OLMASI GEREKEN HUKUK AÇISINDAN TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNE HAKSIZ ERİŞİM SUÇU

Doç. Dr. Ali KARAGÜLMEZ*

ÖZET

Tek başına ya da başta bilişimle ilgili olmak üzere başka bir suçu gerçekleştirmek için de işlenebilen haksız erişim, bilişim suçları içerisinde en yaygın olanıdır. Temel şekli yer almakla birlikte, konuya verilen önem, farkındalık, bilişim teknolojisiyle irtibat düzeyi, uygulamadan kaynaklanan tecrübelerin gözetilmesi gibi nedenlerle karşılaştırmalı hukukta bilişim sistemine haksız erişim farklı düzenlemelere konu edilmiştir.

Türk Hukukunda ilk defa ayrı bir suç olarak bilişim sistemine haksız erişimin düzenlendiği 5237 sayılı Türk Ceza Kanununun (TCK) 243. maddesi, yabancı ülke ve uluslararası örneklere göre kendisine özgü farklılık ve eksiklikler taşımaktadır. Bu farklılık en başta suçun maddi unsuruna ilişkindir.

Ülkemizde yürürlüğe girdiği 1 Haziran 2005 tarihinden itibaren 5237 sayılı TCK'nın 243. maddesine ilişkin soruşturma ve kovuşturma sayılarında yıllara göre artış ve değişim yaşanmakla birlikte bu suç Yargıtay kararlarında çok fazla yer almamaktadır.

5237 sayılı TCK'nın 243. maddesi, sadece olan hukuk açısından incelenmemeli, olması gereken hukuk açısından da değerlendirilerek düzenlemenin yeterli olup olmadığı belirlenmeli, varsa ihtiyaç duyulan hükümler ortaya konulmalıdır. Klasik suçlara göre bilişim alanının kendisine özgü nitelikleri de dikkate alınarak yapılması gerekenlerin belirlenmesinde karşılaştırmalı hukuktaki kanuni düzenlemeler ele alınmalı, başta 5237 sayılı TCK'nın 243. maddesine ilişkin olmak üzere kanuni eksiklikler bir an evvel giderilmelidir. Bu yaklaşım, bilişim sistemine haksız erişim ve hatta buna bağlı olarak işlenebilecek diğer suçlarla mücadelede başarının arttırılmasına, bu suçun işlenmesinin caydırılmasına önemli katkılar sağlayacaktır.

Anahtar Kelimeler: Bilişim sistemi, haksız erişim, olması gereken hukuk, suçla mücadele.

***

* Hâkim, Anayasa Mahkemesi Raportörü.

I- GİRİŞ

Bilişim sistemine haksız erişim karşılaştırmalı hukukta, *"yetkisiz erişim", "yetkili erişimin aşılması", "zorla erişim", "hileyle erişim"* gibi farklı kavramlarla ifade edilmektedir. 5237 sayılı Türk Ceza Kanununun 243. maddesinin başlığında *"Bilişim sistemine girme"* tercih edilmiştir.

Bir bilişim sistemine haksız erişim, bilişim sistemlerinin ve kapsamındaki verilerin, gizlilik, bütünlük, kullanılabilirlik gibi hususları kapsayan güvenliğine yönelen tehdit ve saldırılar biçimdeki hukuka aykırı fiilleri anlatmaktadır. Bilişim sistemlerinin korunma ihtiyacının yanında, ister fert ister kurumsal düzeyde olsun kullanıcıların rahatsız edilmemesi ve engellenmemesi gereklidir. Yalnızca bilişim sistemine haksız erişimin dahi başlıbaşına bir suç olarak düzenlenmesi önemli bir ihtiyaç olarak görülmektedir. Haksız erişim uygulamada, hacking, cracking veya computer trespass gibi yöntemlerle gerçekleştirilmektedir[2].

Başkalarına ait bilişim sistemlerine, merak, farklı duygular, çıkar elde etme veya değişik nedenler, insanları izinsiz girmeye yöneltmektedir. Dışa açık olmayan bir bilişim sistemine haksız erişim, bilişim suçları içerisinde en çok görülen fiillerden birisidir. Bu fiil, genellikle klasik (geleneksel) suçlarda konut dokunulmazlığının ihlâl edilmesi suçuna benzetilmektedir. Şekil itibarıyla konut dokunulmazlığını ihlâl fiiline benzeyen bilişim sistemine haksız erişim, niteliği bakımından çok daha kapsamlı ve ağır sonuçları beraberinde getirebilir. Konut dokunulmazlığını ihlâl eden bir kişinin konutta kalmaya devam etmesi, bunu günlerce sürdürmesi istisnalar dışında görülmezken, haksız erişimde durum farklı olabilmektedir.

Bilişim suçlarında haksız erişim, tek başına gerçekleştirilebileceği gibi, bilişimle ilgili olsun ya da olmasın başka bir suçu işlemek için *"araç suç"* olarak da görülebilir. Hatta haksız erişimin araç suç şeklinde işlenmesi daha yaygındır. Bu yönüyle haksız erişim, konut dokunulmazlığı suçuna daha fazla benzerlik taşımaktadır. Bir başka anlatımla konut dokunulmazlığı suçu da yaygın şekilde örneğin hırsızlık, adam yaralama ya da öldürme gibi bir suçun öncesinde araç suç olarak gerçekleştirilmektedir.

[2] Kit, Burden, Creole Palmer ve Barlow Lyde & Gilbert, Cyber Crime- A New Breed of Criminal, Computer Law and Security Report, Vol.19 No.3, 2003, s.222 vd.

Haksız erişim, bilişim sistemlerinin kullanıcılarının engellenmesine veya sistemlerde onarılması yüksek maliyetli kayıp veya tahribatlara neden olabilir. Haksız erişimler, aleni olmayan verilere veya sırlara ulaşılmasına, hatta bilişim sistemlerinin bedelsiz kullanılmasına yol açabilir. Haksız erişim, öncelikle fark edilmediği ve sonra da teknik ve yasal önlemlerle engellenmediği takdirde failleri bilişimle ilgili daha başka suçlara teşvik edebilir; yöneltebilir[3].

Haksız erişimin hedefine ya da sonuçlarına göre farklı yansımaları söz konusudur. Bunlardan bazıları; gizli bilgileri ifşa etmek ya da ifşasına neden olmak, bilgi çalmak, bilgi manipulasyonu yapmak, kötüniyetli yazılım kullandırmak şeklindedir[4].

Çoğunlukla *"zorla girme"* şeklinde gerçekleştirilen bir bilişim ağına haksız erişim, bilişim ağı için istenmeyen kötü bir durumdur. Bu fiil popüler bir ifadeyle hacking (bilişim korsanlığı) şeklinde bilinir. Bu suçların soruşturması da, karmaşık işlemleri gerektirebilmektedir. Özellikle her geçen gün kamu ve özel alanda ağ bağlantılarının artması, bu tür suçları daha nitelikli hale getirebilmektedir. Özellikle ağ üzerinde haksız erişimde faile ulaşabilmek, kapsamlı ve uluslararası düzeyde araştırma ve işbirliğini gerektirebilmektedir. Kevin Mitnick davası bunun tipik bir örneğini teşkil etmektedir[5]. Haksız erişime ilişkin soruşturmalarda önemli bir sorun da failin erişiminin devam edip etmediğinin belirlenebilmesindeki zorluklardır. Eğer bu husus göz ardı edilmişse, soruşturmada istenmeyen olumsuzluklarla karşılaşılabilir.

Diğer yandan, haksız erişime konu bilgisayar ya da bilişim sistemi özenle araştırılmalı, sistemde haksız erişimin sağlandığı yer ya da yerler iyi belirlenmeli, haksız erişime maruz kalan veri ya da alanlar liste halinde tespit edilmelidir[6]. Kısacası haksız erişim fiili, işlendikten sonra soruşturma safhası bakımından da ciddi zorlukları beraberinde getirebilmektedir.

Karşılaştırmalı hukukta bilişim sistemine haksız erişimin büyük çoğunlukla suç olarak düzenlendiği görülmektedir. Hatta bazı ülkeler bu fiili,

---

3 Kit, Burden, s.222 vd.

4 Computer Crime and Information Technology Security, Computer Crime Examples, Chapter 14, 1.24.2007, s.241-244.

5 Steven Schlarman, *"Network Intrusion Management and Profiling";* CYBER FORENSICS A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Editors Albert J. Marcella, Ph.D., Robert S. Greenfield, Auerbach Publications, 2002, s.117.

6 Steven Schlarman, s.125-126.

önemli bir suç olarak kabul etmişlerdir. Örneğin, Avustralya'da Federal Nitelikteki Siber Suçlar 2001 Kanunu ile 1995 Ceza Kanununda yapılan değişiklikle 477/ 1. maddesinde kasten *"haksız erişim"* önemli bir suç sayılmıştır[7].

