

“Sevgili Eşim Sayın
Vali Erol Arıkan Anısına”

Av. L. Yasemin ARIKAN

TCK 243 VE 244'DE DÜZENLENEN BİLİŞİM SUÇLARI

GİRİŞ

Günümüzün modern yaşam düzeninin ana konularını oluşturan ekonomi, sağlık, eğitim, bilimsel araştırmalar, idare, savunma gibi pek çok yaşamsal alanda bilişim sistemleri vazgeçilmez araçlar olmuşlar, bu alanların pek çok yerinde geri dönülmez şekilde insanların yerini almışlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin kendisinin ya da içerdiği verilerin zarar görmesi ya da bu sistemlerin geçici süreyle de olsa çalışmaması büyük zararlara neden olabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsları,

kurtçuklar, truva atları gibi zarar verici yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana bulaştıran faillerin dahi öngördüğünden daha fazla zarara yol açabilmektedirler. Yasa koyucu da bu büyük tehlikeyi öngörerek sisteme ve/veya verilere zarar verme eylemlerini suç haline getirmiştir¹.

Bilişim suçları, diğer bir deyişle “siber suçlar”, bilgisayar, tablet, cep telefonu gibi çağdaş iletişim araç-

KISALTMALAR

AY: Anayasa

Bkz.: Bakınız

BTK: Bilgi Teknolojileri ve İletişim Kurumu

c.: cilt

CD: Ceza Dairesi

CGK: Ceza Genel Kurulu

CMK: Ceza Muhakemesi Kanunu

E.: Esas

K: Karar

K.: Kanun

s.: sayfa

S: Sayı

TCK: Türk Ceza Kanunu

vd.: ve devamı

1 DÜLGER, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayınları, 2015 (6.Baskı), s. 53.

ları veya pos makinası gibi alışveriş araçları kullanılarak elektronik ortamda işlenen her türlü suç olarak tanımlanabilir. Bu suçları;

1. Sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları),
2. Bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olan suçlar,
3. Kanunda bu sistemin kullanılması zorunlu olmamakla birlikte, söz konusu sistemin suçta vasita olarak kullanıldığı suçlar, şeklinde ayrımlara tabi tutabiliriz.

Bilişim sisteminin kullanılmasıyla işlenebilen suçlar; Bilişim Sistemi-ne Girme md.243), Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK md.244), Banka ve Kredi Kartlarının Kötüye Kullanılması (TCK md.245),

Bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olanlar; Hırsızlık (TCK md. 142/2-e) ve Dolandırıcılık (TCK md.158/1-f),

Bu sistemin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasita olabileceği suçlar ise; Haberleşmenin Gizliliğini İhlal (TCK md. 132), Haberleşmenin Engellenmesi (md.124), Eğitim ve Öğretimin Engellenmesi (md. 112), Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetlerinin Engellenmesi (TCK md. 113), Hakaret ve Sövme (TCK md. 125), Müstehcenlik (TCK md.226), Kumar Oynanması İçinYer ve İmkân Sağlanması (TCK md. 228), Suç İşlemeye Tahrik (TCK md. 214), Cinsel Taciz (TCK md. 105),

suçlarıdır.

Bu incelemede, bilişim sisteminin kullanılmasıyla işlenebilen, 5237 sa-

yılı TCK'nın ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının, "*Bilişim Alanında Suçlar*" başlıklı onuncu bölümü altında, 244. Maddesinde düzenlenen "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", Türk Ceza Hukukunda hakim olan inceleme şekline göre, korunan hukuki değer, suçun unsurları ve suça etki eden sebeplerle suçun özel görünüş şekilleri değerlendirilip, yaptırım ve soruşturma usulü kısaca açıklanmaya çalışılmıştır.

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU (TCK md.244)

I. GENEL AÇIKLAMA

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, 5237

sayılı TCK'nın ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının,

"*Bilişim Alanında Suçlar*" başlıklı onuncu bölümü altında, md. 244'te;

"**Sistemi engelleme, bozma, verileri yok etme veya değiştirme**

Madde 244 - (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 sağlamanın başka bir suç oluşturması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur."

şeklinde düzenlenmiştir. Bu düzenleme ile bir bilişim sisteminin engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme ve var olan veriyi başka yere gönderme fiilleri yaptırım altına alınmıştır.

II. KORUNAN HUKUKİ YARAR

Bu suçla korunan hukuksal yarar, bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisine sahip kişinin, verilerle oluşturulan (yazılım, ekonomik bilgiler, bilimsel çalışma gibi) değerlerine herhangi bir engel ya da gecikme yaşamadan ulaşması ve kullanmasıdır².

244. maddenin 1. ve 2.fıkralarında tanımlanan bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçlarıyla korunmak istenen hukuksal yarar karma bir nitelik göstermektedir. Bu suç tanımlarıyla, bilişim sistemlerinin, veri ve yazılımlardan oluşan soyut unsurlarının yanı sıra aynı zamanda somut unsur olan donanım kısmı da koruma altına alınmıştır.

