BİLİŞİM HUKUKUNUN ÇEŞİTLİ BOYUTLARI ve ZARARLARA KARŞI ALINACAK ÖNLEMLER

Bu çalışmamızda, oldukça geniş bir alan olan bilişim hukukunu, Türk Ceza Kanunu'ndaki bilişim suçları ve yaptırımları ile, internet bankacılığındaki riskler ve bu risklere karşı alınacak önlemlere değindik. Ayrıca, bilişim suçlarıyla mücadelede bireylerin ve devletin alması gereken önlemlere ilişkin görüş ve önerilerimizi sunarak çalışmamızı tamamladık. En son kısımda ise, çalışmamızın temelini oluşturan kaynaklara yer verdik ki okuyuculardan dileyenler, adı geçen kaynaklara ulaşabilsinler. Çalışmanın yararlı olması dileğiyle...

Bilişim Ceza Hukuku ve Suçlar

Bilişim Alanında Suçlar Bölümündeki Suç Tipleri

Türk Ceza Kanunu'nun İkinci Kitabının "Topluma Karşı Suçlar" başlığını taşıyan Üçüncü Kısmı'nın Onuncu Bölümünde 243,244, 245 ve 246. maddelerinde "Bilişim Alanında Suçlar" düzenlenmiş ve yaptırıma bağlanmıştır.

1.) Bilişim Sistemine Girme Suçu: Bu kısımda 243. maddede, bir bilişim sisteminin tümüne veya bir kısmına hukuka aykırı olarak girme ve girdikten sonra hukuka aykırı olarak çıkmama eylemi suç olarak tanımlanmıştır. Burada suçun oluşması bakımından önemli olan bilişim sistemine girmek ve sistemde bir süre kalmaktır. Yalnızca sisteme girmek hukukumuzda suç değildir. Sistemde kalma süresinin ne kadar olduğunu somut olaya göre yargıç takdir edecektir. Bu suçun yasaya konması ile hem bilişim sisteminin güvenilirliği, hem kişilerin özel yaşamı hem de sistemi kullananların kişisel çıkarları korunmuştur.

243. maddedeki suçta herkes fail olabilir. Ancak, takdir edilmelidir ki bu suçun faili olabilmek için, iyi düzeyde (ortalamanın üzerinde) bilgisayar bilgisine sahip olmak aranmalıdır. Bu suçta, sistemine girilmek yoluyla zarara uğrayan herkes mağdur sayılır.

Suçun oluşması için sisteme ne şekilde girildiği önem taşımaz. Örneğin, fail sisteme bizzat girmese ama sisteme girmeye yarayan bir casus programı e-posta yoluyla gönderse de bu suç oluşacaktır. Çünkü, casusu program genellikle güvenilir ve tanıdık bir e-posta aracılığı ile sisteme ulaştırılmakta ve e-postayı açan kişi, kötü niyetli casus programın farkına varmamaktadır. Bu suçun oluşması için mutlaka sistemin tümüne girilmesi gerekmez; bir kısmına girmele de suç oluşacaktır.

Suçun oluşmasına örnek olarak, sistemin şifresinin veya güvenlik duvarının sahibinin rızası dışında kırılması ya da kırma olmasa dahi, sistemin şifresinin bilinmesi durumunda, şifre sahibinin rızası dışında sisteme erişilmesi verilebilir. (MSN şifresini kırmak yoluyla sisteme girmek ve sistemde kalmak ya da şifresini bildiğiniz bir kişinin MSN adresine, ondan habersiz olarak girmek ve o sayfada kalmak) .

Suçun oluşması için mağdurun bir zarara uğramış olması şart değildir. Salt sisteme girmek ve sistemde kalmak dahi suçtur. Failin, sisteme kendi adına ya da bir başkası adına girmesi de suçun oluşmasını önlemeyecektir.

Suçun oluşması için, sisteme erişimin hukuka aykırı olması gerekmektedir. Sözgelimi yalnızca yetkili kişilerin girmesine izin verilen ya da belli bir şifre ile girilebilen sisteme üçüncü kişi tarafından erişilmesi durumunda suç oluşacaktır. Çünkü, bu durumda sistem özel bir şifre ile korunmaktadır. Ancak, sisteme erişmeye yetkili olan kimse, üçüncü kişiye şifresini vermiş ve sisteme o şekilde erişilmişse suç oluşmaz. Bunun dışında, bir mahkeme kararına dayanılarak, sözgelimi, Ceza Muhakemesi Kanunu (CMK) 134 gereğince, bilgisayarda arama işlemine girişilmişse, yine hukuka uygunluk nedeni var sayılmaktadır ve suç oluşmaz. Aynısını, CMK 135'te düzenlenmiş olan "iletişimin tespiti tedbiri" bakımından da söylemek mümkündür. Örneğin, CMK 135 gereğince, şüphelinin e-postalarının izlenmesi için bilişim sistemine girilmesi durumunda da suç oluşmayacaktır. Ayrıca, kanaatimizce, "etik hacker" veya "beyaz hacker" olarak adlandırılan ve bir kurumun sistemindeki zaafiyetleri ortaya koymakla görevlendirilen kişiler de bu suçun faili olamazlar. Ancak bunun için, adı geçen kişilerin, sistemine girilmesine izin veren kuruluşa karşı bir eylemi söz konusu olmalıdır. Örneğin, Microsoft'un sistemindeki zayıflıkları ortaya çıakrmak için bu şirket tarafından görevlendirilen ve şirketin sistemine giren kişilerin durumu bu kapsamda ele alınabilir.