Amerika Birleşik Devletleri'ndeki Bilgisayar Sahteciliği ve Suiistimali Kanununda (Computer Fraud and Abuse Act) (CFAA) *"yetkisiz erişim"* ve *"yetkili erişimin aşılması"* nitelemesiyle haksız erişim suçu düzenlenmiştir. CFAA'da yetkisiz erişim tanımlanmamış, fakat yetkili erişimin aşılması tarif edilmiştir. Buna göre yetkili erişimin aşılması, bir bilgisayara yetkili olarak erişen kimsenin, bilgisayar içerisindeki bilgileri elde etmek veya değiştirmek konusundaki yetkisini ihlâl etmesidir (18 U.S.C. § 1030(e)(6)[8].

II- BİLİŞİM SİSTEMİNE HAKSIZ ERİŞİM

A- 5237 sayılı Türk Ceza Kanununun 243. Maddesi

1) Suçun Temel Şekli

765 sayılı Türk Ceza Kanununda bir bilişim sistemine haksız erişim ayrı bir suç olarak düzenlenmemişti. Bu açıdan 5237 sayılı Türk Ceza Kanunundaki *"Bilişim sistemine girme"* başlıklı 243. maddesindeki düzenleme, Türk Hukukunda ilk defa yer almıştır.

5237 sayılı Türk Ceza Kanununun 243. maddesinin (1) numaralı fıkrasında *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir."* hükmüne yer verilmiştir.

243. maddenin (1) numaralı fıkrası, Fransız Ceza Kanununun 323-1. maddesine benzemektedir. Fransız Ceza Kanununun 323-1. maddesinde, bilgileri otomatik işleme tâbi tutan bir sistemin tamamına ya da bir kısmına hileyle erişmek veya içinde kalmak, iki yıla kadar hapis ve 30.000 Euroya kadar para cezasını gerektirmektedir[9].

Türk Ceza Kanununda *"bilişim sistemi"* tanımlanmamış; 243. maddenin gerekçesinde açıklanmıştır. Gerekçeye göre bilişim sistemi, verileri top-

---

7 Dave Kleiman, Technical Editor, Kevin Cardwell, Timothy Clinton, Michael Cross, Michael Gregg, Jesse Varsalone, Craig WrightThe Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators, Worldwide Forensic Acts and Laws • Appendix B, Burlington, 2007, s.879.

8 Michael Battle, Michael W. Bailie, Prosecuting Computer Crimes, Published by Office of Legal Education Executive Office for United States Attorneys, s.4.

9 Dave Kleiman, s.893-894.

layıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir. Bilişim sisteminin Türk Ceza Kanununda tanımlanmamış olması, bilgi ve iletişim teknolojisindeki durmadan daha büyük bir hızla devam eden gelişmeler karşısında yerinde bir yaklaşımdır.

"Bilişim sistemine girme" başlığı da dikkate alındığında 243. maddede, bilişim sistemine haksız erişimin suç olarak düzenlendiği düşünülebilir. Ancak, madde içeriği bu sonucu tam olarak yansıtmamaktadır.

Maddenin yasalaşmak üzere Türkiye Büyük Millet Meclisi'ne sevk edilen şeklinde *"girme"* veya *"orada kalmaya devam etme"* seçimlik hareketler olarak öngörülmüşken, Meclis Genel Kurulu'nda verilen önergeyle *"veya"* kelimesi *"ve"* şeklinde değiştirilmekle, 243. maddedeki *"suç, yetkisiz erişim + kalmaya devam etme"* şekline dönüştürülmüş, Türk Hukukunda ilk defa getirilen bu suçun işlenmesi zorlaştırılmış ve suçla korunmak istenilen hukukî yarar da zedelenmiştir.

Meclisteki değişiklik önergesinin gerekçesinde, *"Suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiilin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür."* denilmiş ise de, seçimlik hareketlerin birlikte aranmasının sebebi belirtilmemiş, herhangi bir açıklama yapılmamıştır. Üstelik değişiklik önergesindeki gerekçede belirtilenin aksine madde metninde bir suç tanımından veya suç tanımlarındaki belirliliği sağlamaktan söz edebilmek de mümkün değildir.

243. maddenin (1) numaralı fıkrasıyla, karşılaştırmalı hukukta[10] örneğine rastlamadığımız doğrudan *"temadi"* koşuluna bağlanan bir bilişim sistemine yetkisiz erişim suçu türü ortaya çıkartılmıştır. Bunun sonucu olarak, 5237 sayılı TCK'da hukuka aykırı olarak bir bilişim sistemine yalnızca girmek, başka bir ifadeyle *"haksız erişim"*, 243. madde kapsamında teşebbüs aşamasında dahi suç teşkil etmemektedir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin *"Haksız erişim"* başlıklı 2. maddesindeki *"Her Taraf, iç hukukuna uygun olarak, bir bilişim sistemi-*

[10] Bilişim sistemine yetkisiz girme, Avrupa Konseyi tarafından hazırlanan tavsiye kararına eklenen R (89) 9 sayılı yönergede belirtilmiş ve Konsey, hükümetlere bilişim sistemlerine yetkisiz girmeyi suç sayarak cezalandırmayı tavsiye etmiştir; Dave Kleiman, s.874-875; Carlo Sarzana Ippolito, "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum", (İtalyan Temyiz Mahkemesi Ceza Dairesi Başkanı), (Çev.Vesile Sonay Daragenli), İHFM, Sayı 3, 1997, s.399.

ni tamamına veya bir kısmına kasten ve haksız olarak erişimi (illegal access), suç haline getirmek için gerekli görülen kanunî tedbirleri kabul eder" hükmü ile 243. maddenin paralellik taşıdığı görüşü[11] yukarıdaki açıklamalar karşısında yerinde değildir. Sözleşmede, bilişim sistemine haksız erişim suç sayılmasına rağmen, 243. maddede yalnızca haksız erişim, suç için yeterli görülmemekte ayrıca orada kalmaya devam etme de aranmaktadır. Suçun unsuru niteliğinde olan temadi (kalmaya devam etme) dikkate alındığında, suçla korunan başlıca hukukî yarar, bilişim sistemini kullananların belli bir süreden sonra rahatsız edilmemesidir.

Suçun hedefi durumundaki bilişim sistemi kullanıcılarının (sahiplerinin) çıkarlarının zedelenmemesi de korunan hukukî yararlar arasında sayılabilir. 243. maddede, *"haksız erişim + kalma"* değil, *"haksız erişim + kalmaya devam etme"* suç sayılmıştır. Bir başka anlatımla suçta *"kalma"* yetmemekte *"kalmaya devam etme"* aranmaktadır. *"Kalma"* ve *"kalmaya devam etme"* kavramları eş anlamlı değildir. Kalmaya devam etme, kalmaya göre daha fazla bir süreyi ifade etmektedir. Kalmaya devam etmenin belli bir süre gerektirmesi nedeniyle 243. maddedeki suç, *"zorunlu mütemadi suçlar"*ın bir örneğini teşkil etmektedir[12]. Suçta gerekli olan *"kalmaya devam etme",* fiilin ve failin özelliklerine göre her somut olayda hâkim tarafından belirlenecektir.

243. maddede, Avrupa Konseyi Siber Suç Sözleşmesi'nin *"Haksız erişim"* başlıklı 2. maddesindeki düzenlemede olduğu gibi *"Bir bilişim sisteminin bütününe veya bir kısmına"* ibaresi kullanılmıştır. Teknik yapısı ve niteliği göz önüne alındığında bir bilişim sisteminin bütününe girilmesinin zorluğu karşısında, maddede *"bütününe veya bir kısmına"* şeklindeki bir ayırım yerine *"bir bilişim sistemine"* ibaresinin kullanılmış olması daha yerinde olurdu. 243. maddedeki suçta öngörülen fiilin *"hukuka aykırı olarak"* gerçekleştirilmesi aranmıştır. Bir suç maddesinde anılan ibareye yer verilmesi, *"hukuka özel aykırılık hali"* olarak nitelendirilebilir ve bu durumda failin kastının, hukuka aykırılığı da ayrıca kapsamış olması aranmaktadır[13].

---

11 Paralellik taşıdığı düşüncesi için bkz.: Murat Volkan Dülger, Bilişim Suçları, Seçkin Yayınevi, Ankara, 2004, s.212.

12 Zorunlu mütemadi suç için bkz.: Timur Demirbaş, Ceza Hukuku Genel Hükümler, Ankara, 6. Baskı, Seçkin Yayınevi, 2009, s.229.