244. Maddenin 4.fıkrasında tanımlanan, bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu ile korunmak istenen hukuksal değer ise suçun işleniş biçimlerine göre zilyetlik üçüncü kişilerin iyi niyetleri ve maddi ya da manevi mülkiyet

² ARTUK, Mehmet Emin/ GÖKCEN, Ahmet/ YENİDÜNYA, A. Caner, Türk Ceza Kanunu Şerhi, Özel Hükümler, Ankara, Turhan Kitabevi, 2009. S. 4659,4660



haklarıdır. Bilişim sistemlerinin veya verilerin zarar görmesi halinde kişinin mal varlığında bir azalma meydana gelebileceği gibi toplumun bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar bulunduğu için bir suç tanımına TCK'nın "Topluma Karşı Suçlar" kısmında yer verilmiştir. Bu suç nedeniyle korunan hukuki yararın bilişim sisteminin somut ve soyut unsurlarının bütünlüğü olduğu da kabul edilmektedir.

III. SUÇUN KONUSU

Kanunun birinci fıkrasında " sistemin işleyişi", ikinci fıkrada ise " sistem içindeki veriler" suçun konusu oluşturmaktadır.

İçinde veri bulunmayan bir bilişim sistemi, ya da veri taşıma aracı, bu

suçun konusunu oluşturmayacaktır. Çünkü maddenin düzenlenme amacı bilişim sisteminin somut yapısı olan donanım unsurlarına verilen zararı cezalandırmak değil, bilişim sisteminin soyut unsurları olan verilerde ve bilişim sisteminin işleyişinde meydana getirilen zararları cezalandırmaktır³.

IV. FAİL VE MAĞDUR

A. Fail

Kanun, suçun faili olmak bakımından herhangi bir sınırlama getirmediğinden, herkes fail olabilir⁴.

Suçun işlenmesi suretiyle bir tüzel kişi yararına haksız menfaat sağlan-

ması durumunda ise tüzel kişiler suç faili olamayacağından cezalandırmayacaktır. Ancak TCK md. 246 atfıyla, TCK md. 60 uygulama alanı bularak tüzel kişi hakkında güvenlik tedbirine hükmolunacaktır.

B. Mağdur

Bu suç tipi mağduru bakımından da bir özellik göstermemektedir. İşleyişi engellenen, bozulan, yok edilen veya değiştirilen sistem üzerinde hak sahibi kimse, suçun mağduru- dur. Failin eyleminin birden fazla kimsenin hakkını ihlal ettiği durumlarda, bu kişilerin hepsi mağdur sıfatını kazanacaktır.

V. SUÇUN MADDİ UNSURU

TCK 244'deki düzenlemeye genel olarak baktığımızda; bilişim sisteminin işleyişini engelleme-bozma, verilere zarar verme ve bilişim sistemlerini kullanarak haksız menfaat

3 GÜL, Ahmet, Doğrudan-Dolaylı Bilişim Suçları, Ankara, Seçkin Yayınları, 2018. s.87,Dn. 73.

4 DÜLGER,Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayınları, 2015. s. 413.

sağlama fiillerinin cezalandırıldığı görülmektedir. Suçun maddi unsurunun izahı bakımından söz konusu düzenlemede bahsi geçen bu hareketlerin her birini ayrı ayrı açıklayacak olursak;

A. Bilişim Sisteminin İşleyişini Engelleme veya Bozma (TCK md.244/1)

Bilişim sisteminin işleyişini engelleme veya bozma fiili, TCK 244/1'de yaptırım altına alınmıştır. Suç, "işleyişi engelleme" veya "bozma" fiillerinden birinin icrasıyla gerçekleşeceği için seçimlik hareketlidir. Engelleme ve bozmadan ne anlaşılması gerektiğini kısaca izah edecek olursak; **engelleme**, "sistemin gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesidir"⁵.

Sisteme yöneltilecek yoğun elektro manyetik dalgalarla sistem merkezinin etkilenmesini sağlama ya da sisteme yapılacak müdahaleyle işletim sisteminin geçici bir süre devre dışı bırakılması, söz konusu kavram doğrultusunda sayılabilecek örneklerdendir.

Bunların dışında bilişim sistemi hiç kullanılmaksızın, bir iç ağda (intranet) bilgisayarları birbirine bağlayan

Bilişim sisteminin işleyişini engelleme veya bozma fiili, TCK 244/1'de yaptırım altına alınmıştır.

kabloların kesilmesi veya sistemin olağan işleyişinin yavaşlatılması, sisteme bilişim virüsü ya da mantık bombası gibi zararlı bir yazılımın buluşturulması ya da sistemde olmayan bir şifrenin sisteme yerleştirilmesi veya mevcut şifrenin değiştirilmesi de engelleme sayılır⁶.

Bozma ise "sistemin veri işleme faaliyeti yapamayacak hale getirilmesidir"⁷. Sistemin olağan ve normal koşullarda yerine getirmiş olduğu işlevini yapamaz hale getirmesi bu kapsamda bozmadır⁸. Bozma, bilişim sistemi kullanılarak, sistemin bütününe veya bir kısmına yönelik gerçekleştirilebileceği gibi, sisteme fiziksel müdahaleyle de gerçekleştirilebilir⁹.

B. Verilere Zarar Verme (TCK md. 244/2)

Bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek fiilleri, TCK md.244/2'de yaptırım altına alınmıştır. Maddede bahsi geçen bu seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanmış olacaktır.

Anılan kavramları açıklamak gerekirse; **bozmak**, verilerden elde edilmek istenen faydanın, değiştirme,

tamamen veya kısmen tahrip etme gibi hareketlerle, elde edilememesini sağlamaktır. Bilişim sistemlerine sızan ve virüs olarak adlandırılan programlar vasıtasıyla sistemde yer alan verilerin tahrip edilmesi bozma örneklerdir¹⁰.

