacking, Bilişim Korsanlığı ve Korunma Yöntemleri, İstanbul 2004.