13 "Hukuka aykırılığın kanunda ayrıca belirtildiği suç tiplerine, *tam olmayan suçlar* denir. Bu suç tipleri ihlâl edildiği zaman, hâkim bu ihlâlin hukuka aykırılığı da ihtiva ettiği ve hukuka aykırılığın karinesini teşkil ettiği esasından hareket edemeyecektir. Yani, hâkimin bu suçlarda hukuka

Uygulamada 243. maddedeki suç, genellikle bir bilişim sistemine yetkisi olmaksızın uzaktan veya ağ üzerinden gizli erişimle işlenmektedir. Erişimin teknik açıdan değişik yol ve yöntemlerinden söz edilebilir. Bilinen yaygın yöntemlerden birisi *"casus yazılım"* kullanmaktır. Ancak bilgi ve iletişim teknolojisindeki ortaya çıkan yenilik ve olanaklar, bu suçun yeni işlenebilme yöntemlerini de beraberinde getirmektedir.

Haksız erişimde temel hedef, güvenlik yapılarını aşarak ya da yeterli koruma olmamasından yararlanarak bir bilişim sistemine veya bilişim ağına erişim elde etmektir. Faillerin hareketleri, geniş ölçüde kâr amaçlı ya da eğlence eksenli olabilir. Failler, kâr amaçlı haksız erişimlerde özel kurumları veya özel bilgi kaynaklarını hedef almaktadırlar. Eğlence arayan failler ise yeterli koruması bulunmayan veya kolay erişim imkânı olan hedeflere değişik oyunlarla veya aldatmacalarla yönelmektedirler[14].

İşlenme şekli de dikkate alındığında bu suç, herkes tarafından fark edilemez. Özellikle failin bilişim alanındaki bilgisi, yeteneği ve elindeki imkânlara (araçlara, yazılımlara) bağlı olarak suçta kullandığı yöntemler, mağdurun bu suça maruz kaldığını tek başına fark edebilmesini neredeyse imkânsız kılmaktadır. Üstelik bilişim alanındaki sürekli katlanarak devam eden gelişmeler karşısında bilişim sistemlerine haksız erişimin benzerine rastlanmayan yeni biçimlerinin ortaya çıkması sorunu daha da artırmaktadır. Bu suçu, bilişim alanında teknik bilgiye, casus yazılımlar konusunda deneyime sahip örneğin bilişim yöneticileri, adli bilişim uzmanları gibi kişiler tespit edebilirler.

2) Suçun Bedeli Karşılığında Yararlanılabilen Sistemler Hakkında İşlenmesi

243. maddenin (2) numaralı fıkrasında, girme ve orada kalmaya devam etme fiilinin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde verilecek cezanın yarı oranına kadar indirilmesi öngörülmüştür.

"Bedeli karşılığında yararlanılabilen sistemler" kavramı bilişim suçları bakımından Türk Ceza Kanununa ilk defa girmiştir. 5237 sayılı TCK'nın 163. maddesinin (1) numaralı fıkrasında[15], otomatlar aracılığı ile sunulan

aykırılığın varlığını ayrıca tespit etmesi zorunludur. Çünkü, bu suçlarda failin kusurunun, hukuka özel aykırılığı da kapsaması zorunludur"; Timur Demirbaş, s.252.

14 Computer Crime and Information Technology Security, s.243.

15 "Karşılıksız yararlanma
Madde 163- (1) Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan kişi, iki aydan altı aya kadar hapis veya adlî para cezası ile cezalandırılır."

ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan kişi cezalandırıldığı için, otomatlara yönelik söz konusu fiiller 243. madde kapsamında değildir.

Karşılık anlamını da taşıdığı için *"bedel"* kavramını, yalnızca para olarak anlamamak gerekir. Bir hizmetin karşılığı genellikle para ile ödenirse de, bazen başka şeyler de bedel kavramına girebilir. Örneğin, internet ortamında abonelerine hizmet sunan bir site tarafından belirtilen sayıda yayın gönderilmesi halinde üyelik imkânı sağlanacağının duyurulmuş olmasında, istenilen yayın, bedel niteliğini taşıyacağından anılan bedel yerine getirilmeden bu siteye yönelik suçta (2) numaralı fıkradan indirime gidilmesi gereklidir.

243. maddenin (2) numaralı fıkrasında verilecek cezada indirim öngörülmesi, işin mahiyeti itibarıyla yerinde bir düzenlemedir. (2) numaralı fıkradaki suça konu bir bilişim sistemi, tamamen erişime kapalı olmayıp, bedel koşulu yerine getirildiğinde erişime açık hale gelmektedir. Oysa 243. maddenin (1) numaralı fıkrasında, başkalarının erişimine tamamen yasak olan (izin verilmeyen) bir bilişim sistemi söz konusudur. (1) numaralı fıkradaki bilişim sistemi bir kişinin dışa kapalı olan konutuna, (2) numaralı fıkradaki bilişim sistemi ise bedel ödeyenlerin (üyelerinin) girmesine müsaade edilen bir işyerine benzetilebilir; bu binalara yönelik dokunulmazlıkların ihlâli aynı vehamette olamaz[16]. Benzer şekilde, dışa tümüyle kapalı olan bir bilişim sisteminde korunan hukukî yarar ile bedel ön koşuluyla dışa açık hale gelen bir bilişim sistemindeki korunan hukukî yarar aynı nitelik ve önemi haiz değildir.

3) Fiil Nedeniyle Sistemdeki Verilerin Yok Olması veya Değişmesi

243. maddenin (3) numaralı fıkrasında *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."* denilmiştir. 243. maddenin (3) numaralı fıkrası, Fransız Ceza Kanununun 323-1. maddesindeki *"Fiil, sistemdeki bir verinin yok olmasına veya değişmesine veya sistemin fonksiyonunun herhangi bir*

[16] Nitekim, 5237 sayılı TCK'nın 116. maddesinin (1) numaralı fıkrasında "Bir kimsenin konutuna, konutunun eklentilerine rızasına aykırı olarak giren veya rıza ile girdikten sonra buradan çıkmayan kişi, mağdurun şikayeti üzerine, altı aydan iki yıla kadar hapis cezası ile cezalandırılır." denilmiş; maddenin (2) numaralı fıkrasında ise "Birinci fıkra kapsamına giren fiillerin, açık bir rızaya gerek duyulmaksızın girilmesi mutat olan yerler dışında kalan işyerleri ve eklentileri hakkında işlenmesi hâlinde, mağdurun şikâyeti üzerine altı aydan bir yıla kadar hapis veya adlî para cezasına hükmolunur." hükmüyle, girilmesi mutat olmayan işyeri ve eklentilerinin dokunulmazlığının ihlâlinde cezanın üst sınırı yarı oranında az öngörülmüştür.

şekilde değişimine neden olursa hapis cezası üç yıla, para cezası 45.000 Euroya kadardır." hükmüne kısmen bezmektedir[17].

5237 sayılı TCK'nın 243. maddesinin (3) numaralı fıkrasında, verinin yok olması veya değişmesinde failin kastının bulunup bulunmaması gerektiği açıkça belirtilmemiştir. (3) numaralı fıkrada *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse"* ibaresi kullanılmıştır. Burada *"yok olur veya değişirse"* ibareleri pasif niteliktedir ve verinin yok olmasında veya değişmesinde faile değil, fiile vurgu yapılmıştır. Başka bir anlatımla maddede örneğin *"her kim veriyi yok eder veya değiştirirse"* şeklinde, failin kastını gerektiren bir ifade yer almamıştır. Bu nedenle 243. maddenin (3) numaralı fıkrasında, girme ve orada kalmaya devam etme fiilinin sonucunda verinin yol olması veya değişmesi neticesi esas alınmıştır. Yalnızca (3) numaralı fıkranın kaleme alınış biçimi dahi, veriyi yok etme veya değiştirme konusunda failin bir kastının olmaması gerektiğini ortaya koymaktadır.

Bunun dışında 5237 sayılı TCK'nın 244. maddesinin (2) numaralı fıkrasındaki *"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."* hükmüyle, bir bilişim sistemindeki verinin kasten yok edilmesi veya değiştirilmesinin ayrı bir suç olarak düzenlenmiş olduğu da gözetildiğinde, 243. maddenin (3) numaralı fıkrasında failin belirtilen seçimlik sonuçlar için kastının olmaması gerekir. Eğer fail, bir bilişim sistemine haksız olarak girip, orada kalmaya devam ederken sistemdeki bir veriyi kasten yok eder veya değiştirirse, bu fiil için 243. maddenin (3) numaralı fıkrası değil, 244. maddenin (2) numaralı fıkrası uygulanmalıdır. 243. maddenin (3) numaralı fıkrası, 5237 sayılı TCK'nın 23. maddesindeki netice sebebiyle ağırlaşmış suçun bir örneğini teşkil etmektedir.