Sistemin fiziki varlığına yapılacak saldırıda içindeki verilerin de zarar görmesi halinde, verilerin bozulmasından söz edilebilir¹¹.

Yok etmek, verilerin ortadan kaldırılması anlamına gelmektedir. Verilerin silinmesi veya bulunduğu sistemin biçimlendirilmesi hareketlerinin yok etme olduğu söylenebilir. Bu hareketler sisteme fiziksel müdahale yoluyla olabileceği gibi bir ağla bağlanmak suretiyle de gerçekleştirilebilir¹².

Değiştirmek, veriler üzerinde yapılan bir tür manipülasyondur. Verilerin başka biçimlere sokulması, yeni içerik kazandırılması veya niteliklerinin değiştirilmesi bu eyleme örnek gösterilebilir¹³.

Erişilmez kılmak, "verilere erişimi sağlayan yolların (path) değiştirilmesi veya silinmesidir"¹⁴. Bu halde aslında veriler mağdurun sisteminde olduğu halde fail, yaptığı birtakım işlemlerle, mağdurun kendi verilerine ulaşmasını imkânsız hale getirmektedir.

Sisteme veri yerleştirmek, "sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkânını ortadan kaldırmadan ek birtakım veriler eklemek.

5 ÖNGÖREN, İnternet Hukuku, s. 48; Engelleme bakımından bilişim sistemini kesintiye uğratmanın geçici mi yoksa sürekli mi olması gerektiği doktrinde tartışma yaratmıştır. Bu doğrultuda ARTUK/GÖKÇEN/YENİDÜNYA; sistemi kesintiye uğratmanın geçici olması gerektiği, MERAN, DÜLGER ve YAŞAR/GÖKCAN/ARTUÇ; geçici veya sürekli olması arasında bir fark olmadığı yönünde görüş bildirmiştir. Sistemi engellemenin geçici veya sürekli olması arasında bir fark olmadığını savunan ikinci görüş daha isabetlidir. (ARTUK/GÖKÇEN/YENİDÜNYA, Türk Ceza..., s.4661; DÜLGER, Bilişim Suçları, s.234; MERAN, Yeni Türk Ceza..., s.371; YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s.6758)

6 GÜL, s.87, Dn. 74

7 ÖNGÖREN, İnternet Hukuku, s.48

8 MERAN, Yeni Türk Ceza..., s.371

9 ARTUK/ GÖKÇEN / YENİDÜNYA, Türk Ceza.. s. 4659,4660

10 ARTUK/ GÖKÇEN / YENİDÜNYA, Türk Ceza.. s. 4666

11 ARTUK/ GÖKÇEN / YENİDÜNYA, Türk Ceza.. s. 4666

12 DÜLGER, Bilişim Suçları, s.236-237

13 ARTUK/ GÖKÇEN / YENİDÜNYA, Türk Ceza.. s. 4667

14 ARTUK/ GÖKÇEN / YENİDÜNYA, Türk Ceza.. s. 4667

Var olan verileri başka yere göndermek ise, mağdura ait verilerin farklı bir bilişim sistemine gönderilmesidir.

C. Bilişim Sistemini Kullanarak Haksız Menfaat Sağlama (TCK md.244/4)

TCK md. 244/4'te 1. ve 2. fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlama-sı suç olarak düzenlenmiştir. Fakat kanun koyucu madde kapsamında sayılan fiillerin işlenmesi halinde, başkaca suçların oluşması ihtimalini de gözetenerek, fiillerin başka bir suç oluşturulmaması halinde bu maddenin uygulanacağını öngörmüştür.

VI. SUÇUN MANEVİ UNSURU

Sistemi engelleme, bozma, verileri yok etme veya değiştirme, bilerek ve istenerek, yani "genel kastla" işlenebilen suçlardan olmakla beraber, TCK 244/4. maddesinde ayrıca "haksız çıkar sağlama kastı" da gerekmektedir. Suçun taksirli hali ise cezalandırılmaz

Fail, bilişim sistemini engellediğini, bozduğunu, verileri yok ettiğini veya değiştirdiğini bilmeli ve istemelidir. Suç tipinde doğrudan kasta ilişkin bir ibare bulunmadığından, olası kastla işlenmesi de mümkündür.

VII. HUKUKA AYKIRILIK VE UYGUNLUK

A. Hukuka aykırılık unsuru

Bilişim sistemin işleyişinin engellenmesi bozulması verilerin yok edilmesi veya tasarruf yetki değiştirilmesi suçunun işlenmesiyle suçla korunan hukuksal değerler konusunda da açıklandığı gibi bilişim sistemi veya veriler üzerinde tasarruf yetkisi bulunan kişinin bilişim sistemine veya verilere herhangi bir engel arıza ya da gecikme olmadan

ulaşması ve kullanmasındaki çıkarı zedelenmektedir.

B. Hukuka uygunluk unsuru

Eğer bilişim sisteminden yararlanmaya yetkili olan kimse *faile giriş için izin vermişse ya da şifresini söylemişse* artık eylem hukuka aykırı olarak kabul edilmeyecektir¹⁵.

