BİLİŞİM SİSTEMLERİ ÜZERİNE ARAMA VE EL KOYMA TEDBİRİNE İLİŞKİN MEVZUAT VE UYGULAMADA YAŞANAN SORUNLAR

Fehmi Ünsal ÖZMESTİK

111692045

İSTANBUL BİLGİ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Yrd. Doç. Dr. Leyla KESER BERBER

2015

BİLİŞİM SİSTEMLERİ ÜZERİNE ARAMA VE EL KOYMA TEDBİRİNE İLİŞKİN MEVZUAT VE UYGULAMADA YAŞANAN SORUNLAR

REGULATIVE AND PRACTICAL PROBLEMS ARISING OUT FROM SEARCH AND SEIZURE MEASURES ON INFORMATION SYSTEMS

Fehmi Ünsal ÖZMESTİK
111692045

Yrd. Doç. Dr. Leyla KESER BERBER :

Yrd. Doç. Dr. Mehmet Bedii KAYA :

Öğr. Görv. İbrahim Halil SARUHAN :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı : 95

Anahtar Kelimeler (Türkçe)

1) Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbiri
2) Adli Bilişim
3) Bilişim Hukuku
4) Bilişim Suçları Hukuku
5) Bilişim Suçları

Anahtar Kelimeler (İngilizce)

1) Information Systems on Search and Seizure Measure
2) Computer Forensics
3) Information Technology Law
4) It Crimes Law
5) Computer Crimes

ÖZET

Tezin ilk bölümünde, genel olarak dijital delil ve dijital delil ile ilgili kavramlara değinilmiştir. Bilişimin sisteminin terminoloji ve uygulamadaki tanımlarına kısaca yer verilmiştir. Dijital delil tanımı, hash değeri önemi ve özelliklerinden bahsedilmiştir. Bununla ilgili terminolojik yaklaşımlarda bulunulmuştur. Devamında, bilişim sistemlerinin sağladığı avantaj ve dezavantajlar konusunda bilgi verilmiştir. Özellikle tezin ana konusunun temelini oluşturan bilişim suçu kavramı, tanımı, bu suç ile ilgili işleniş biçimleri ve bir takım örnekler verilmiştir.

Tezin ikinci bölümünde ise Türk Hukukunda ki bilişim suçları üzerinde durulmuştur. Kanun koyucunun bilişim suçu olarak hangi eylemleri kabul ettiği, hangi eylemlere bilişim vasıtalı suçlar olarak tanımladığı üzerinde durulmuştur. Bilişim suçlarının tanımları yapılarak, madde metinlerinin neyi ifade ettiği ayrıntılı bir şekilde açıklanmıştır. Özellikle öğretide bu suçlarda yaşanan bir takım tartışmaların neler olduğu konusuna değinilmiştir.

Tezin üçüncü bölümünde adli bilişim kavramı ve adli bilişim sürecinde yaşananlar anlatılmıştır. Adli bilişim alanında belli bir Standardizasyonun olup olmadığı, mevcut durumun ne şekilde devam ettiği açıklanmıştır. Olay mahalline gidilmeden önce yapılması gerekenler ile olay mahallinde ve sonrasında teknik açıdan yapılması gerekenlerin neler olması gerektiği hususuna değinilmiştir. Adli bilişim evreleri tanımlanmıştır.

Tezin son bölümünde ise ana konumuz olan Ceza Muhakemesi açısından bilişim sistemleri üzerine arama ve el koyma mevzuatı irdelenmiştir. Özellikle Ceza Muhakemesi Kanunu 134. Maddesinde 6526 sayılı kanun ile yapılan son değişikler ve mevcut yasal düzenlemelerin yerinde olup olmadığı açıklanmaya çalışılmıştır. Mevcut kanun maddesinde yer alan hükümlerin hangi hususlarda yetersiz kaldığı, ne şekilde değiştirilmesi gerektiği yorumlanmıştır. Ayrıca CMK 134. Maddesi ile ilgili olarak yönetmelik maddeleri incelenmiş ve mevcut hali ile neden yetersiz kaldığı açıklanmıştır. Bunun haricinde, Kanun maddeleri ile uygulamada yaşanan sorunlar üzerinde durulmuştur. Emsal Yargıtay kararlarından kısaca örnekler verilerek yan mevzuatlar incelenmiştir. Son olarak; haksız bir şekilde arama ve el koyma tedbirine maruz kalan bir kişinin başvurabileceği hukuki haklarından bahsedilerek tezin değerlendirme ve sonuç kısmına geçilmiştir.

ABSTRACT

The first section of the thesis focuses mainly on digital evidence and concepts relevant to it in general, in which definitions of information systems within terminology and practice are also given in brief. The definition of digital evidence, the importance of hash value and its characteristics are covered and terminologically approached as well. The advantages and disadvantages of information systems are discussed under this section and information, along with several examples, is given about the informatics crime, which is the main subject of the thesis, its forms of committing the crime.

The second section focuses on informatics crimes under Turkish Law where it is discussed which acts are considered as an informatics crime, which acts are considered as crimes committed through informatics. In this section, informatics crimes are defined and the

provisions of the Law are explained in detail. The doctrinal discussions about such crimes are also covered under this section.

The third section explains the concept criminal informatics and what happens through the criminal procedure. It is explained that there is not any standardization on criminal informatics field and how the current situation is. Here, criminal informatics stages are described and it is further mentioned what needs to be done technically before entering the crime scene, in the crime scene as well as in the period after leaving it.

The last section of the thesis focuses on the regulations on search and seizure measures on information systems as per Criminal Procedure. In this section, an emphasis is put on recent amendments made on Article 134 of the Criminal Procedure Law as per the Law numbered 6526 and it is discussed whether or not the current regulations are legitimate. Opinions on why some provisions of the current law are required to be amended and to what they are required to be replaced with. Also, secondary regulations regarding Article 134 are examined and the reasons for what they are deemed inadequate are addressed. Furthermore, it is focused on the practical problems arising out from the provisions of the Law and extracts from the Supreme Court precedents are given. Lastly, the rights of a person who has been subject to search and seizure measures in an unjust manner are explained which is then followed by the conclusion part of the thesis.

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
age	: Adı geçen eser
ARPANET	: Advanced Research Projects Agency Network
Bkz/.Bknz.	: Bakınız
CD.	: Ceza Dairesi
DNS	: Domain name server (Alan adı sistemi)
E.	: Esas
EFTS	: Elektronik Funds Transfer System
E-imza	: Elektronik imza
E-posta	: Elektronik posta
E.T	: Erişim Tarihi
EİK	: Elektronik İmza Kanunu
HD	: Hukuk Dairesi
http	: hypertext transfer protocol
IP	: internet protocol
ISP	: Internet Service Provider
İYTE	: İzmir İleri teknoloji Enstirüsü
MİT	: Milli İstihbarat Teşkilatı
Mp3	: Moving Picture Experts Group Layer-3 Audio
POSS	: Point of Sale System
RF	: Radyo Frekansı
s	: sayfa
S.R.G.	: Sayılı resmi gazete
Stj.	: stajyer
STK	: Sivil toplum kuruluşu
TL	: Türk Lirası
T.C.	: Türkiye Cumhuriyeti

TCK	: Türk Ceza Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TİB	: Telekomünikasyon İletişim Başkanlığı
Vb.	: ve benzeri
Vd.	: ve devamı
TL	: Türk Lirası
WAP	: Wide Application Protocol (Kablosuz Uygulama Protokolü)
Wifi	: Wireless Fidelity
www	: World Wide Web

KAYNAKÇA

AHİ, Gökhan. (2009) "İnternet Sitelerinin Erişime Kapatılmaması İçin Bazı Hukuki Tavsiyeler". (http://www.bilisimhukuk.com/2009/07/internet-sitelerinin-erisime-kapatilmamasi-icin-bazi-hukuki-tavsiyeler/) adresinden alındı.