5237 sayılı TCK'nın 23. maddesindeki *"Bir fiilin, kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet vermesi halinde, kişinin bundan dolayı sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir."* hükmü gereğince, 243. maddenin (3) numaralı fıkrasının uygulanabilmesi için, verinin yok edilmesi veya değişmesinde failin taksir derecesinde kusurunun bulunması gereklidir. 243. maddenin (3) numaralı fıkrasındaki sonuç, 243. maddenin (1)

[17] Fransız Ceza Kanunu'nundaki bu hükme ilişkin olarak bkz.: İleride "6) 243. Maddenin Son Fıkrasına, Fiil Nedeniyle Bilişim Sisteminin İşleyişinin Etkilenmesi de Eklenmelidir" başlığına.

veya (2) numaralı fıkrası kapsamındaki bir fiilden kaynaklanabilir. Failin 243. maddenin (1) ya da (2) numaralı fıkra kapsamına giren fiili nedeniyle, sistemdeki veri yok olmuş veya değişmişse, burada (1) veya (2) numaralı fıkra değil yalnızca (3) numaralı fıkradaki ceza uygulanacaktır.

B- Ülkemizde TCK'nın 243. maddesine ilişkin İstatistikî Veriler

1) Soruşturma ve Kovuşturma Konusunda

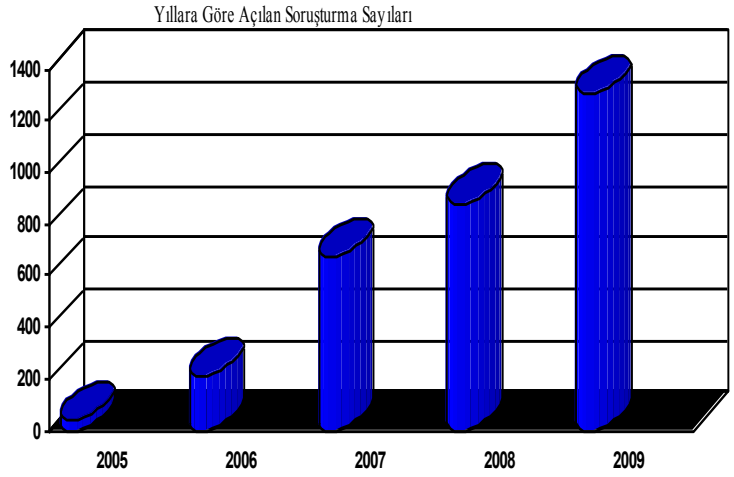
Ülkemizde TCK'nın 243. maddesine ilişkin olarak 2005 ilâ 2009 yıllarındaki[18] istatistikî veriler aşağıdaki Tabloda gösterilmiştir:

Konular	2005	2006	2007	2008	2009
Açılan Soruşturma Sayısı	40	210	672	882	1307
Tutuklanan Kişi Sayısı	0	3	17	19	11
İddianame Sayısı	12	67	182	238	282
Dava Açılma Oranı (%)	30	32	27	27	21,6
Kovuşturmaya Yer Olmadığı Kararı	14	43	178	176	251
Görevsizlik	0	1	1	5	7
Yetkisizlik	8	71	218	285	398
Fezleke	1	4	4	12	6
Birleştirme	1	3	23	41	45

Tablo – 243. maddeye ilişkin istatistikî veriler

Yıllara göre 5237 sayılı TCK'nın 243. maddesinden açılan soruşturma sayıları ise aşağıdaki grafikte gösterilmiştir:

[18] 1- Uyap projesi kapsamında işletim çalışması 2004 Yılında pilot adliyelerde başlatılmış olup, 2008 yılında yaygınlaştırma çalışmaları kapsamında tüm Türkiye genelinde işletim çalışması tamamlanmıştır. Bu nedenle işletim çalışmasının tamamlandığı yılların öncesine ilişkin bilgilerde, mahkemelerin giriş yapabildiği dosya sayıları vardır. Bu nedenle 2007 ve 2009 yıllarına dair veriler değerlendirilmesi gerekmektedir. 2005 ilâ 2006 yıllarına ilişkin verilere ise pilot bölgelerle sınırlı da olsa, 5237 sayılı TCK'nın 243. maddesiyle ilgili ilk uygulama bilgilerini içermesi açısından tabloda yer verilmiştir.
2- Bir savcılıktan diğer bir savcılığa görevsizlik, yetkisizlik ve fezleke ile gönderilen dosyalar har savcılık için ayrı ayrı görülmektedir.
3- Tutuklanan kişi sayısı, soruşturma aşamısında, savcılık talebi ile tutuklananan ile yargılama aşamasında dava dosyasında yapılan tutuklamaları kapsamaktadır.



Yukarıdaki bilgilere göre, 5237 sayılı Türk Ceza Kanununun yürürlüğe girdiği 1 Haziran 2005 tarihinden itibaren 243. maddeye ilişkin açılan soruşturma sayılarında yıllara göre sürekli bir artış söz konusudur.

2005 yılında, 1 Haziran 2005 ilâ 31 Aralık 2005 tarihleri arasındaki yedi aylık sürede 40 soruşturma açılmışken, yıllık düzeyde yaklaşık olarak bu rakam; bir önceki yıla göre 2006 yılında % 200'den fazla, 2007 yılında % 220, 2008 yılında % 31, 2009 yılında ise % 48 oranında artmıştır.

Bu artışta, sadece işlenen suç sayısının yükselmesi değil, aynı zamanda suça maruz kalanların bu konudaki farkındalıklarının artması da etkili olmuştur denilebilir. Bununla birlikte, yıllara göre 243. madde kapsamında açılan dava oranında ise düşüş söz konusudur.

2) Yargıtay Kararları

5237 sayılı TCK'nın 243. maddesine ilişkin Yargıtay kararlarına az da olsa rastlamak mümkündür. Bunlardan bazılarını ele alabiliriz:

- Bilişim sistemine hukuka aykırı müdahale ederek haksız çıkar sağladığı suçlamasıyla fail hakkında 5237 sayılı TCK'nın 244. maddenin (4) numaralı fıkrasından açılan kamu davasında yerel mahkemece verilen kararı inceleyen Yargıtay:

"Sanığın, katılanın yetkilisi olduğu Z... Tekstil İmalat Pazarlama Sanayi ve Ticaret Limited şirketinin ... Bankası Denizli şubesinde bulunan hesa-

bına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK'nun 243/1.maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK. nun 244/4, 35/2. maddeleri gereğince) hüküm.."[19] *tesis etmenin yasaya aykırı* olduğu sonucuna varmıştır.

Kararda sanığın bilişim sistemine haksız erişim yaptıktan sonra, iddiaya konu başkasına ait banka hesabında oynama yapmak suretiyle para havalesi yapmadığı kabul edildiğine göre, fiil TCK'nın 244. maddesinin (4) numaralı fıkrasındaki var olan verileri başka bir yere göndererek kendisine haksız çıkar sağlama niteliğinde olmadığından, 243. maddenin (1) numaralı fıkrasına uymaktadır.

Sanığın bilişim sistemine haksız erişimden sonra, *"orada kalmaya devam etme"* fiilini gerçekleştirme konusu Yargıtay kararında açık olmamakla birlikte, sanığın bilişim sistemine haksız erişimden sonra, başkasına ait banka hesabına girdiği ve hesapta oynama yaparak para havalesi yapacak kadar sistemde kaldığı da kabul edildiğine göre, 243. maddedeki *"orada kalmaya devam etme"* olgusunun gerçekleştiği sonucuna varıldığı söylenebilir.

- 5237 sayılı TCK'nın 243. maddesinin (1) ve (2) numaralı fıkraları uyarınca 50 TL adli para cezasıyla sanığın cezalandırılmasına dair yerel mahkeme kararının Cumhuriyet savcısının suç vasfına yönelik temyiz istemini değerlendiren Yargıtay tarafından, … (TV yayın) şifresinin müdahil şirkete ait decoder dışında özel bir alet yardımıyla çözüldüğü saptanamadığına göre, abonelik sözleşmesiyle evinde kullanılmak üzere alınan decoderin, sözleşme hükümlerine aykırı olarak başka yerde kullanılmasından ibaret eylemin hukukî nitelikte bulunduğuna ve 243. madde kapsamına girmediğine karar verilmiştir[20].

Yargıtay kararında, şifrenin decoder dışında özel bir alet yardımıyla çözüldüğü saptanamadığı belirtilerek, sisteme girildiğinin belirlenememiş olduğu ve dolayısıyla 243. maddenin tartışılamayacağı üzerinde isabetli olarak durulmuştur.

[19] 11. CD., 26.03.2009, E.2008/18190, K.2009/3058.
[20] 11. CD., 13.04.2009, E.2006/7779, K.2009/4153.