Yasaların verdiği yetkiye dayanarak bilişim sistemine müdahale edilmesi durumunda eylem artık hukuka aykırı olarak kabul edilmeyecektir. 5651 sayılı yasa veya CMK madde 134-135 uyarınca bu görevleri yapmak zorunda kalan kişilerin eylemleri bu kapsamda değerlendirilecektir.

VIII. CEZADA İNDİRİM NEDENİ

TCK 244. Maddede bu suç ile ilgili hafifletici neden düzenlenmemiştir.

IX. CEZANIN AĞIRLAŞTIRICI NEDENİ

TCK md. 244/3'te, 1. ve 2. Fıkralardaki fiillerin (özel veya kamuya ait) bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, cezanın yarı oranında arttırılması öngörülmüştür.

X. SUÇA TEŞEBBÜS, İŞTİRAK, ZİNCİRLEME SUÇ, İÇTİMA

A. Teşebbüs

Bu suça teşebbüs mümkündür. İcra hareketlerinin failin elinde olmayan nedenlerle yarıda kalması ve bu nedenle sisteme etki edememe-

si halinde teşebbüsten bahsedilir. Söz konusu suçun seçimlik hareketli olmasından dolayı akla, maddede sayılan hareketlerin birden fazlasının olayda mevcut olması, ancak bunlardan bir kısmının tamamlanmış, diğer kısmının ise teşebbüs aşamasında kalması durumunda, nasıl bir değerlendirme yapılacağı sorusu gelmektedir. Burada dikkat edilmesi gereken, seçimlik hareketli suçlarda, birden fazla hareket aynı anda gerçekleşse de olayda tek bir suçun oluştuğunun kabul edileceği kuralıdır. Bu kural uyarınca, seçimlik hareketlerden biri teşebbüs aşamasında kalmış olsa bile, diğeri tamamlanmışsa, ortada yine tek bir suçun varlığından söz edilecektir.

Sisteme veri yerleştirmek için erişen fail, isteyerek bu fiilden vazgeçmiş ise, TCK 244/2'ye teşebbüsten değil, TCK 243'ten sorumlu tutulacaktır. İsteyerek vazgeçme halinde failin vazgeçtiği ana kadar yapmış olduğu eylemler eğer başka bir suç oluşturuyorsa fail bu suçtan cezalandırılır.

B. İştirak

Söz konusu suç, iştirak açısından ayrı bir özellik göstermez. TCK'nda yer alan iştirake ilişkin genel hükümler burada da uygulanır.

C. İçtima

Bilişim sisteminin işleyişinin bozulması ve verilere zarar verilmesi, aynı zamanda TCK md. 151'de düzenlenen mala zarar verme suçunu da oluşturmaktadır. Bu duruma ilişkin olarak doktrinde farklı görüşler mevcuttur. Bir görüşe göre burada, TCK md.44 uyarınca farklı neviden fikri içtima kuralının uygulama alanı bulacağı ve failin ağır olan suçtan cezalandırılacağı kabul edilmektedir¹⁶.

¹⁵ AYHAN Önder, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, Filiz Kitabevi, İstanbul, 1994, s. 505; YAZICIOĞLU, R.Yılmaz, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi" Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C 2, S. 2, Y. 2005, s. 396

¹⁶ YENİDÜNYA/DEĞİRMENÇİ, Mukayeseli Hukukta..., s.27

Buna karşın diğer görüş ise; anılan suç tipinde bahsi geçen bilişim sisteminin, TCK md.151'de yer alan tanımdaki mal kapsamında olmadığını, işleyen ve fayda sağlayan bir araç olduğunu, bu nedenle de TCK md. 151 ile 244'ün farklı hukuksal değeri koruduğunu ileri sürmüştür¹⁷.

Bu suçla korunan hukuksal değerler, sadece soyut olan veriler olmayıp aynı zamanda somut olarak bilişim sistemine ait donanımlardır¹⁸. Bu sebeple bilişim sisteminin donanımlarına zarar verilmesi halinde hem mala zarar verme hem de TCK md.244 oluşacaktır. Buradaki sorun özel normun genel norma önceliği prensibi gereği bilişim sistemini özel olarak koruyan bir norm olan TCK md.244'ün uygulanması ile çözüleceğidir. Zira aynı hukuki değeri koruyan farklı iki normun ihlali söz konusudur. Ancak md. 244, mala zarar verme suçuna göre birtakım ek özelliklere sahip olan özel norm niteliğinde olduğundan uygulama alanı bulacaktır¹⁹.

Yine bu maddede yer alan suçun işlenmesi için hukuka aykırı olarak bilişim sistemine girmek ve sistemde kalmak gerektiğinden bahisle TCK md.243'ün, TCK md.244'e nazaran geçit suç olarak kabul edilmesi ve failin sadece TCK md.244'e göre cezalandırılması gerektiğini ifade eden görüşe²⁰ karşılık diğer bir görüş, TCK md.244'ün, TCK md.243'ün öngördüğü şekilde sisteme girmeden gerçekleştirilmiş olmasının olanaklı olabileceğini,

bu sebeple de TCK md.243'te yer alan eylemlerin TCK md.244'un ögesi ya da nitelikli hali olmadığı gerekçesiyle burada gerçek içtima hükümlerinin uygulanması gerektiği ileri sürülmektedir. Gerçekten bilişim sistemine girmeden verilerin bozulması söz konusu olabilir. Bu durumda zaten TCK md.243'ten bahsedemeyiz.