AHİ, Gökhan. (2009). "Doğal olmayan yoldan yapılan cinsel davranışlar" ne demektir?" (http://www.bilisimhukuk.com/2009/08/%e2%80%9cdogal-olmayan-yoldan-yapilan-cinsel-davranislar%e2%80%9d-ne-demektir/) adresinden alındı.

AKBULUT, Berrin. (2000). Bilişim Suçları. Konya: Selçuk Üniversitesi Hukuk Fakültesi.

AKINCI, Hatice/Alıç, Emre/ER, Cüneyd. (2004). "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk Derleyen. (Y. M. ATAMER, Düz.) İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

AKSOY, Eylem. (2002). Avrupa Konseyi Siber Suçluluk Sözleşmesi. İstanbul: Galatasaray Üniversitesi Hukuk Fakültesi Dergisi.

ALTAYLI, Behçet. (1985). Bilgisayar ve Basic ile Programlama (Cilt 2.). İstanbul: Filiz Kitabevi.

AYDIN, Emin. D. (1992). Bilişim Suçları ve Hukukuna Giriş. Ankara: Doruk Yayınları.

BERBER, Leyla. Keser. "Elektronik İmza Kanunu Yönetmelik Çalışmaları" Bilişim Hukuku, Türkiye II. Bilişim Hukuku Sempozyumu. (M. Tevetoğlu,) İstanbul: Kadir Has Üniversitesi Yayınları.

BAŞTÜRK İhsan., & ÖZEN Muharrem (2011) Bilişim İnternet ve Ceza Hukuku Ankara: Adalet Yayınevi

ÇAKIR Hüseyin., & KILIÇ Mehmet Serkan. (2014) Adli Bilişim ve Elektronik Deliller Ankara: Seçkin Yayınevi

DEĞİRMENCİ, Olgun. (2002). Bilişim Suçları. İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı.

DEĞİRMENCİ, Olgun., & YENİDÜNYA, Caner. (2003). Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları. İstanbul: Legal Yayıncılık.

DEĞİRMENCİ Olgun. (2014). Ceza Muhakemesinde Sayısal (Dijital) Delil Ankara Seçkin Yayınevi.

DOĞAN, Yusuf. Hakkı. 09 12, 2009 tarihinde www.ceza-bb.adalet.gov.tr/makale/146.doc adresinden alındı.

DÖNMEZER, Sulhi. (2001). Uluslar arası İnternet Hukuku Sempozyumu, 21-22 Mayıs 2001. İzmir.

DÜLGER, M. Volkan. (2004). Bilişim Suçları. Ankara: Seçkin Yayınevi.

DÜLGER, M. Volkan (2004). Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi. İstanbul: İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayın.

DÜLGER, M. Volkan (2012). Bilişim Suçları ve İnternet İletişim Hukuku. Ankara Seçkin Yayınevi.

ERSOY, Yüksel. (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları. Ankara: Ankara Üniversitesi Siyasl Bilimler Dergisi.

ERGÜN İsmail; Siber Suçların Cezalandırılması, Adalet Yayınevi Eylül 2008 1. Bası

HENKOĞLU Türkay, (2011). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi İstanbul Pusula: Yayınevi

KAPILI Kübra, (2013). Bilgisayarlarda ve Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama, El Koyma Bilgi Üniversitesi Sosyal Bilimler Enstütüsü (Yayınlanmamış Proje).

KARAGÜLMEZ, Ali. (2009). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri. Ankara: Seçkin Yayın.

KURT, Levent. (2005). Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Ankara: TODAİE Kamu Yönetimi Bölümü.

MEMİŞ, Tekin. (2001). Hukuki Açıdan Kitlelere E-posta Gönderilmesi. Erzincan: Atatürk Üniversitesi. Erzincan Hukuk Fakültesi Dergisi.

MITNICK, Kevın D; "Aldatma Sanatı" Çeviren: Nejat Eralp Tezcan Odtü Yayıncılık 3. Bası Şubat 2009.

ÖNEMLİ, Murat. (2004). İnternet Suçlarıyla Mücadele Yöntemleri. TODAİE Yüksek Lisans Tezi Ankara.

ÖZDİLEK, Ali. Osman. (2006). Bilişim Suçları ve Hukuku. İstanbul: Vedat kıtabevi.

ÖZDİLEK, Ali. Osman. (2002). İnternet ve Hukuk. İstanbul: Papatya Yayınevi

ÖZEL, Cevat. (2009). "Bilişim İnternet Suçları." (http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm) adresinden alındı

ÖZGENÇ, İzzet. (2007). Türk Ceza Hukuku Genel Hükümle. Ankara: Seçkin Yayınları 2. Bası.

ÖZMESTİK, Fehmi. Ünsal. (2009). "Sitesi Erişime Kapatılanlar İçin İtiraz Yolları" (http://www.bilisimhukuk.com/2009/08/sitesi-erisime-kapatilanlar-icin-itiraz-yollari/) adresinden alındı.

ÖZMESTİK Fehmi Ünsal. (2010). "Bilgisayardaki görüşme kayıtları sadece "veri" değildir, başlı başına bir "iletişim"dir" (http://www.bilisimhukuk.com/2010/03/bilgisayardaki-gorusme-kayitlari-sadece-veri-degildir-basli-basina-bir-iletisimdir/) adresinden alındı.

ÖZTÜRK, Bahri. (2002). "Ceza Muhakemesi ve İnternet", Uluslar arası İnternet Hukuku Sempozyumu. İzmir: Dokuz Eylül Üniversitesi.

TANRIKULU Cengiz. (2014) Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma Ankara: Adalet Yayınevi

YAZICIOĞLU, R. Yılmaz. (1997). Bilgisayar Suçları Kriminoloji Sosyolojik ve Hukuki Boyutları. İstanbul: Alfa Yayınevi.

YAZICIOĞLU, Yılmaz. (2001). Bilgisayar ağların ile ilgili suçlar konusunda Türk Ceza Konunu 2000 Tasarısı, Uluslararası İnternet ve Hukuku sempozyumu, 21-22 mayıs. İzmir: Dokuz Eylül Üniversitesi Yayını (2002)

YILMAZ, Davut. (2004). Hacking Bilişim Korsanlığı ve Koruma Yöntemleri. İstanbul: Hayat Yayıncılık.

YILMAZ, Zekeriya. (2004). Gerekçe ve Tutanaklarla Yeni Türk Ceza Kanunu. Ankara : Seçkin Yayınevi.