II- BİLİŞİM SUÇLARINDA YENİ DÜZENLEME İHTİYACI

A- 5237 sayılı TCK'nın 243. Maddesiyle İlgili Olarak

Bilişim sistemlerine haksız erişim, bilişim suçlarında ve bu suçlarla mücadelede adeta giriş kapısı niteliğindedir. Çoğunlukla bilişim suçlarının işlenmesinin ön koşulu haksız erişimdir. Haksız erişim sanıldığı kadar basit ve masum bir fiil değildir. Haksız erişimle, klasik suçlarla mukayese edilemeyecek boyutlarda bilişim sistemlerine, içerisindeki verilere ve gizli bilgilere ulaşılabilir. Bunun faillere sağlayacağı yararın yanında, bilişim sistemlerine getireceği zarar akla gelebilecek hususlardır. Ancak haksız erişimin neden olduğu sonuçlar kimi zaman bunlarla sınırlı olmayabilir. Bu bağlamda, Ülkemizde yakın zamanda yaşanan bilişim sistemlerindeki ülke çapında uygulanan farklı alanlardaki sınav sorularına haksız erişimle ulaşıldığı isnadları ve bunun devamında sınavların iptal edilmesi, atamaların yapılamaması, bazı tamamlanmış işlemlerin riske girmesi gibi hususlar, haksız erişim suçunun sadece fail ve bilişim sistemi ile sınırlı sonuçlar doğurmadığını, bunun dışında kalan pek çok kişi ve kurumu, hatta ülkeyi etkilediğini açıkça ortaya koymaktadır. Aşağıda 5237 sayılı TCK'nın 243. maddesiyle ilgili olarak öncelikle yapılması gereken tartışma ve düzenlemelere başlıklar halinde temas edilmiştir.

1) Maddedeki *"ve"* İbaresi *"veya"* Olarak Değiştirilmelidir

Yukarıda 5237 sayılı TCK'nın 243. maddesindeki suçun temel şekli ele alınırken (1) numaralı fıkradaki *"veya"* kelimesinin *"ve"* yapılmış olmasının yerinde olmadığını belirtmiştik.

Şu ana kadar Türkiye Avrupa Konseyi Siber Suç Sözleşmesini imzalamamıştır. Ülkemizin Siber Suç Sözleşmesini imzalaması yararlı ve gerekli bir adım olacaktır. Ancak, Sözleşmeyi imzalayan akit tarafların iç hukuklarını da buna uygun hale getirme yükümlülükleri gözetildiğinde Ülkemiz, Avrupa Konseyi Siber Suç Sözleşmeni imzalamadan önce 5237 sayılı TCK'nın 243. maddesinin (1) numaralı fıkrasındaki *"ve"* ibaresi *"veya"* şeklinde değiştirilmeli; bilişim sistemlerine haksız erişim (girme) tek başına suç haline getirilmelidir.

2) Sisteme Hukuka Uygun Girdikten Sonra, Hukuka Aykırı Olarak Kalma Maddeye Eklenmelidir

Bir bilişim sistemine hukuka uygun olarak girdikten sonra orada hukuka aykırı olarak kalmaya devam etme, 5237 sayılı TCK'nın 243. maddesindeki suçun kaleme alınış şekli de dikkate alındığında suçta kanunilik il-

kesi gereğince suç tanımına girmemektedir. Çünkü 243. maddede *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden"* denilmekle, suçtan söz edilebilmesi için bilişim sistemine öncelikle hukuka aykırı olarak girilmesi ön koşul niteliğindedir. Bir bilişim sistemine hukuka uygun olarak girdikten sonra, hukuka aykırı olarak orada kalmaya devam etme de, ayrıca suç sayılacak şekilde konut dokunulmazlığına ilişkin 116. maddedeki gibi[21] yapılacak bir düzenleme ile mevcut hukukî boşluk giderilmelidir. Esasında bu sorun, 243. maddenin (1) numaralı fıkrasındaki *"veya"* kelimesi *"ve"* olarak değiştirildiğinde kendiliğinden halledilmiş olacaktır.

ABD'de CFAA'da yetkisiz erişim bağlamında düzenlenen *"yetkili erişimin aşılması"* fiilleri uygulamada önemli bir yer tutmaktadır. Yetkili erişimin aşılması suçu, erişimcinin sahip olduğu erişim yetkisini aşması, ihlâl etmesi şeklinde geniş bir kapsama sahiptir. Erişimci, erişim konusundaki yetkisini aşarak, bilgilere ulaşmakta ya da bunları değiştirmektedir[22]. Yukarıda ele aldığımız 5237 sayılı TCK'nın 243. maddesi açısından hukuka uygun olarak bir bilişim sistemine girip orada kalmaya devam eden kişinin daha sonra yetkisi kapsamındaki süresinin dolmasına rağmen sistemde hukuka aykırı olarak kalmaya devam etmesi konusu, CFAA'daki *"yetkili erişimin aşılması"* suçundan daha dar ve farklıdır.

Bu başlık altındaki önerimiz değerlendirilirken, CFAA'daki *"yetkili erişimin aşılması"* fiilleri de birlikte ele alınıp, konu kapsamlı bir şekilde çözüme kavuşturulmalıdır.

3) Şifre veya Benzeri Yapıyla Korunan Bir Bilişim Sisteminin, 243. Maddedeki Suçun Ön Koşulu Olması Düşünülmelidir

Bilişim sistemlerini kullananların farkındalığının artırılmasının bilişim suçlarıyla mücadeledeki tartışılmaz önemi dikkate alınarak, bilgisayarlarda ve/veya bilişim sistemlerinde gerekli şifre vs. önlemlerin alınmasını sağlamak amacıyla, 243. maddede yeni düzenlemeye gidilebilir. Bu konuda karşılaştırmalı hukukta örnekler bulunmaktadır.

Finlandiya Ceza Kanununda *"Her kim, kendisine ait olmayan bir kodu kullanarak veya bir koruma sistemini etkisiz hale getirerek, elektronik veya diğer teknik bir yöntemle veya ayrıca korunan böyle bir sistemin bir*

21 "(1) Bir kimsenin konutuna, konutunun eklentilerine rızasına aykırı olarak giren veya rıza ile girdikten sonra buradan çıkmayan kişi, mağdurun şikayeti üzerine, altı aydan iki yıla kadar hapis cezası ile cezalandırılır." (m.116).

22 Michael Battle, Michael W. Bailie, s.4-10.

kısmında verinin işlendiği, depolandığı veya iletildiği bir bilişim sistemine zorla girerse, veri tecavüzünden bir yıl kadar hapis veya para cezasıyla cezalandırılır"[23] hükmüyle, haksız erişim suçundan söz edilebilmesi için, *"elektronik veya diğer teknik bir yöntemle veya ayrıca korunan bir bilişim sistemi"* gerekmektedir.

Japonya'da 128 sayılı Kanunun 3. maddesinde, bilgisayara yetkisiz erişim suç olarak düzenlenmiştir. Ancak bilgisayara yetkisiz erişim suçundan söz edilebilmesi için, söz konusu bilgisayara fiziken ya da internet yoluyla başkalarının erişimi şifre ile sınırlandırılmış olmalıdır[24]. Başka bir anlatımla, fiziken veya ağ yoluyla mağdura ait bilgisayara girilmesinde şifre engeli bulunmuyorsa, yetkisiz erişim suçundan söz edilemez. Diğer yandan, teknik olarak da bir bilişim sistemi tasarlanırken, erişim kontrollerinin yapılması, özellikle yetkisiz ya da zorla sisteme erişimlerin olabileceğinin göz önünde bulundurulması ve gerekli güvenlik yapılarının oluşturulması gerekmektedir[25].

Bütün bunlar dikkate alındığında 5237 sayılı TCK'nın 243. maddesindeki suçta, öncelikle anılan koruyucu önlemleri almamış olanların maruz kaldıkları haksız erişim fiilleri daha az bir cezayla korunabilir; gerekli önlemleri almış olanlar ise daha fazla bir ceza ile korumaya tabi tutulabilir ya da daha etkili bir yaklaşımla koruyucu önlemleri almayanların maruz kaldıkları haksız erişim, suç sayılmayabilir. Böylece bu suçla mücadelede, bilişim sistemlerini kullananların farkındalıkları artırılarak aktif katkıları sağlanabilir.

4) Bilişim Sistemine Girmeksizin İzleme Fiili de Maddeye Eklenmelidir

Bilişim teknolojilerindeki gelişme ve imkânlar gözetilerek 5237 sayılı TCK'nın 243. maddesinde, bir bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme suçuna, *"bilişim sistemine girmeksizin verilerin izlenmesi fiili"* de eklenmelidir. Nitekim bu husus Adalet Bakanlığı tarafından kurulan Komisyon tarafından hazırlanan 2007 Tasarısında[26] yer almıştır.

---

23 Dave Kleiman, s.892-893.

24 Stein Schjolberg, *"The Legal Framework - Unauthorized Access To Computer Systems, Penal Legislation in 44 Countries"*, http://www.mosstingrett.no/info/legal.html (15.7.2010).