Bu suçun yasada öngörülen cezası bir yıla kadar hapis veya adli para cezasıdır. Ancak, sistemin içerdiği veriler yok olur veya değişirse ceza altı aydan iki yıla kadar hapis olarak uygulanacaktır.

2.) Bilişim Sistemine Müdahale ve Bilişim Sistemi Aracılığıyla Yarar Sağlama Suçu: TCK'daki diğer düzenleme ise TCK'nın 244. maddesindedir. Buna göre, bu suç bakımından aşağıdaki ölçütlere göre değerlendirmeye gidilecektir.

TCK 244/4'te "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 adli para cezasına hükmolunur." ifadesi yer almaktadır. Öyleyse, öncelikle, yukarıdaki fıkralarda tanımlanan fiillerin **(suçun maddi unsurunun)** neler olduğunun açıklığa kavuşturulması, suçun nitelendirmesi bakımından önem taşımaktadır.

TCK 244/1'de bir bilişim sisteminin **işleyişinin engellenmesi veya bozulması** fiili yaptırıma bağlanmıştır. İşleyişin engellenmesinden kasıt, sistemin düzgün işleyişinden ötürü elde edilecek yararın engellenmesi veya sistemin olağan işlevini yerine getiremeyecek hale getirilmesi ya da sisteme yapılan eklerle, sistemin usulune uygun şekilde değerlendirilmesi olanağının kaldırılması, sistemin amacını yerine getiremeyecek duruma getirilmesi olarak anlaşılmalıdır.

Belirtmek gerekir ki işleyişin engellenmesi her somut olayda farklı biçimde ortaya çıkabilir. Örneğin sistemi besleyen elektirik kesilebilir, sistemin çalışması için mutlaka gerekli olan bir donanım çıkarılabilir, sistemin kabloları sökülebilir, sisteme virüs veya benzeri bir zararlı yazılım yüklenebilir, sistemde olmayan bir şifre sisteme yerleştirilebilir veya sistemdeki mevfcut şifre değiştirilebilir. Sistemin elektronik posta yoluyla kilitlenmesi de işleyişinin engellenmesi olarak tanımlanabilir.

TCK 244/1'de tanımlanan diğer bir hareket ise sistemin **işleyişini bozmaktır.** Buna göre, sistem bozulduğunda tamamen çalışamaz hale gelmektedir. Çalışamaz hale gelmekten kasıt ise, sistemin çökertilmesi, program akışının değiştirilmesi, bozulması, sistemin soyut unsurlarının örneğin virüsler aracılığıyla işleyemez hale getirilmesidir .Buna göre, yazılımın kısmen veya tamamen çalışamaz hale geitirilmesi durumunda ya da sistemin çalışmasına yarayan düzeneğe zarar verilmesi durumunda sistem eğer bir daha çalışamayacak hale geliyorsa, sistemin işleyişinin bozulduğu kabul edilmelidir. Buna örnek olarak bilgisayarın harddiskini kırmak ya da fiziki bir etkiyle (örneğin baltayla parçalamak gibi) harddiske zarar vermek gösterilebilir. Çünkü harddiske bu şekilde verien zarar sonucunda, harddiskteki verilere ulaşabilmek olanaksız olacaktır. Bunun sonucu da sistemin işleyemez hale gelmesidir. Aynısı, CD, DVD, taşınabilir bellek gibi veri taşıma araçları için de geçerlidir.

TCK 244/2'de ise suçun maddi unsuru olarak verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi tanımlanmıştır. Bu fiillerin sonucunda faile altı aydan üç yıla kadar hapis cezası verilecektir.

Veri kavramından neyin kast edildiğini tanımlamak da TCK 244'teki suçun anlaşılması bakımından önem taşımaktadır. Bilişim Hukuku anlamında veri, "olgu, kavram veya komutların, iletişim, yorum veya işlem için elverişli biçimde gösterilmesi" olarak tanımlanmaktadır. Örneğin, perakende satış yapan bir mağazada, bir müşterinin siparişinde yer alan kimliği, sipariş ettiği ürün, satın almak istediği ürün miktarı ve ürün fiyatı o mağaza için