ELEKTRONİK AĞ ADRESLERİ

http://www.tbmm.gov.tr

http://www.kazanci.com

http://tdkterim.gov.tr/?kelime=Bili%FEim&kategori=terim&hng=md

http://www.bilisimhukuk.com/2009/08/sitesi-erisime-kapatilanlar-icin-itiraz-yollari/

http://www.bilisimhukuk.com/2009/08/%e2%80%9cdogal-olmayan-yoldan-yapilan-cinsel-davranislar%e2%80%9d-ne-demektir/

http://www.bilisimhukuk.com/2009/07/internet-sitelerinin-erisime-kapatilmamasi-icin-bazi-hukuki-tavsiyeler/

http://www.bilisimhukuk.com/2010/03/bilgisayardaki-gorusme-kayitlari-sadece-veri-degildir-basli-basina-bir-iletisimdir/

http://www.resmigazete.gov.tr/eskiler/2005/06/20050601-15.htm

http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.8200&sourceXmlSearch=&MevzuatIliski=0

http://www2.tbmm.gov.tr/d24/1/1-0676.pdf

http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

http://www.hukukihaber.net/bilgisayar-verilerinin-yedeklenmesi-ve-yasak-veriler-makale,3527.html

http://www.ekizer.net/bilisimsuclari-sibersuclar/

http://www.adlibilimler.net/content/adli-bilimler-0

http://www.leylakeser.org/search/label/Adli%20Bilişim

http://www.iso27001security.com/html/27037.html

http://www.iso27001security.com/html/27042.html

http://www.iso27001security.com/html/27043.html

(BİRİNCİ BÖLÜM)

GENEL OLARAK DİJİTAL DELİLLER

§ I. Giriş

Bilgi teknolojisinin giderek artması ile 21. Yüzyılda Bilişim Çağının yaşandığı kabul edilmektedir. Bu teknoloji karşısında ortaya çıkan yeni hukuki aykırılıklar, mevcut klasik suçlardan bir takım farklılıklar arz etmektedir. Bilişim suçları, diğer suç tiplerine nazaran çok farklı yöntemler ile işlenebilmektedir. Bu suçlar, özellikle işlenme cazibesi ve kolaylıkları başta olmak üzere, kendisine has özellikler bakımından gerçekten büyüleyici olarak nitelendirilebilir[1]. Örneğin; Çengelköy sahilde, bilgisayarı ile oturan ve bu alanda ciddi bilgi sahibi olan bir kişi *"hacker"* internet sayesinde çok farklı yöntemlerle kişilerin kredi kartı bilgilerini elde edebilir, birtakım internet sitelerine yetkisiz erişebilir, o sitelerin içindeki verileri yok edebilir ya da sevmediği kişilere internet üzerinden hakaret edebilir, onlar yerine sosyal paylaşım sitelerinden hesap açabilir yada var olan hesaplarını ele geçirebilir. Bir başka deyişle; aklınıza gelebilecek birçok suçu kendisini gizleyerek birkaç saat içinde gerçekleştirebilir. İşte bu tip suçlarda, özellikle faile ulaşılması bir hayli zor olduğundan ve faile ulaşıldığında suçun işlendiğine ilişkin en önemli kanıtın dijital deliller olması sebebi ile Adli Bilişim alanında çalışmalara ihtiyaç duyulmuştur. Adli bilişim, adli bilimler dalının altında yer almaktadır. Adli bilimler esas olarak tıp, kimya, fizik, biyoloji, jeoloji, özel teknikler, sosyoloji, hukuk, psikoloji, felsefe gibi birçok bilim dalı ve teknolojiden destek alan bir bilimler topluluğudur. Bu bilim dallarının adli sisteme yansıyan kısımları adli bilimleri oluşturmaktadır[2]. Adli Bilişim ise bilişim incelemelerinin Mahkeme süreci göz önünde bulundurularak gerçekleştirilmesi, delil toplama ve inceleme süreçlerinin kanuni ihtiyaçlar gözetilerek yapılması sürecidir. Bu durumun farkına varan birçok ülke kanunlarını ivedilikle yenilemişlerdir. Fakat ülkemizde maalesef kanun koyucu tarafından işin uygulama kısmını da göz önüne alan doyurucu bir düzenleme getirilmemiştir.

Bilişim ve Bilgisayar kelimeleri uygulamada eş anlamlı ifade ediyormuş gibi kullanılsa da bu bir yanılgıdan ibarettir. Sözlüklerde bilgisayarın tanımı; "Çok sayıda

[1] ALTAYLI Behçet, Bilgisayarlar ve Basic ile programlama, Filiz kitabevi, İstanbul, 1985, Sahife 37vd; Karagülmez Ali, Bilişim Suçları Ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayın, Ankara 2009, 2. Bası, Sayfa; 29 vd.

[2] http://www.adlibilimler.net/content/adli-bilimler-0 "Adli Bilimler" Dr. Ertan SEVEN Son Erişim 05.03.0215.

aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, elektronik beyin olarak" verilmiştir. Bilişim ise "insanların teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı bir biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi" olarak tanımlanmıştır[3]. Zira gelişen teknolojiyle, bilgisayar kavramı yerine yeni kavramlar gelebilecek, yeni ürünler piyasaya çıkabilecektir.

Günümüzde bilişim sistemlerinin kullanılmadığı bir alanın kalmaması, bilişim suçlarının etki sahasını da her geçen gün genişletmektedir. Bilişim suçu kavramını tahlil ederken, önce konunun teknik kavramları üzerinde durulması gerekmektedir.

Bununla birlikte tezin ana konusu olan bilişim sistemleri üzerin arama ve el koyma tedbirinin uygulanmasında yaşanan aksaklıklar ve kanun koyucu tarafından çıkartılan kanun maddeleri karşılaştırılmıştır. Yeni teknolojik gelişmeler ve uygulayıcıların yaşadığı problemler ışığında yeni kanuni düzenlemelere gidilmesi gerektiği kanaatine varılmıştır. Tezde konuya ilişkin mevcut hukuki düzenlemeler vurgulanmış, söz konusu düzenlemenin ayrıntılı açıklaması yapılmış, öğretide ve emsal Yargıtay kararlarında varılan sonuca değinilerek bir sonuca varılmıştır.

§ II. Temel kavramlar

A- Bilişim ve bilişim alanı

Bilişim Fransızca "inormatique" kelimesinden ortaya çıkan ve "enformatik" şeklinde Türkçe kullanılan ve türetilen bir kavramdır[4].

Bilişim alanı ise kavram olarak bir bilim kurguya dayanmaktadır. "Neuromancer" adındaki, William Gibson tarafından yazılan romanda "cyberspace" olarak adlandırılan bir dünyadan bahsedilmektedir. Bugünlerde ise artık bilimsel temele dayanan büyük bilgi sistemlerine ulaşılmıştır[5].

---

[3] ÖZEL Cevat, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm (Erişim 07.02.2012), sayfa 1.

[4] DEĞİRMENCİ Olgun - Caner YENİDÜNYA; Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul, 2003, sayfa 42.

[5] YAZICIOĞLU R. Yılmaz; Bilgisayar Suçları Kriminoloji Sosyolojik ve Hukuki Boyutları ile Alfa Yayınevi, İstanbul, 1997, sayfa 29.

Bilişim kavramı Türk Dil Kurumu'nun Bilim ve Sanat Terimleri Ana Sözlüğünde şu şekilde tanımlanmıştır:

"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır." [6]

Bilişim kavramı öğretimizde şu şekillerde tanımlanmıştır:

"bilişim teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi ve değerlendirilmesi ve aktarılmasıyla ilgili bir bilim dalıdır"[7].

"İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir"[8]. Bilişim alanı ise bilgisayarları da içine alan, verilerin toplanıp yerleştirildikten sonra bunların otomatik işlemlere tabi tutma imkanı veren manyetik sistemleridir[9].

B- Bilişim sistemi

Bilişim Sistemi, yazıcı, modem gibi tüm çevre birimleri de dahil olmak üzere bilgisayardan beklenen tüm amaçları gerçekleştirmeye elverişli donanım ve yazılım öğelerinin bütünüdür[10].

---

[6] (http://tdkterim.gov.tr/?kelime=Bili%FEim&kategori=terim&hng=md) (Erişim: 07.09.2014)

[7] DEĞİRMENCİ Olgun - YENİDÜNYA Caner, 2003 age s 27.

[8] DÜLGER M. Volkan; Bilişim Suçları, Ankara Seçkin Yayınevi, Kasım 2004, s 47.

[9] YAZICIOĞLU R. Yılmaz, 1997 age s 29.

[10] ÖZDİLEK Ali Osman; Bilişim Suçları ve Hukuku, Vedat Kitapçılık 2006, s 179.

5237 sayılı yeni TCK'nun 243. Maddesinin gerekçesinde ise bilişim sistemi "veri toplayıp yerleştirdikten sonra bunları otomatik işlemelere tabi tutma olanağını veren manyetik sistemlerdir" şeklinde tanımlanmıştır.

C- Bilgisayar

Belirli komutlara göre veri işleyen ve depolayan bir makine olarak da adlandırılan bilgisayar, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, elektronik beyin anlamına gelmektedir.

Bilgisayar denilen sistem aslında verilerin "1" ve "0" lı hallere dönüştürülmüş biçimidir. İlk olarak 1948 yıllında ünlü matematikçi Dr. Claude Shannon'un matematik formüllerinin bağlantı süreçlerini, ikili kod (binary code) ve hesaplama şekillerini bulmasıyla ortaya çıkmıştır. O günden bu günü geliştirilen birtakım elektronik cihazlarda, ikili sayma sistemine dayalı kodlama kullanılmaktadır[11].

Bilgisayar çalışırken, verileri (0) ve (1) sayılarına çevirir ve bu sayılara denk gelen "açık" veya "kapalı" durumlarda olabilen elektronik anahtarlar söz konusudur. Bu kodların ikili bileşenlerine "bit" denilmektedir. 8 bitlik bir gruba "1 byte" denilir. Bilgisayarda "0" ve "1" sayılarının değişik sistemleri söz konusudur[12]. Aynı zamanda bilgisayarda yer alan klasör ve dosya yapıları 0 ve 1'lerden oluşan verilerdir.

D- Veri

Veri, bilişim sistemlerinin temel birimidir. Bilişim sistemlerinin amacı, veriyi saklamak, işlemek ve sonuç çıkartmaktır[13]. Veri, bilgilerin bir formata dönüştürülmüş halidir[14]. Veri, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgiyi ifade eder[15].

---

[11] KARAGÜLMEZ Ali; Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayın, Ankara 2009, 2. Bası, s 29.

[12] YILMAZ Davut; Hacing Bilişim Korsanlığı ve Koruma Yöntemleri, 2. Basım, Hayat Yayıncılık, İstanbul 2004, s 20.

[13] ERGÜN İsmail; Siber Suçların Cezalandırılması, Adalet Yayınevi, Eylül 2008, 1. Bası, s 6.

[14] YAZICIOĞLU R. Yılmaz, 1997 age s 29.

[15] Avrupa Konseyi Siber Suç Sözleşmesi Madde 1.

E- Bilgisayar ağı kavramı

Birbirlerine bir kabloyla bağlanmış ve bu sayede bilgi alışverişinde bulunabilen birden fazla bilgisayardan oluşan yapıdır. Bilgisayar ağlarının farklı türleri mevcuttur;

1. Yerel alan ağları

Birbirlerine yakın bilgisayarları birbirine bağlayan ağlara yerel ağ denir. Yerel alan ağları (LAN-Local Area Network) adından da anlaşılacağı üzere belli bir lokasyon içerisinde oluşturulmuş ağ sistemidir.

2. Geniş alan ağları

Ağa dahil olan bilgisayarlar arasında mesafe sınırı yoktur. Şehirler veya ülkeler arası bilgisayarları birbirine bağlı ağlara geniş alan ağ denir[16]. Bir mekanda bulunan kullanıcı ve bilgisayarların başka bir mekanda bulunan kullanıcı ve bilgisayarlarla iletişim kurabilmesi ve başka tip ağları birbirine bağlamakta kullanılır.

F- İnternet

İnternet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır. İnternet 20. Yüzyılın en büyük buluşlarından biridir. İnternet dünyada geçerli olan TCP/IP protokolü ile bilgisayar sistemlerinin dünya çapında birbirine bağlayan ağdır[17]. Bir başka ifade ile İnternet TCP/IP protokolü ile bilgisayar sistemlerini Dünya çapında birbirine bağlayan ağdır. Bilgisayarların internet üzerinde bilgi ve mesaj paylaşımı yapmalarını sağlayan sistem, basit olarak şöyle özetlenebilir; 1) Her mesaj ve bilgi, paket denilen ufak parçalara ayrılır. 2) Bu paketler bir yol boyunca gidecekleri yere ulaştırılır. 3) Paketler gidecekleri yere ulaştıktan sonra yeniden birleştirilerek ilk orijinal hallerine dönüştürülür[18]. Bu işleri yapmak, Internet üzerindeki en önemli iki iletişim protokolü olan TCP ve IP'nin görevidir. TCP, (Transmission Control Protocol) demektir. Gönderilecek paketlere ayırma ve yeniden birleştirme işini yapar. IP, Internet Protocol demektir. Gönderilecek paketlerin doğru hedefe gitmelerini sağlamakla yükümlüdür.

---

[16] YILMAZ Davut; s 24.

[17] ÖNEMLİ Murat; İnternet Suçlarıyla Mücadele Yöntemleri TODAİE (Yayınlanmış Yüksek Lisans Tezi) , Ankara, Nisan 2004, s 4.

[18] İzmir Yüksek Teknoloji Enstitüsü Mühendislik Fakültesi "6-11 Haziran 2009 Adli Bilişim" kursu ders notları.

Bilgisayarların birbirleriyle veri alışverişi ve ortak iş yapacak biçimde bağlanması ile oluşan bilgisayar ağları, bilgisayarların potansiyel gücünü inanılmaz boyutlara çıkarmıştır. Bunun sonucunda oluşan internet, bilgiye ve bilgisayar kaynaklarına global erişimi sağlamaktadır. Bir ağ (Network) yapısı olarak adlandırılan internetin ilk adımları, 1960'lı yıllarda Amerikan Savunma bakanlığında, Pentagon'un sabit bilgisayar sistemlerinin nükleer saldırılara karşı korunma yöntemlerini araştırması ve sonra akademisyenler, Amerikan Birleşik Devletleri ve haberleşme uzmanlarının, birbirleri ile uzak mesafede bulunan bilgisayarları, birbirlerine nasıl bağlayabileceklerini araştırmaya başlamaları ile atılmıştır. 1990 yılından itibaren dünya çapında yaygınlaşmaya başlayan internet, kısa sürede hızlı gelişme göstermiştir. İnternet'e bağlanma maliyeti düşerek, güçlü ve kullanımı kolay programlar internet vasıtasıyla iletişim kurmayı ve bilgi erişimini ve yayıncılığı herkese açık bir imkân haline getirmiştir. Bir internet uygulaması olan world wide web, multi-medya verilerin (metin, ses, resim, film) tek bir sistemle bütünleşik bir biçimde yayılmasına ve erişilmesine imkân vermesiyle, internet kullanıcı sayısında ve internette yayınlanan bilgi miktarında patlamaya yol açmıştır. Artık internet bir bilgi denizi olarak da tanımlanabilmektedir. 2009 yılına gelindiğinde 7-8 milyar kişinin internet ile ilgilendiği ifade edilmektedir[19].