Ancak bilişim sistemine girerek veri bozma, yok etme halleri var ise bu durumda yine görünüşte içtima söz konusu olup fikri içtimayı kabul eden ikinci görüş isabetsizdir. Zira TCK md. 244'ün oluşması halinde bu suç tipinin gerçekleşebilmesi için TCK md.243deki unsurların gerçekleştirilmiş olması gerekir. Bu halde md. 244, md.243 açısından tüketen norm niteliğindedir. Tüketen-tüketilen norm ilişkisi gereği TCK md. 244'un uygulanacağı kabul edilmelidir.

Bir belgenin gerçeğe aykırı şekilde düzenlenmesi ya da gerçeğe uygun bir belgenin değiştirilmesi amacıyla bilişim sistemine veri eklenmesi, verilerin değiştirilmesi gibi hallerde, fail belgede sahtecilik suçundan ve 244/2'den cezalandırılacaktır.

TCK md. 244/2 kapsamında bir bilişim sistemindeki verilerin başka bir yere gönderilmesi aynı zamanda TCK md. 136'daki kişisel verilerin hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek fiillerini de gündeme getireceğinden bu iki suç arasında TCK md. 44 gereği farklı neviden fikri içtima kurallarının uygulanması söz konusu olacaktır.

Bir belgenin gerçeğe aykırı şekilde düzenlenmesi ya da gerçeğe uygun bir belgenin değiştirilmesi amacıyla bilişim sistemine veri eklenmesi, verilerin değiştirilmesi gibi hallerde, fail belgede sahtecilik suçundan ve 244/2'den cezalandırılacaktır.

İçtima ile ilgili başkaca önemli bir problem ise TCK md. 244/4'te yer alan bilişim sistemini kullanarak haksız yarar sağlama suçunda gündeme gelecektir. İlk olarak belirtmek gerekir ki, bu fıkranın kapsamına giren hallerde fail aynı zamanda TCK md. 244/2 ve md. 244/3'ten cezalandırılmayacaktır. TCK md. 244/4 tamamlayıcı norm niteliğinde olduğundan, fail tarafından gerçekleştirilen fiiller başka bir suç tipi kapsamına girmekteyse, TCK md. 244/4 uygulanmayacaktır. Bu nedenle TCK md. 244/4 ile TCK md. 142/1-e ile TCK md. 157 arasındaki ilişkiye değinmek gerekir. Öncelikle belirtmek gerekir ki madde metninin aksine gerekçede eylemin daha ağır bir cezayı gerektiren suçu oluşturması halinde TCK md. 244/4'ün uygulanmayacağına belirtilmesinin hatalı olduğu, çünkü madde metninde ağır ya da hafif farkı olmaksızın eylemin başka bir suçu oluşturması halinde TCK md. 244/4'ün uygulanmayacağı belirtilmektedir.

TCK md. 142/1-e ve md. 157'nin TCK md. 244/4 ile ilişkisine gelince md. 244/4'ün uygulanabilmesi için

17 DÜLGER, Bilişim Suçları, s.242; TAŞKIN, Bilişim Suçları, s.55

18 PARLAR, Türk Ceza..., s.24

19 YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.27

20 YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.27

filin başka bir suçu oluşturmaması gerekir. Yani md. 244/4 tamamlayıcı norm niteliğindedir. Bu sebeple bu gibi hallerde koşulları varsa TCK md. 142/1-e veya md. 157 uygulanacaktır.

XI. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA

İşlenen suç şikâyete bağlı olmayıp, C. Başsavcılığı tarafından doğrudan soruşturma yapılır. Maddenin 2. Fıkrasında yazılı suç için hapis cezasının üst sınırı üç yıldan fazla olmadığından 02.12.2016 tarihinde yürürlüğe giren 6763 sayılı Kanun'unun 34. Maddesi gereği uzlaştırma kapsamına alınmıştır.

5235 sayılı yasanın 11. Maddesi gereği, yargılama yapmaya görevli mahkeme asliye ceza mahkemesidir. Yer itibarıyla yetki temadinin sona erdiği yerdeki mercilere aittir.

5237 sayılı TCK'nın 244. maddesinin 4. fıkrasında düzenlenen eylemler açısından iki yıldan altı yıla kadar hapis cezası ve beş bin güne kadar adli para cezası öngörülmüştür. Görüldüğü üzere, bu suçu işleyen failler açısından hem adli para cezası hem de hürriyeti bağlayıcı ceza öngörülmüştür. Zira fail, işlediği suç neticesinde haksız bir çıkar sağlamaktadır. Bu sebeple madde metnine göre, hapis cezası ile birlikte adli para cezasına da hükmedilecektir.

XI. YARGITAY KARARLARI

Yarg. 11.CD. 28.01.2009 gün, 2008/16570 Esas, 2009/101 Karar: Sanığın savunması ve tüm dosya kapsamı dikkate alındığında, dosyada mevcut Türk Telekomünikasyon A.Ş.'nin yazısından hesaplara gelen paraların internette 85.97.000.000 IP numarası kullanılarak aktarıldığının anlaşılması karşısında, bu nu-



maranın kullanım bilgileri istenerek EFT'nin yapıldığı anda anılan numaranın bu şirket tarafından hangi kullanıcıya atandığının ilgili kurumdan araştırılıp tespit edildiğinde sanık ile irtibatı olup olmadığının saptanması gerektiğinin gözetilmemesi sonucu eksik soruşturmaya dayanarak yazılı şekilde hüküm kurulması nedeniyle hükmün bozulması.