25 Dennis C. Brewer, Security Controls for Sarbanes-Oxley Section 404 IT Compliance: Authorization, Authentication, and Access, Canada, Wiley Publishing, Inc., 2006, s.67.

26 "**Bilişim sistemine girme ve veri elde etme**

Benzer bir düzenleme, Finlandiya Ceza Kanununda, bilişim sistemine haksız erişim suçunun hemen devamında *"Bir bilişim sistemine zorla girmeksizin, özel teknik aygıtlar kullanarak böyle bir bilgisayardan bilgi elde etmek de veri tecavüzüdür"*[27] denilerek yer almıştır.

5) Suça Konu Bilişim Sisteminin Niteliği Dikkate Alınmalıdır

Suça konu bilişim sisteminin kamu veya özel kesime ait olması konusunda 5237 sayılı TCK'nın 243. maddesinde bir fark öngörülmemiştir. Burada özellikle kamuya ait bilişim sistemlerinin başta nitelikleri, etki alanlarının genişliği de gözetilerek, suça daha çok maruz kalma olasılıkları karşısında, karşılaştırmalı hukuktaki örnekler de dikkate alınarak bilişim sisteminin kamuya ait olması suçun nitelikli hali olarak düzenlenmelidir. Ülkemizdeki yakın zamanda görülen sınav sorularının bilişim sistemine haksız erişimle elde edilme iddiaları dahi 5237 sayılı TCK'nın 243. maddesinin bu yönden yetersiz olduğunu ve konunun ne kadar önemli olduğunu ortaya koymaktadır.

5237 sayılı TCK'nın 243. maddesinin son fıkrasında, fiil nedeniyle verilerin yok olması veya değişmesinde ceza ağırlaştırılmış ise de, söz konusu verinin önem ve niteliği ayrıca gözetilmemiştir.

ABD'de her hafta medyadaki raporlarda, Federal Hükümet içerisindeki bilişim sistemlerinin dış erişim kontrollerine ve verilerin korunmasına yönelik bazı vahim yetkisiz erişim olaylarına yer verilmektedir. Bu bağlamda devletlerin vatandaşların özel bilgilerini korumada çok duyarlı davranmaları gerektiği kabul edilmektedir. Hatta her seviyedeki kamuya ait bilişim sistemleri haksız erişimlere karşı yasalarla da ayrıca korunmalıdır[28].

Bu bağlamda ABD'de, örneğin yetkisiz erişim veya yetkili erişimin aşılması ulusal güvenlik bilgilerine ilişkin ise CFAA (Title 18, United States Code, Section 1030(a)(1)'da konu ayrıntılı bir biçimde ayrıca düzenlenerek farklı yaptırımlar öngörülmüştür[29].

MADDE 15 - (1) Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren veya sistemde kalmaya devam eden kişi altı aydan iki yıla kadar hapis cezası veya üçbin güne kadar adlî para cezası ile cezalandırılır. **Sisteme girmeksizin verilerin izlenmesi halinde, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, bu fıkraya göre cezaya hükmolunur…"** (Tasarı).

27 Dave Kleiman, s.892-893.

28 Dennis C. Brewer, s.69.

29 Michael Battle, Michael W. Bailie, s. 10 vd.

Bulgaristan'da bilişim sistemine haksız erişimin, kamuya ait gizli bilgilere yönelik olması halinde, bir yıldan üç yıla kadar hapis, fiil dolayısıyla ağır sonuçların meydana gelmesi halinde ise bir yıldan sekiz yıla kadar hapis cezası söz konusudur[30].

Bu nedenlerle, 5237 sayılı TCK'nın 243. maddesinde de konu yeniden ele alınarak düzenleme yoluna gidilmelidir.

6) 243. Maddenin Son Fıkrasına, Fiil Nedeniyle Bilişim Sisteminin İşleyişinin Etkilenmesi de Eklenmelidir

5237 sayılı TCK'nın 243. maddesindeki fiil nedeniyle failin kastı olmaksızın (taksirle), *"bilişim sisteminin işleyişinin herhangi bir şekilde değişimine neden olunması"* da mümkün olduğu halde, bu husus 243. maddenin (3) numaralı fıkrasında yer almamıştır. Üstelik bilişim sisteminin işleyişinde bu yöndeki bir değişiklik, bir verinin yok edilmesi veya değiştirilmesinden çok daha önemli olabilir ya da ağır sonuçları ortaya çıkarabilir. Fransız Ceza Kanununun 323-1. maddesinde, sistemdeki bir verinin yok olması veya değişmesinden başka ayrıca *"veya sistemin fonksiyonunun herhangi bir şekilde değişimine neden olursa"* şeklinde bir düzenleme yer almıştır.

5237 sayılı TCK'nın 243. maddesinin (3) numaralı fıkrasına, haksız erişim nedeniyle *"bilişim sisteminin işleyişinin herhangi bir şekilde değişimine neden olunması"* da seçenek sonuç olarak eklenmelidir.

7) Haksız Erişim Nedeniyle Başkalarının Erişimine Olanak Sağlanması Suça Tesir Eden Sebep Sayılmalıdır

Bir bilişim sistemine haksız erişimin sistemde oluşturabileceği bir açık (gedik) nedeniyle başkalarının (3. kişilerin) erişim sağlamaları veya veri elde etmeleri söz konusu olabilir. Esasında bu husus, 5237 sayılı TCK'nın 243. maddesinin (3) numaralı fıkrasına benzer görünmekte ise de niteliği itibarıyla farklılık taşımaktadır. Çünkü 243. maddenin (3) numaralı fıkrasında fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi ele alınmıştır. Tartışılan konu ise haksız erişimin bilişim sisteminde neden olduğu açığın, ortaya çıkardığı başkalarının haksız erişim ya da veri elde edebilme olanağıdır.

Letonya'da 17 Haziran 1998 tarihinde kabul edilen yeni Ceza Kanununun bilişim suçlarına ilişkin hükümlerinin yer aldığı *"Genel Güvenliğe ve*

30 Dave Kleiman, s. 885.

Kamu Düzenine Karşı Suçlar" başlıklı XX. Bölümündeki *"Bilişim Sistemlerine Haksız Erişim"* başlıklı 241. maddesinde;

"(1) Her kim bir bilişim sistemine haksız (keyfi) olarak erişirse; eğer bu fiil sistemden başkalarının bilgi elde etmelerine neden olursa, hapis veya aylık asgari ücretin 80 katını geçmemek üzere para cezasıyla cezalandırılır.

(2) Her kim aynı fiili işler ve eğer fiil nedeniyle bilişim sistemini koruma yazılımında veya iletişim hatlarına erişimde gedik açarsa (breaching), bir yılı geçmemek üzere hapis veya aylık asgari ücretin 150 katını geçmemek üzere para cezasıyla cezalandırılır.[31]*"*hükmüne yer verilmiştir.

5237 sayılı TCK'nın 243. maddesinde de Letonya'daki kademeli düzenleme de gözetilerek belirtilen eksikliğin giderilmesi yararlı olacaktır.

B- Diğer Bazı Konular

5237 sayılı TCK'da, bilişim suçları açısından, aşağıda değinilecek konularda düzenleme yapılması gerekliliği, karşılaştırmalı hukuktaki örnekler de gözetilerek etraflıca tartışılmalıdır:

1) Bilişim Suçlarının İşlenmesinin Hazırlığına İlişkin Suçlar

TCK'nın 243. maddesindeki suçta, bilişim verilerine yönelik suçların hazırlığına dair suçlar yer almamıştır.

Alman Ceza Kanununun *"veri casusluğunun ve verilerin iletilirken ele geçirilmesinin hazırlığı"* başlıklı 202c maddesinde, madde başlığında belirtilen suçların işlenmesini hazırlamak üzere her kim;

1. Verilere giriş yapmayı sağlayan şifre ve sair güvenlik kodlarını veya

2. Bu tür fiilleri işlemeyi amaçlayan bilgisayar programlarını

üretir; kendisine veya bir başkasına sağlar, satar veya bir başkasına verir, yayar veya sair şekilde ulaşılabilmesini sağlarsa, bir yıla kadar hapis cezası veya adli para cezası ile cezalandırılmaktadır. Burada Alman Ceza Kanununun para ve kıymetli damgalarda sahteciliğin (yani kalpazanlığın) hazırlığına dair 149. maddesinin ilgili hükümleri kıyasen uygulanmaktadır[32].

---

31 Dave Kleiman, s.898-899.

32 Feridun Yenisey, Gottfried Plagemann, 15 Mayıs 1871 tarihli Alman Ceza Kanunu, Strafgesetzbuch, İstanbul, Beta Yayım, 2009, s.277, 224-225.