§ III. Bilişim sistemlerinin sağladığı yararlar ve ortaya çıkardığı yeni problemler

A- Bilişim sistemlerinin sağladığı yararlar

Bilişim sistemleri günlük hayatımızın hemen hemen her alanında yer almakta ve buna bağlı olarak da bilişim teknolojisi de günden güne gelişmektedir. Bilişim sistemleri dediğimizde aklımıza sadece bilgisayarlar değil, yazılımlar, banka kartları, cep telefonları, internet aracılığıyla para transferleri, elektronik imza, bilgisayar ortamına aktarılmış ve hizmete sunulan elektronik devlet uygulamaları, elektronik ortama atılmış veriler ve bunun gibi teknolojik gelişmelerde gelmelidir.

Bilişim sistemleri artık sınırları çizilebilecek bir teknoloji olmaktan çıkmıştır. Bilişim sistemleri günlük hayatın ve iş hayatının yaklaşık bütün sektörlerinde kullanılmakta ve bilişim teknolojisi gelecek yıllar düşünüldüğünde henüz başlangıç aşamasında bulunmaktadır. Gelecekteki toplumlar hayatlarında bilgi işleme, günümüzde olduğundan çok daha fazla yer vereceklerdir.

[19] KARAGÜLMEZ Ali, 2009 age s 35.

Günümüzde askeri kuruluşlar, ticari kuruluşlar, adalet sarayları, finans kuruluşları ve üniversiteler, bilişim teknolojilerini kullanarak hayatımızı kolaylaştıran yeniliklere olanak vermişlerdir. Bu yeniliklerin başında; elektronik kredili yaşam (POSS: Point of Sale System), mali kaynakların elektronik aktarımı (EFTS: Elektronik Funds Transfer System), bankamatik kartları, kredi kartları, yine internet sayesinde haberleşme (sesli-görüntülü), borsa oynamak, her türlü bilgiye ulaşabilme, sosyal paylaşım, arkadaşlık edinme gibi de birçok olanaklar gelmektedir. 3G denilen teknolojinin de ülkemizde kullanılmaya başlanması sonucu her zaman ve her yerde internet kullanımı giderek yoğunlaşacak ve buna bağlı olarak yenilikler de giderek artacaktır. Bilişim sistemlerinin hayatımıza kattığı yararlar sadece bu sayılanlarla sınırlı kalmayacaktır. Gelecek yıllarda akıllı evlerin yaygınlaşması, akıllı robotlar, yapay zekalı robotların ortaya çıkması ile bilişim sistemleri farklı bir boyuta ulaşacaktır.

B- Bilişim sistemlerinin ortaya çıkardığı yeni problemler

Her yenilik beraberinde birtakım sorunları da getirmektedir. Öncelikle bilgisayar ve internet gibi teknolojiler günümüz gençlerinin ilgisini her ne kadar çekse de, internet üzerinde, özellikle chat gruplarında kişilerin sorumsuz davranması, rumuz kullanımı veya sahte isim kullanma kolaylığı nedeniyle internette gerçekleşen ilişkilerde, kişiler ahlâk sınırlarını zorlayan davranışlarda bulunabilmektedirler. Yine bu şekilde, çocuk pornosu içerikleri, illegal akımlar, şiddet ve değişik türde sapıklıklar içeren web sayfalarının bulunması da sıkıntılara yol açmaktadır. Nitekim internet üzerinden gerçekleştirilen hareketlerde kimlik gizlemenin kolay olması, bu tür suçların işlenmesini daha da cazip hale getirmektedir. Özellikle uzmanlarca yapılan araştırmalarda da internet kullanımının yarattığı bağımlılığın sonuçlarının, en az alkol ya da ilaç bağımlılığı kadar ciddi bir sorun teşkil ettiği ortaya çıkmaktadır. Son zamanlarda sosyal ağ kullanımının artması ve her bireyin bir muhabir edası ile çevresinde olup biten her şeyi kendi hesabından umuma paylaşması ortaya yeni bir kavram sosyal medya ismi çıkarmıştır. Son günlerde ülkemizde ve dünyada yaşanan gelişmelere baktığımızda sosyal medya üzerinden yayılan haberlerin çok kısa sürede milyonlarca kişiye ulaştığı görülmektedir. Burada asıl sıkıntı bu platformda yayınlanan bu içeriklerin gerçek dışı, yalan, iftira içerikli olması halinde yaşanmaktadır. Zira paylaşılan haberin doğru olup olmadığını denetleyen bir mekanizma olmadığı gibi bu bilgilerin belirli etik değerlere sahip çıkılarak paylaşılması hususunda bir fikir birliği de yoktur. Bu da ortaya bu tezin dışında tartışılması gereken farklı bir konuyu çıkarmaktadır.

Tüm bunların yanında makinelerin ve bilgisayarların yapabilecekleri şeylerin gün geçtikçe artması, insan gücüne olan ihtiyacı azalttığından istihdamda da bir azalmaya sebebiyet vermektedir. Günümüzde yavaş yavaş insan gücünün yerini teknoloji almaya başlamıştır. Tüm bu durumların varlığı insanların sosyal ve kültürel davranışlarında farklılıklara yol açabilecektir. İşte bu sebeplerle meydana gelen yeniliklere ve teknolojilere uygun düzenlemelerin geciktirilmeden oluşturulması ve doğması muhtemel olan zararların önüne geçilmesi gerekmektedir.

§ IV- Bilişim suçları

A- Bilişim suçu kavramı

Bilgi Teknolojisinin gelişmesi sonucu tartışılmaya başlanan bu kavram üzerinde henüz doktrinde kuvvetli bir fikir birliğine varılamamıştır.

Bu suçlar tanımlanırken değişik kavramlar kullanılmaktadır. Bunlar arasında, uluslar arası alanda en çok kabul, "siber suç", "elektronik suç", "dijital suç", "bilgisayar suçu", "bilişim suçu" dur[20].

Bilişim Suçları, ilk etapta geleneksel suçların bilgisayar yoluyla işlenmesi şeklinde algılanırken, bilişim teknolojilerinin hızla gelişmesi ile yeni suç tiplerini yarattığı artık kabul edilmektedir. Zira, bilgisayar teknolojilerinde ve bunun daha üstünde yer alan internet üzerindeki hızlı gelişmeler, bilişim suçlarının değişik kategorilerini oluşturan yeni teknolojik suç çeşitlerini üretmektedir.