Yrg. 11.CD.25.06.2007, 2007/2168-4372 E-K: Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından EFT'nin şikayetçi şirketin hesabından sahte olarak açtırmış olduğu hesaba intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır.

Yrg.11.CD.12.05.2009, 2009/3700-6207 E-K: Sanıkların, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdıkları hesaba bilişim sistemi aracılığıyla göndererek yine sahte kimliklerle çekmek istemesinden ibaret eylemlerinin paranın açılan hesaplara transferiyle suçun tamamlanacağı gözetilme-

den paranın çekilmemesi nedeniyle teşebbüs aşamasında kaldığından bahisle eksik ceza tayini isabetsizliği karşı temyiz olmadığından bozma nedeni yapılmamıştır.

Yrg. 11. CD, 26/09/2007, 2007/6122-5897 E-K: Sanığın, evrakı tefrik edilen suç ortaklarıyla birlikte fikir ve eylem birliği içinde Hasdağ Tekstil Sanayi ve Ticaret Limited Şirketi adına Akbank Kayseri Ticari Şubesinde bulunan 888-843-184019 nolu YTL hesabına internet üzerinden girerek, mevduatta bulunan 7.250.00 YTL. parayı, aynı bankanın Konya Truva Şubesinde kendi fotoğrafının yapıştırıldığı ve Veysel Tekin'e ait kimlik bilgilerini içeren sahte nüfus cüzdanı ile açtığı 888-773-0009847 nolu banka hesabına havale edip, bu şekilde hesaba yatan paradan 5000 YTL yi bankadan çektikten ve bakiye parayı çekmek isterken yakalandığı oluştaya uygun şekilde kabul edilmiş olmasına göre, eylemin 5237 sayılı TCK'nın 244/4. Maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden suçun nitelendirilmesinde yanılığa düşülerek hırsızlık suçundan yazılı şekilde hüküm kurulması.

Yrg. 11. CD, 28/01/2008, 2007/8337 E, 2008/269K: Dolandırıcılık suçundan unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği somut olayda ise, sanıkların açık kimlikleri tespit edilemediği için evrakı tefrik edilen faillerle fikir ve eylem birliği yaparak, İstanbul'da bulunan bir bilgisayardan katılanın Vakıfbank Ankara Şubesindeki hesabına ait internet şifresi kırılarak hesapta bulunan 41.500 YTL'nin, sanık Yaşar Aslan'ın Vakıfbank Gaziantep Şubesindeki hesabına EFT yoluyla havale etmeleri ve buradan da sanıklar Yaşar ile Eren'in parayı çekmelerinden ibaret eylemlerinde, gerçek kişiye yönelen hileli bir hareket bulunmaması nedeniyle dolandırıcılık suçunun unsurlarını oluşturmadığı, fiilin 5237 sayılı TCK'nın 244/4 maddesine uygun "bilgi sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama" suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilgi sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetlerine karar verilmesi.

Yrg. 11.CD, 24/03/2008, 2007/9407 E, 2008/1807 K: Sanığın, Denizbank A.Ş. Antalya Şubesi'nde kendi adına hesap açtırdıktan sonra, katılan F.A'ya ait aynı bankanın Karadeniz Ereğli Şubesi'ndeki banka hesabından, ele geçirdiği "interaktif bankacılık şifresini" kullanarak internet aracılığı ile banka hesabına para transferi yapmaktan ibaret eyleminin, gerçek kişiye yönelmiş bir hile bulunmadığı cihetle, suç tarihinde yürürlükte bulunan 765 sayılı Yasanın 525/b-2. Maddesinde öngörülen "bilgi sistemini oluşturduğu ve sonradan yürürlüğe giren

Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde "bilgi sistemine girerek haksız çıkar sağlama suçu" gerçekleşecektir.

5237 sayılı Yasanın 244/4. maddesi ile karşılaştırma yapılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması.

Yrg. 11.CD, 01/07/2008, 2006/1800 E, 2008/7126 K: Dolandırıcılık suçunda unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği, somut olayda ise, sanığın katılan Türk Telekom A.Ş. tarafından üretilen ve ankesörlü telefonlardan konuşma yapmaya yarayan telefon kartlarının manyetik şeritlerine teyp bandı ile dolmuş yapılarak suretiyle kaçak görüşme yaptığının

iddia ve kabul olunması karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı, ayrıntıları Ceza Genel Kurulu'nun 19.06.2007 gün ve 136-150 sayılı kararında belirtilen dolandırıcılık suçunun unsurlarının bulunmadığı, fiilin 5237 sayılı TCK'nın 244/4 maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi.

Yrg. 11.CD, 07/10/2009, 2009/1616-11328 E-K: Dolandırıcılık suçu; hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlanması suretiyle oluşur. Suçun maddi unsurunu oluşturan hareketlerin, gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekir. Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunda ise, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler araç olarak kullanılıp gerçek kişiler aldatılarak çıkar sağlanmaktadır. Bankaların etkin işlevi bulunan çek, hesap cüzdanı, dekont gibi maddi varlıklarının kullanılması halinde ise, banka vasıta kılınarak dolandırıcılık suçu oluşacaktır.

Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde "bilgi sistemine girerek haksız çıkar sağlama suçu" gerçekleşecektir.

Somut olayda ise; sanığın, katılanın Garanti Bankası 1. Levent Şubesinde bulunan hesabına internet bankacılığı yoluyla girip hesaptaki paradan 3.200.00 TL'yi Garanti Bankası Osmanbey Şubesindeki kendi hesabına internet yoluyla havale ettikten sonra parayı çekerek haksız menfaat sağladığı iddia ve dosya içeriğine uygun kabul edilmesi karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı "veri"nin taşınabilir bir mal olarak kabul edilmesinin olanaklı olmaması nedeniyle hırsızlık suçunun unsurlarının da gerçekleşmediği eylemin, suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b. (5237 sayılı TCK'nın 244/4. maddesine uygun "bilişim sistemini engelleme, bozma verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama") maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suçun nitelenendirilmesinde yanılığa düşülerek bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi.

Yargıtay Ceza Genel Kurulu 17/11/2009 gün, 2009/11-293 Esas, 2009/268 karar sayılı kararı:
"Sanık V.E. ile firari S.T. birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Şekerbank Ankara Küçüksat Şubesindeki hesabından 10.750 YTL'yi internet kanalı ile Şekerbank İstanbul Zeytinburnu Şubesinde sanık V. adına açtırdıkları hesaba havale ettikleri ve aynı gün banka şubesinden çektikleri olayda, Yargıtay Ceza Genel Kurulunca çözümlü gereken uyuşmazlık, sanığın 765 sayılı TCK'nın 525/b-2 maddesine uyan

eyleminin, suç tarihinden sonra yürürlüğe giren 5237 sayılı TCK'nın 244/4 maddesine mi, yoksa 142/2-e maddesine mi, uyan suçu oluşturduğuna ilişkindir.

244. maddenin 4. fıkrasında yer alan; "Yukarıdaki fıkralarda tanımlanan fillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamanın başka bir suç oluşturulmaması halinde..." biçimdeki ifadeden bu fıkradaki düzenlemenin tali norm niteliğinde olduğu anlaşılmaktadır. Buna göre, bilişim sistemleri aracılığıyla haksız çıkar sağlanmış olması halinde öncelikle Yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirilmeli, şayet gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değilse, o zaman 244. maddenin 4. fıkrası hükmü uyarınca uygulama yapılmalıdır. ...

Bu konu öğretide de tartışmalı olup, bir kısım yazarlar bilişim sistemiyle hukuka aykırı yarar sağlama eylemlerinin, genellikle bilişim suçları veya dolandırıcılık suçu kapsamında değerlendirilebileceği, gelişen teknolojiyle birlikte değişen suç türleri nedeniyle bilişim hırsızlığı suçuna yer verilmesinin gerekli bulunduğu, ancak bu suçun bağımsız bir suç tipi olarak düzenlenerek, hangi eylemleri kapsayacağını açıkça belirlenmesi gerektiğini, bilişim sistemini kullanmak suretiyle hırsızlık suçunu düzenleyen hükmün uygulanmasının bir iki örnek dışında olanaksız olduğunu ileri sürmüş; bir kısım yazarlar ise başkasının banka hesabına internet üzerinden girerek bu hesaptan failin kendisi veya başkasının hesabına para aktarması şeklinde gerçekleşen olaylarda da bilişim sistemlerini kullanarak hırsızlık veya dolandırıcılık suçlarının unsurları itibarıyla gerçekleşip gerçekleşmediği

tartışmalıdır şeklinde görüş bildirmektedirler..

Bu bilgiler ışığında somut olay değerlendirildiğinde;

"Sanık V.nin; firari S.T. ile birlikte hareket ederek, daha önceden haksız

bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Şekerbank Ankara Küçüksat Şubesindeki hesabından 10.750 YTL'yi Şekerbank İstanbul Zeytinburnu Şubesinde sanık V. Adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCK'nın 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır." denmiştir. Yargıtay Ceza Genel Kurulu'nun bu kararı ilgili ceza dairesi tarafından da benimsenmiş ve uygulamada bu görüş üzerinde birlik sağlandığı gözlemlenmiştir.

SONUÇ

Bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin kendisinin ya da içerdiği verilerin zarar görmesi ya da bu sistemlerin geçici süreyle de olsa çalışmaması büyük zararlara neden olabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsleri, kurtçuklar, Truva atları gibi zarar verici yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana bulaştıran faillerin dahi öngördüğünden daha fazla zarara yol açabilmektedirler. Yasa koyucu da bu büyük tehlikeyi öngörerek sisteme ve/veya verilere zarar verme eylemlerini suç haline getirmiştir.

5237 sayılı TCK'nda, bilişim alanında işlenen suçlarla mücadele edebilmek için bu suçlar ve yaptırımları "Bilişim Alanında Suçlar" başlığı altında düzenlenmiştir. Yukarıda belirtildiği üzere, günümüz şartları ve mukayeseli hukuktaki gelişmelere paralel olarak ayrı bir başlık altında düzenlenmesi oldukça önemlidir.

5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar TCK'nın 244/4 maddesinin uygulama-

si kişilere karşı işlenen suçlar ile banka veya kredi kurumlarına ve kamu kurumlarına yönelik işlenen suçların cezaları arasında ayırım yapılmıştır.