Yukarıda temas edildiği üzere, haksız erişimin suç sayıldığı bilişim sisteminin şifre ve sair güvenlik önlemiyle korunuyor olması, bilişim suçlarıyla mücadelede büyük önem taşımaktadır. Bunun doğal bir sonucu olarak da, bazı düzenlemelerde bilişim sistemlerindeki *"şifre"* ve benzeri *"güvenlik yapıları"*nın ele geçirilmesi ya da bunu sağlayan şifre çözücülerin ya da güvenlik yapılarını ortadan kaldıran bilgisayar programlarının üretimi, sağlanması … vs. de ayrıca suç sayılmaktadır.

Estonya, 12 Mayıs 2003 tarihinde Avrupa Konseyi Siber Suç Sözleşmesini onaylamak için, Ceza Kanununda uyum amacıyla değişiklikler yapmıştır. Estonya Ceza Kanununun *"Korunan kodları ele geçirmek"* başlıklı 284. maddesine göre, bir bilgisayarı, bilişim sistemini veya bilişim ağını koruyan kodu hukuka aykırı olarak ele geçiren, eğer kişisel bir kazanç elde etmek için fiili işlemişse ve bu fiil sonucu önemli bir zarar veya diğer ciddi sonuçlar meydana gelirse, 3 yıla kadar hapis veya para cezası verilir[33]. 5237 sayılı TCK'da, 243. maddesindeki suçla bağlantılı olarak belirtilen örnekler de dikkate alınarak bilişim verilerine yönelik suçların hazırlığına dair suçlara yer verilmelidir.

2) Bilişim Suçlarının İştirak Halinde İşlenmesi

5237 sayılı TCK'da bilişim suçlarının birden fazla kişi tarafından iştirak halinde işlenmesi, ayrıca suça tesir eden sebep olarak öngörülmemiştir. Karşılaştırmalı hukukta konuyla ilgili düzenlemeler söz konusudur.

Bulgaristan'da 13 Eylül 2002'de kabul edilen Ceza Kanununun *"Siber Suç"* başlıklı yeni bölümündeki 319a maddesinin (1) numaralı fıkrasında, bir kişinin bir bilgisayar kaynağına ve kopyalarına yetkisiz erişmesi veya yetkisi olmaksızın bilgisayar verisini kullanması suç sayılmış; (2) numaralı fıkrasında ise anılan fiillerin iki veya daha fazla kişi tarafından birlikte gerçekleştirilmesi suçun nitelikli hali olarak kabul edilmiş ve ceza[34] ağırlaştırılmıştır[35].

Belçika Kasım 2001'de, bilişim suçlarıyla ilgili olarak Ceza Kanununa bazı maddeler eklemiştir. Belçika Ceza Kanununun *"IV. COMPUTER HACKING"* üst başlığı altında yer alan 550(b) maddesinin (1) ve (2) numaralı fıkralarında bilişim sistemine haksız erişim, (3) ve (5) numaralı fıkralarında verilere yönelik suçlar düzenlenmiş; (6) numaralı fıkrasında

33 Dave Kleiman, s.891-892.

34 Suçun basit şeklinde para cezası söz konusuyken, nitelikli halinde bir yıla kadar hapis veya para cezası öngörülmüştür.

35 Dave Kleiman, s.885.

ise yukarıdaki fiillerden birisini emreden ya da tahrik edenin, altı aydan beş yıla kadar hapis ve para cezası veya bunlardan birisiyle cezalandırılması öngörülmüştür[36].

5237 sayılı TCK'da da, başta haksız erişime ilişkin olmak üzere bilişim suçlarının iştirak halinde işlenmesi, ayrıca suça tesir eden neden olarak düzenlenmelidir.

3) Bilişim Suçlarında Örgütlenme

Dünyada bilgisayarların ve bilişim sistemlerinin pek çok klasik suçta örgütlü olarak kullanımı yaygınlaştığı gibi, bu durum bilişim suçlarının işlenmesinde de söz konusudur. Bir başka ifadeyle örgütler suç işlerken, bilişimi fazlasıyla kullanmaktadırlar[37].

Fransız Ceza Kanununun 323-4.maddesine göre, 323-1'deki haksız erişim, 323-2'deki bilişim sisteminin işleyişini engelleme veya bozma, 323-3'deki sahtecilikle ve yasal bir amaç olmaksızın herhangi bir ekipmanı, aracı, bilgisayar programını ithal etmek, tutmak, satmak veya erişilebilir kılmak ya da herhangi bir veriyi tasarlamak suçlarından; birisini veya daha fazlasını gerçekleştirmek amacıyla kurulmuş bir gruba veya gizli bir anlaşmaya katılmak, tasarlanan fiillerin veya işlenen fiilin en ağır cezasıyla cezalandırılmaktadır[38].

Türk Ceza Kanunu Tasarısının[39] *"Suç işlemek için örgütlenme"* kenar başlıklı 351. maddesindeki, *"Yukarıdaki maddelerde öngörülen suçları işlemek için oluşturulmuş bir örgütü kuran veya buna katılan kimselere, işlemek istedikleri suçlardan en ağırının cezası verilir"* hükmüne, 5237 sayılı TCK'da yer verilmemiştir. Tasarıdaki maddede belirtilen *"suçlar"*, bilişim alanındaki suçları ifade etmekteydi[40].

Hükümet Tasarısının 351. maddesinin gerekçesinde, *"maddeyle, suç işlemek için örgütlenme cürmünün özel bir şekli kabul edilmiş bulunmaktadır. Örgütlü suçlarla mücadelede böyle bir hükme kesin ihtiyaç vardır.*

36 Dave Kleiman, s.887-888.
37 Rosa Codina, "Information Age Crime", ScienceDirect – Computer Fraud & Security, June 2003, s.2.
38 Dave Kleiman, s.893-894.
39 Türk Ceza Kanunu Tasarısı, 5237 sayılı Türk Ceza Kanunu olarak kabul edilen metin öncesinde TBMM'ne sevk edilen Hükümet Teklifini ifade etmektedir.
40 Örneğin 346. maddede "Bilişim sistemine girme, verileri tahrip ve bozma" suçu yer almaktaydı.

Tasarının 4 üncü maddesinde[41] *örgütün genel tanımı ve dolayısıyla genel koşulları belirtilmiştir."* denilmekteydi.

Uluslararası boyutta özellikle kredi kartı dolandırıcılığında örgütlü suçluluk yaygınlaşmış durumdadır. Kredi kartı dolandırıcılığında, değişik türde örgütlü suçlar görülmektedir. Kredi kartı dolandırıcıları bir seferde zengin olmaktansa, sistematik şekilde geniş bir zaman dilimi içinde hareket etmeyi tercih etmektedirler. İnternet yoluyla yapılan satışlarda kullanılan kredi kartı bilgilerini, satıcı firmaların kayıtlarından elde eden korsanlar, kredi kartı sahiplerinin hesap hareketlerini takip ederek, ele geçirdikleri kredi kartı bilgileriyle aylık miktarlara yakın alışveriş yapmaktadırlar. Bu alışverişlerde, alınan mallar ve satıcı firmalar hayalidir (sahtedir). Bu suç yapısında, firma yetkilileri de bu suçun içerisindedirler ve örgütlü hareket söz konusudur[42]. Üstelik anılan suçların işlenmesinden önce çoğu zaman haksız erişim fiilleri gerçekleştirilmektedir. Bu nedenlerle, 5237 sayılı TCK'da başta haksız erişim suçu açısından olmak üzere, Hükümet Tasarısındaki *"Suç işlemek için örgütlenme"* kenar başlıklı 351. maddesindeki gibi bir hükme yer verilmesi gereklidir.

4) Teşebbüsün Tamamlanmış Suç Sayıldığı Durumlar

Suç ve ceza siyaseti açısından bazı bilişim suçlarının[43] teşebbüsü dahi, tamamlanmış suç sayılmıştır. Belçika Ceza Kanununun 550(b) maddesinin; (1) numaralı fıkrasındaki haksız erişimin işlenmeye teşebbüs edilmesi dahi tamamlanmış suç olarak kabul edilmiştir. Finlandiya Ceza Kanununda da bilişim sistemine zorla girme fiilinin teşebbüsünde benzer bir düzenleme yer almaktadır[44]. Suç ve ceza siyaseti açısından, 5237 sayılı TCK'nında bilişim suçlarının, teşebbüs açısından yeniden gözden geçirilmesinin yararlı olacağı düşünülmektedir.

5) Veri veya Programları Hukuka Aykırı Olarak Elde Etme

5237 sayılı TCK'nın hırsızlığa ilişkin 142. maddesinin (2) numaralı fıkrasının (e) bendinde hırsızlık suçunun *"Bilişim sistemlerinin kullanılması*

41 "Örgüt deyiminden, önceden belirlenmemiş suçları işlemek üzere anlaşmış ve birleşmiş birden çok kişinin yapılanmaları ve birleşmenin dıştan gözlemi yapılabilecek biçimde oluşturulmuş bulunması anlaşılır" (Hükümet Tasarısı m.4/8. bent).