B- Bilişim suçunun tanımı

Gerek uygulama da gerekse doktrinde bilgisayar suçu ile bilişim suçu ayrımı net olarak ortaya konulamamış ve bu konuda ortak bir tanım da yapılamamıştır[21]. Türk hukukunda, bilişim suçlarına ilişkin farklı tanımlar bulunmaktadır. Bunlardan bazıları şöyledir;

Bilişim suçu; bir görüşe göre, "elektronik bilgi işlem kayıtlarına yasa dışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılmasıdır".[22] Başka bir görüşe göre,

[20] KARAGÜLMEZ Ali, 2009 age s 35.

[21] AKBULUT Berrin; Bilişim suçları, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Sayı 1-2 c.8 2000, s 399.

[22] AYDIN Emin Doğan; Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara, 1992 s 27.

"verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar"[23]. Bir diğer görüşe göre, bilgisayarları da kapsayan ancak daha geniş olan bilişim araçları işlenen veya bilişim araçlarına karşı işlenen suçlardır[24]. Bir başka tanımda ise aracı bilgisayar konusunu, vasıtasını veya simgesini oluşturduğu, suç olgusu içeren fiiller bilgisayar suçudur[25].

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" dır[26].

Bilişim suçlarını genel olarak üç ana başlık altında kategorize edilebilir[27].

1. Hedef olarak bilişim sistemleri

Burada bilişim sistemleri tabiri caizse suçun mağduru konumundadır. Bir bilişim sistemine yetki dışı erişim, sistemin işleyişinin aksatılması veya kesintiye uğratılması, bilişim sistemi üzerindeki verilerin silinmesi, değiştirilmesi bu ana başlık altına alınabilir. Örneğin bir bilgisayar virüsünün yazılması ve hedef sisteme bulaştırılması sonucu sistemin işleyişinin durması, sistem üzerindeki verilerin zarar görmesi maddi manevi birçok zarara yol açabilir. Bilişim sistemine yetkisiz olarak girişin sonucunda yine zararlar meydana gelebilir. Örneğin; her hangi bir kamu kuruluşunun veya özel kurumun bilişim sistemine yetkisiz erişim sonucu sızma veya uzaktan servis dışı bırakma eylemleri sonucu oluşabilecek zararlar. Yada istihbarat teşkilatlarının sistemlerine erişim ile bilgilerin çalınması, hastane veri tabanlarındaki bilgilerin veya havayolu firmalarının uçuş planlarının değişmesi, banka verilerinin çalınması veya iletişimi sağlayan servislerin durdurulması inanılmaz derecede zararlar meydana getirir. Burada hedef direk olarak bilişim sistemleridir.

2. Bilişim bağlantılı suçlar

[23] AKBULUT Berrin; 2000 age s 551.

[24] ERSOY Yüksel; Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, Ankara Üniversitesi Siyasal Bilimler Dergisi Cilt: 49, s 3-4 Ankara 1994.

[25] YAZICIOĞLU R. Yılmaz, 1997 age s 142.

[26] ÖZEL Cevat, age s 2-3.

[27] İYTE; Mühendislik Fakültesi "6-11 Haziran 2009 Adli Bilişim" kursu ders notları.

Bilişim sistemlerinin hayatımızın her alanına girmesi ile birlikte bilişim sistemlerinin getirileri, özellikle elektronik ticaret gün geçtikçe daha çok kullanılır olmaktadır. Bunu fırsat bilen suçlular, bu alanda da çıkar sağlayabilmek amacıyla harekete geçmiş ve hepimizin bildiği gibi bilişim sistemlerini kullanarak başkalarına ait ödeme sistemleri bilgilerini ele geçirip çok büyük zararlara sebep olmaktadırlar. Bunun dışında kopya yazılım kullanımı ve eserlere karşı telif haklarının ihlali de bilişim sistemleri vasıtası ile gerçekleştirilebilmektedir.

3. Bilişim vasıtalı suçlar

Teknolojinin ilerlemesi ve hayatın her alanına girmesiyle birlikte suçlularında, teknolojiyi kullanmaya başladığı hepimiz tarafından bilinmektedir. E-posta veya internet siteleri vasıtası ile hakaret sövme, kimlik saklamanın kolay olması sebebiyle oldukça kolay yapılabilmekte ve yine kimlik saklanabilmesinin kolay olması sebebiyle internet üzerinde terör propagandalarının yapılması, yahut uyuşturucu trafiğinin yönlendirilmesi oldukça kolay olmaktadır.

C-Bilişim suçlarının işlenme şekilleri ve saldırgan profili

1. Genel olarak

Bilişim suçlarını klasik suç tiplerinden ayıran en önemli özellik bu suçların işlenme şekillerinin farklılığıdır. Zira bilişim suçlarında, diğer suçlara nazaran daha çok ve yeni işlenme şekilleri söz konusu olmaktadır. Klasik suç tiplerinde suçun maddi unsurlarından birini oluşturan eylemler, faillerin fiziki hareketleriyle meydana gelmektedir. Bu fiziki hareket örneğin failin somut bir belgeyi değiştirmesi (evrakta sahtecilik suçu) eylemi ile olmaktadır. Bilişim suçlarında ise genellikle failin bir bilgisayar klavyesine dokunması dışında başkaca bir fiziki hareket olmamakta birlikte meydana gelebilecek zararlar çok daha fazla olmaktadır[28].

2. Bilişim suçlarındaki saldırgan profilleri[29]

a) Hedefli ve bilinçli saldırgan profili

[28] DÜLGER Volkan Murat, 2004 s 69.

[29] İYTE; Mühendislik Fakültesi "6-11 Haziran 2009 Adli Bilişim" kursu ders notları.

Bu gruptaki saldırganlara gerçek bilgisayar korsanı *"hacker"* denilebilir. Genellikle geçimlerini bilişim teknolojileri alanından sağlar ve üst düzey bilgi birikimine sahiptirler. Programlama konusunda oldukça ileri düzeyde olan bu kişiler özellikle sistem programlama ve network programlama alanlarında uzmandırlar. Bu kişiler bilişim teknolojilerinin, iletişim teknolojilerinin ve işletim sistemlerinin işleyişlerini, zafiyetlerini bulabilecek derecede teknik detay bilmenin yanında, art niyetli faaliyetlerini icra edebilmek amacıyla kendi programladıkları saldırı araçlarını kullanırlar. Sistem ve İletişim konularında bilgili oldukları için art niyetli faaliyetlerini sürdürürken geride iz ve delil bırakmamak için maksimum özeni gösterirler.

b) Hedefsiz ama bilinçli saldırgan profili

Bu gruptaki saldırganlar genellikle art niyetli faaliyetlerini icra ederek eğlence amaçlı suç işlerler. Belirli bir hedefleri yoktur ve rastgele kurban seçerler. Teknik bilgi ve becerileri mevcuttur ve çoğunlukla üniversite mezununu iş sahibi insanlardır. Programlama konusunda bilgileri bulunmakla birlikte çok nadir durumlarda kendilerinin programladıkları saldırı araçlarını kullanırlar. Genelde daha önceden bahsedilen birinci gruptaki saldırgan kitlesi tarafında programlanmış araçları kullanır ve bu araçların programlama kodları üzerlerinde değişiklik yaparak art niyetli faaliyetlerini icra ederler. Yakalanma kaygıları vardır ve gizlenmeye, iz bırakmamaya özen gösterirler.