Bu arada bilişim suçlarıyla mücadele etmek amacıyla yasal düzenleme yapılırken, bu suçların uluslararası boyutları da unutulmamalıdır. Teknolojinin sağladığı olanaklar sayesinde, ülkeler arasında bu suçlar çok hızlı bir şekilde ve iz bırakmadan işlenebilmektedir. Suç örgütlerinin aksine, ülkeler arası işbirliğinin istenen seviyede olmaması, bürokratik kısıtlamalar ve diğer etkenler nedeniyle, suçla tam anlamıyla mücadele edilememektedir. Bu durum ceza kanunundaki maddeleri de etkisizleştirmektedir. Bilişim suçlarıyla uluslararası alanda mücadele ederken ilk akla gelen sözleşme olan Siber Suç Sözleşmesi 2001 yılında yürürlüğe girmiş ise de, o tarihten beri Türkiye bu sözleşmeyi imzalamamış ve sözleşmeye taraf olmamıştır. Dolayısıyla Ceza Kanunu'na 243, 244, 245, 246. maddelerinde yazılı bilişim suçlarına yönelik hükümleri koymak, bu suçlarla her anlamda mücadele edildiğini göstermeye yetmemektedir. Bilişim suçuyla mücadelede samimiyetin ve siyasi iradenin ortaya konması bakımında

acilen "Siber Suç Sözleşmesi" imzalanmalıdır. Bilişim suçlarıyla mücadelede uluslararası alandaki tavır bir tarafa, ülke içindeki sorunlar da ayrıca değerlendirilmelidir.

Kolluk güçleri bünyelerinde bilişim suçlarıyla mücadele etmek için özel birimler kurmuşlarsa da, uygulamada teknik ve fiziki altyapı eksiklikleri nedeniyle faillerin yakalanmasında sorunlar yaşanmaktadır. Bu amaçla kolluk güçlerinin bilişim suçlarıyla ilgili birimleri güçlendirilmeli, teknolojik altyapıları geliştirilmelidir. Yakalanan şüphelilerin yargılanıp cezalandırılmasında ise, ülkemizin yargı sistemine dair temel yapısal sorunlarla karşılaşmaktadır.

Bilişim suçlarının mahiyetleri ve yarattıkları olumsuz etkiler nedeniyle daha hızlı bir yargılama sürecine ihtiyaç vardır. Dolayısıyla bu suçları yargılamakla görevli ihtisas mahkemeleri oluşturulmalı, konunun uzmanları ile mahkemeler donatılmalı, mahkemelerin oluşumu için gerekli sayıda hakim ve C. Savcısı ataması yapılmalıdır. Çünkü kolluk güçleri uzmanlaşsa bile, yargılama makamında aynı uzmanlaşma olmazsa, istenen sonuca ulaşmak mümkün olamayacaktır.

KAYNAKÇA

- ARTUK**, Mehmet Emin/ **GÖKÇEN**, Ahmet/ **YENİDÜNYA**, A. Caner, Türk Ceza Kanunu **Şerhi, Özel Hükümler**, Ankara, Turhan Kitabevi, 2009.
- DEMİRBAŞ**, Timur, Ceza Hukuku Genel Hükümler, Ankara, 2011.
- DÖNMEZER**, Sulhi /**ERMAN**,Sahir, Nazari Ve Tatbiki Ceza Hukuku, Genel Kısım C. II,11. Bası, İstanbul,Beta Yayınevi, 1997.
- DÜLGER**,Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayınları, 2015.
- GÜL**, Ahmet, Doğrudan-Dolaylı Bilişim Suçları, Ankara, Seçkin Yayınları, 2018.
- KANGAL**, Zeynel, Tüzel Kişilerin Ceza Sorumluluğu, Ankara, 2003.

- KARAGÜLMEZ**, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,2.bası, Ankara, 2011.
- MAHMUTOĞLU**, Fatih Selami, Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu, İUHFM,C. IIX, S.1-2, İstanbul, 2001,
- MERAN**, Necati, Yeni Türk Ceza Kanununda Sahtecilik- Malvarlığı Bilişim Suçları İle Ekonomi Ve Ticaret Alanında Suçlar, Ankara, 2005.
- ÖNGÖREN**, Gürsel, **İnternet Hukuku**, İstanbul, 2006.
- ÖZGENÇ**, İzzet. Türk Ceza Hukuku Genel Hükümler, 6. Bası,Ankara, Seçkin Yayıncılık,2006.
- PARLAR** , Ali, Bilişim Alanında İşlenen Suçlar, Ankara, Bilge Yayınevi, 2011.

- TAŞKIN**, Şaban Cankat, Bilişim Suçları, İstanbul, 2008.
- TEZCAN** Durmuş, **ERDEM** Mustafa R, ÖNOK R. Murat, Teorik Ve Pratik Ceza Özel Hukuku, Seçkin Yayınevi, Ankara,2014.
- ÜNVER**, Yener, Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer, Ankara, Seçkin Yayınevi,2003.
- YENİDÜNYA**, Caner/DEĞİRMENCI, Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, Legal Yayıncılık, 2003.
- YENİDÜNYA**, Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu",Legal Fikri ve Sınai Haklar Dergisi, İstanbul, Nisan 2005.