42 Fred, Cohen, *"Computer Fraud Scenarios"*, Computer & Security, Volume 2003, Issue 1, January 2003, s.16-17.

43 Örneğin 5237 sayılı TCK'nın "Kamu görevinin usulsüz olarak üstlenilmesi" başlıklı 262. maddesinde "Bir kamu görevini, kanun ve nizamlara aykırı olarak yerine getirmeye teşebbüs eden veya terk emri kendisine bildirilmiş olduğu halde görevi sürdüren kimseye üç aydan iki yıla kadar hapis cezası verilir." denilmiştir.

44 Dave Kleiman, s.892-893.

suretiyle" işlenmesi, 158. maddesinin (1) numaralı fıkrasının (f) bendinde ise dolandırıcılık suçunun *"Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"* işlenmesi suçların nitelikli halleri olarak belirtilmiştir.

Bu düzenlemelerin, yürürlükten kaldırılan 765 sayılı Türk Ceza Kanununun 525a/1 maddesindeki bir bilişim sisteminden *"program, veri veya başka bir unsuru"* hukuka aykırı olarak *"ele geçirme"* hükmünü tamamen karşılamadığını düşünmekteyiz.

Örneğin 5237 sayılı TCK'nın 243. maddesinde fail hukuka aykırı olarak bir bilişim sistemine girer ve orada kalmaya devam ettiği sırada sistemden çok önemli bilgileri kopyalamadan öğrenir. Bu fiil, 5237 sayılı TCK'nın 142/2-e maddesine uyan bir hırsızlık ya da 158/1-f maddelerine uyan dolandırıcılık sayılabilecek midir? Bir kere örnekteki fiil, dolandırıcılık değildir; hırsızlığın ise başta sanığın kastı açısından olmak üzere tartışmalı olacağını düşünmekteyiz.

Nitekim Adalet Bakanlığı tarafından oluşturulan komisyonca hazırlanan 2007 Tasarısında, *"Bilişim sistemine girme ve veri elde etme"* başlıklı 15. maddenin (1) numaralı fıkrasında bilişim sistemine haksız erişim suç sayılmış, (2) numaralı fıkrasında ise *"Bir bilişim sistemindeki veri veya programları hukuka aykırı olarak elde eden kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."*; (3) numaralı fıkrasında ise *"İkinci fıkrada belirtildiği şekilde elde edilen veri veya programların başkalarına iletilmesi hâlinde, verilecek ceza yarı oranında artırılır."* hükmüne yer verilmiştir. 2007 Tasarısının 15. maddesinin (2) numaralı fıkrasındaki düzenleme, 5237 sayılı Türk Ceza Kanununa alınmalıdır.

SONUÇ

Bir bilişim sistemine haksız erişim, bilişim suçlarının ilkini ve en yaygın olanını teşkil etmektedir. Her geçen gün kamu ve özel kesimde bilişim sistemlerinin neredeyse girmediği bir yerin kalmamış olması haksız erişime maruz kalabilecek alanları artırırken, bilgi ve iletişimdeki sürekli gelişim ise bu suçta yeni işlenme yöntemlerini beraberinde getirmektedir.

Haksız erişim, diğer bilişim suçlarının (örneğin bilgisayar sabotajının) işlenmesinin çoğu zaman ön koşulunu oluşturur. Bu nedenle bilişim suçlarıyla mücadelede başarılı olunabilmesinin önemli bir yolu, haksız eri-

şim suçunun elden gelebildiği ölçüde kapsamlı ve hukukî bir boşluk bırakılmadan yasal düzenlemesinin yapılmasını sağlamaktır.

Bilgi ve iletişim teknolojisini yeterli düzeyde üreten bir ülke olmamamızın yanında bu alandaki sürekli katlanarak devam eden gelişmeler, yabancı ülkelerdeki bilişim sahasındaki faaliyetler dikkate alındığında bilişim suçlarına ilişkin yasa çalışmalarının, ulusal düzeydeki araştırma, bilgi ve uygulamalara dayandırılması yeterli ve kapsamlı bir yöntem olamaz. Konunun karşılaştırmalı hukuk ve uluslararası örnekleri mutlaka gözetilmeli, bunların Ülkemize uygulanabilirliği irdelenmelidir. Çalışmamızda bu doğrultuda şu ana kadar, Ülkemiz dışındaki bilişim sistemine haksız erişim konusundaki farklılık taşıyan düzenleme ve yaklaşımlara olabildiğince yer verilmiştir.

Türk Hukukunda ilk defa getirilen 5237 sayılı TCK'nın 243. maddesindeki suç, karşılaştırmalı hukukta ve Avrupa Konseyi Siber Suç Sözleşmesi'ndeki bilişim sistemine haksız erişim suçundan farklı kaleme alınmıştır. Buradaki en temel farklılığı, 243. maddenin (1) numaralı fıkrasındaki *"girme"* ve *"orada kalmaya devam etme"* fiillerinin seçimlik olmaması, başka bir ifadeyle tek başına *"girme"* fiilinin madde kapsamında suç teşkil etmemesi oluşturmaktadır.

Yukarıda ayrıntılı şekilde belirtildiği üzere 5237 sayılı TCK'nın 243. maddesi, pek çok yönden de eksiklik taşımaktadır ve oldukça yetersiz kalmaktadır. Örneğin bir bilişim sistemine zorla girilmeksizin özel teknik araçlarla verilerin izlenmesi fiili, 243. madde kapsamında değildir. Bu nedenlerle, 243. maddedeki düzenleme, bilişim sistemine haksız erişim suçuyla korunmak istenilen hukukî yararı da gereği gibi sağlamaktan uzaktır.

Olması gereken hukuk açısından yapılması gerekenler parça parça değil, bütüncül bir yöntemle değerlendirilerek başta 243. maddede olmak üzere 5237 sayılı Türk Ceza Kanununda gerçekleştirilmelidir. Bu yaklaşım tarzı, bilişim alanındaki asıl koruma hedefi olan *"ihlâlleri önleyici koruma"* sonucuna daha çok ulaşılmasını sağlayacaktır. Başka bir anlatımla burada, yalnızca suç işlendikten sonra sonuçlarını giderme yöntemi değil, öncelikle suç teşkil edecek fiillerde yasal boşluk bırakılmadan yapılacak düzenlemelerle etkin bir şekilde suçtan önce caydırıcılığın sağlanabilmesi esas alınmalıdır.

***

KAYNAKÇA

Carlo Sarzana Ippolıto, *"Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum",*(İtalyan Temyiz Mahkemesi Ceza Dairesi Başkanı), (Çev.Vesile Sonay Daragenli), İHFM, Sayı 3, 1997.

Computer Crime and Information Technology Security, Computer Crime Examples, Chapter 14, 1/24/2007.

Dave Kleiman, Technical Editor, Kevin Cardwell, Timothy Clinton, Michael Cross, Michael Gregg, Jesse Varsalone, Craig Wright The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators, Worldwide Forensic Acts and Laws • Appendix B, Burlington, 2007.

Dennis C. Brewer, Security Controls for Sarbanes-Oxley Section 404 IT Compliance: Authorization, Authentication, and Access, Canada, Wiley Publishing, Inc., 2006.

Feridun Yenisey, Gottfried Plagemann, 15 Mayıs 1871 tarihli Alman Ceza Kanunu, Strafgesetzbuch, İstanbul, Beta Yayım, 2009.

Fred, Cohen, *"Computer Fraud Scenarios"*, Computer & Security, Volume 2003, Issue 1, January 2003.

Kit, Burden, Creole Palmer ve Barlow Lyde & Gilbert, Cyber Crime- A New Breed of Criminal, Computer Law and Security Report, Vol.19 No.3, 2003.

Michael Battle, Michael W. Bailie, Prosecuting Computer Crimes, Published by Office of Legal Education Executive Office for United States Attorneys.

Murat Volkan Dülger, Bilişim Suçları, Seçkin Yayınevi, Ankara, 2004.

Rosa Codina, *"Information Age Crime",* ScienceDirect – Computer Fraud & Security, June 2003.

Stein Schjolberg, *"The Legal Framework - Unauthorized Access To Computer Systems, Penal Legislation in 44 Countries"*, www.mosstingrett.no/info/legal.html (15.7.2010).

Steven Schlarman, *"Network Intrusion Management and Profiling";* CYBER FORENSICS A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Editors Albert J. Marcella, Ph.D., Robert S. Greenfield, Auerbach Publıcatıons, 2002.

Timur Demirbaş, Ceza Hukuku Genel Hükümler, Ankara, 6. Baskı, Seçkin Yayınevi, 2009.