c) Hedefli ama bilinçsiz saldırgan profili

Bu grup saldırganın amacı vardır. Ancak teknik bilgisinin zayıf olmasının yanında plansız ve programsızdır. Genelde olarak saldırganın teknik alt yapısı ve bilgisi bulunmamaktadır. Bunun yanında, basit düzeyde öğrendiği sınırlı bilgiye sahiptir. İnternet üzerinden kolayca bulunabilecek saldırı araçları kullanır. Kendini ispatlama çabası içerisindedir. Bu gruptaki saldırganlar yakalandıklarında en iyi olduklarını çeşitli şekillerde ima ederek ilgi toplamaya ve yaptıkları iş kötüde olsa övgü alacak derecede hava atma meraklılarıdır. Genellikle ergenlik çağında veya biraz geçmiş genç insan grubundadır. Arkasında çok fazla iz bırakır ve yakalanması çok kolaydır.

d) Hedefsiz ve bilinçsiz saldırgan profili

Amacı yoktur ve rast gele hedefler seçer. Sadece normal düzeyde bilgisayar kullanıcılarıdır ve teknik bilgisi yoktur. İnternet'ten bulduğu araçları kullanır ve çoğunlukla ne yaptığının farkında değildir. Tehlikelidir ve saldırgan kitlesinin büyük çoğunluğu bu guruptadır.

3. Bilişim suçlarında suçlu tipleri

a) Bilgisayar korsanı "hacker"

Aslında hacker tabirinin bir çok farklı tanımı mevcuttur. Doktrindeki en yaygın tanımına göre; Hacker, bilgisayar ve bilişim sistemleri konusunda, dahi derecede bilgi seviyesi olan yeni şeyler üreten, programlama konusunda uzman, sistemlerin yeni zayıflıklarını tespit edebilme ve bunları kapatabilme yetisine sahip kişilerdir.

Bir başka tanıma göre; "*Hacker"* diye tabir edilen insanlar teknik düzeyde dahi derecesinde bilgi sahibi, sistemler üzerinde giriş kapısı olarak kullanılabilecek yeni açıklar bulma, bu açıkları kullanma ve kapatabilme konusunda uzman kişilerdir. Daimi olarak yeni şeyler üretirler.

*"Hacker"*lar grup olarak ikiye ayrılır; iyi niyetli *"hacker"* (Beyaz Şapkalı / White Hat), Kötü niyetli "*hacker"* (Siyah Şapkalı / Black Hat). İyi niyetli *"hacker"*lar genellikle bilişim sistemlerinin güvenliği ve yeni sistemlerin geliştirilmesi konusunda çalışan insanlardır. Kötü niyetli "*hacker"*lar ise bilgi seviyelerinin kendilerine çıkar sağlamak amacıyla kullanırlar. Kimliklerini gizler ve yaptıkları eylemleri açıklamazlar, şan şöhret peşinde koşmazlar[30].

b) Cracker

Her türlü sistemin ve yazılımın şifrelerini kırabilme yetisine sahiptirler. Genellikle yazılım şifrelerini kırmaya yönelik eylemleri vardır. Bilişim sistemlerindeki şifreleri kırma yetkisine sahip değil, amacı zararlı iş yapmak şeklinde olacak. Hacker olabilme yolundadırlar. Bilişim sistemleri ve programcılık konusunda ileri düzey bilgiye sahiptirler.

c) Lamer

[30] ÖZDİLEK Ali Osman; İnternet ve Hukuk; Papatya Yayınları 2002 1. Bası s 166.

Hazır programlar vasıtası ile sistemlere erişim sağlamaya çalışan, hazır kodları kullanarak şifre kırma ve yetkisiz erişim eylemlerini gerçekleştiren orta düzeyde teknik bilgiye sahip kişilerdir. Kendilerini hacker zanneder ve başkalarına karşı kendilerinin hacker olduğu imajını vermeye çalışırlar. Şan ve şöhret peşindedirler.

d) Script Kiddie

Bilişim sistemleri, konusunda gün geçtikçe kendini geliştiren, çoğunlukla yaş grubu olarak 14-22 yaşlarında bulunan, iyi derecede bilgisayar kullanıcılarından oluşurlar. Tamamen hazır yazılımlar vasıtası ile güvenlik açıkları oldukça fazla olan sistemler üzerinde zararlı faaliyetlerini yürütürler. Yaş itibari ile kendilerini ispat çabası içerisindedirler. Programlama konusunda bilgileri az seviyede olsa da, genellikle kendi yazdıklar veya modifiye ettikleri trojanları başkalarının sistemlerine bulaştırmak suretiyle yetkisiz erişim eylemlerini gerçekleştirmektedirler. En çok karşılaşılan suçlulardandır.

e) Meraklılar ve kullanıcılar

Bilgisayar konusunda meraklı olup farkında olmadan merakları sebebiyle suç işleyenlerdir. Ya da çalıştığı kuruma kızgınlığı sebebiyle elinde bulunan yetkileri art niyetli olarak kullanan kişilerdirler.

Bilişim suçlarını klasik suç tiplerinden ayıran ve kendine özgü suçlar olmasını sağlayan en önemli özellik; bu suçların işlenme şekillerinin ve araçlarının farklılığıdır. Klasik suçlarda elle tutulur kolay bir şekilde gözle görülür bir fili davranış ve suçun aracı varken bu suçlarda böyle bir şey söz konusu değildir. Bu suçlarda her şey sanal alemde elektronik devreler arasında verilerle gerçekleşmektedir.

4. Bilişim suçlarının en yaygın işleniş araçları

a) Truva atı

Truva atı, bilişim sistemlerinde kullanılan en yaygın zararlı yazılımdır. Kullanıcının yararınaymış gibi gözüken ama içerisinde casus yazılımlar barındıran yazılımlara truva atı (Trojan horse) denilmektedir. Bir bilişim sistemi üzerinde yer alacak truva atı ile art niyetli bilgisayar korsanı truva atının programlandığı özelliğe göre, her türlü veriyi elde edebilecek, değiştirebilecek veya akla gelebilecek art niyetli tüm faaliyetleri icra edebilecektir. Yani truva

atı yazılımı, kurulmuş olduğu bilgisayarın yazılımının açıklarından yararlanarak bütün sisteme hakim olmakta ve failin bütün komutlarını yerine getirmektedir[31].

b) Bilişim virüsleri

Biyolojik hayatta var olan virüslerden farklı olarak, bilgisayar virüsleri aslında birer bilgisayar programlarıdır. Bilgisayarın kullanıcısından habersiz olarak sistemde bulunur ve art niyetli programcısının tasarladığı şekilde eylemler gerçekleştirir. Bilgisayar virüslerinin trojanlardan farkı kendi kendine bulaşabilme özellikleri vardır. Virüsler hedef sistem üzerine çeşitli yollar ile taşınarak bulaşır ve gerekli şartlar gerçekleştiği takdirde art niyetli eylemleri icra ederler. Çok çeşitli olmakla birlikte genel olarak dosya virüsleri, çalışabilir dosya virüsleri, boot sektör veya dosya sistemi virüsleri vs gibi çeşitleri mevcuttur. Bilgisayar ağları üzerinden(e-posta vs), disket, cd'ler, taşınabilir diskler vasıtası ile bulaşabilmektedirler. Virüslü bir dosya veya disk taşındığı bilgisayarında virüsten etkilenmesini sağlar. Virüsün bulaşabilmesi için muhakkak taşınması gerekir[32].

c) Ağ solucanlar

Ağ solucanları, virüslerden farklı olarak, taşınmadan kendi kendine yayılabilme özelliğine sahip bilgisayar programlarıdır. Yine virüsler gibi kullanıcıdan habersiz sisteme yerleşerek art niyetli faaliyetlerini icra ederler. Ağ solucanları genellikle bilgisayar ağları vasıtası ile hedef sistem üzerinde bulunan zafiyetten yani güvenlik açığından yararlanarak sistemlere bulaşırlar. Bu özelliklerin haricinde çoğunlukla virüslere benzemekle birlikte virüslerden farklı olarak dosya sistemi veya boot sector wormları yoktur. Genellikle çalışan bir servis veya hafıza bulunması muhtemel dosyaları etkilemektedir[33].

d) Casus yazılımlar

Yukarıdaki tüm zararlı yazılımlardan farklı olarak bunlar sisteme kendi kendilerine bulaşamazlar. Kullanıcının kandırılması vasıtası ile genellikle girmiş olduğu bir internet

[31] DEĞİRMENCİ Olgun; Bilişim Suçları, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı,(Yayınlanmış Yüksek Lisans Tezi), (İstanbul, 2002), s.79.

[32] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

[33] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

sitesinden sisteme bulaşan casus yazılımlar, sisteme bir şekilde yerleşerek art niyetli faaliyetin icra edilmesine sebebiyet vermektedir[34].

e) Mantık bombaları

Mantık bombaları genellikle bir bilişim sistemini servis dışı bırakmak amacıyla kullanılmaktadır. Mantık bombaları virüslerin, trojanların yada ağ solucanlarının içerilerinde yer alabilecekleri gibi ana sistemi uzaktan da servis dışı bırakabilirler. Mantık bombalarının adından da anlaşılacağı gibi bu art niyetli yazılım parçacıkları sistemi çeşitli mantıksal işlemlerle meşgul ederek başka bir iş yapamaz hale gelmesini sağlamaktadır. Örneğin; bir bilgisayarın sonsuz ve içinden çıkılamaz bir matematiksel döngüye girmesi sonucu işlemci başka bir işlemle uğraşamayacak ve servis dışı kalacaktır[35].

f) Şifre kırıcılar

Adından anlaşılabileceği üzere şifre kırıcılar, bilgisayar sistemleri üzerinde bulunan bir çok şifreyi bertaraf edebilmekte yada bertaraf edemese bile yenisi ile değiştirilmesini sağlamaktadır. Şifre kırıcılar bu bağlamda ya deneme yanılma yöntemi ile (zorlama brut-force) yada verinin şifrelenmiş halini değiştirmek suretiyle şifreleri kırmaktadırlar. Kırılacak şifreye göre bu yöntemler, yazılımlar vasıtası ile uygulanmaktadırlar. Deneme yanılma yönteminde doğru şifre bulununcaya kadar ya belirli bir sözlükteki tüm kelime ve varyasyonları şifre olarak denemekte yada tüm alfanumerik sıralama kombinasyonu denenmektedir. Bu yöntem şifrenin uzunluğuna göre oldukça vakit alabilir. Şifrelenmiş verinin değiştirilmesi yönteminde ise, verinin üzerinde bulunan şifre alanı bilinen bir şifre ile şifreleme algoritmasına uygun olarak değiştirilmektedir. Bu yöntem ise her zaman sonuç vermemekte şifrenin bertaraf edilebilmesi için saldırgan öncelikle şifreleme algoritmasının mantığını ve şifre alanının yerini iyi bilmelidir[36].

[34] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

[35] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

[36] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

g) Ağ koklayıcılar

Bilindiği gibi bilgisayar ağları iletişiminde veriler dijital aktarım medyaları üzeride akmaktadır. Ağ koklayıcıları veri aktarılan medyalar üzerinde akan verileri toplamakta ve buralardan bilgi elde etmektedirler. Günümüzde bilgisayar ağları üzerinde ne tür verilerin aktarıldığı düşünülürse bu saldırı aracı oldukça tehlikelidir. Çoğu zaman aktarılan veri iletişim ortamından şifreli olarak aksa bile günümüzde bu şifreleri deşifre edebilecek kapasitede ağ koklayıcıları mevcuttur.

h) Zafiyet avcıları

Zafiyet avcı yazılımları günümüzde bilgisayar sistemlerinde olması muhtemel ve giderilmemiş açıkları tespit ederek hedef sisteme sızma noktasını belirleyen yazılımlardır. Günümüzde neredeyse tüm saldırganlar bu yazılımları kullanarak art niyetli faaliyetlerini gerçekleştirmek istedikleri hedef sisteme nereden giriş yapabileceklerini tespit etmeye çalışmaktadırlar.

ı) Sosyal mühendislik

Sosyal mühendislik (Social Engineering) diye adlandırılan şey en genel anlamıyla insanları aldatarak kişisel bilgilerine veya direk şifrelerine ulaşma yöntemidir. Çok basit bir yöntem olmasına rağmen, aynı zamanda en etkili ve en çok kullanılan yöntemdir. Dünya'nın en tanınmış bilgisayar korsanlarından biri olan *"Kevin Mitnick"* aynı zamanda büyük bir sosyal mühendistir[37]. Telefonda herhangi bir bankadan arıyormuş gibi, sizden kişisel bilgileriniz almaya çalışılabileceği gibi, doğum yeri bilginizin sorulduğu bir maile "ne önemi var ki" diyerek verdiğiniz bir yanıt, gizli sorusu doğum yeri olan mail adresinizi kaptırmanıza da neden olabilecektir[38].

[37] MITNICK Kevın D; "Aldatma Sanatı" Çeviren: Nejat Eralp Tezcan Odtü Yayıncılık 3. Bası Şubat 2009 s 5.

[38] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

i) Protokol aldatmacaları

İnternet ve bilişim ağlarının yapı taşı bilgisayar iletişim protokolleridir. Buradaki aldatmaca sahte iletişim paketlerinin üretilmesi vasıtası ile hedef sisteme erişim veya hedef sistemin istenilen tuzağa yönlendirilmesi vasıtasıyla gerçekleşebilmektedir[39].

j) Salam tekniği

Salam tekniği, genellikle bankalarda yaygın olarak gerçekleştirilen bir bilişim suçu metodudur. Bu yöntem ile fail, banka hesaplarındaki küsuratların veya virgülden sonraki son bir ya da iki rakamı kendi belirlediği bir hesaba aktarmaktadır. Böylelikle banka çalışanları veya hesap sahipleri hesaplarda meydana gelen bu küçük miktarların yetkisiz hareketini fark edememektedir. Ancak bu küçük miktarların faile ait başka bir hesapta toplanması faile büyük miktarlarda hukuka aykırı yarar sağlamaktadır[40]. Bu tekniğin gerçekleştirilmesi için de genellikle truva atı yazılımının çeşitleri veya benzer işleve sahip yazılımlar kullanılmaktadır[41].

k) İstem dışı alınan elektronik postalar

Günümüzde özellikle büyük bilişim sistemlerinin önemli bir sorunu haline gelen istem dışı alınan elektronik postalar (spam mail), bir bülten veya haber gurubu üzerinden ticari amaç taşımayan, bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklâm olarak tanımlanmaktadır[42].

Ülkemiz açısından istem dışı alınan elektronik postalara ilişkin olarak 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkındaki Kanun[43] bulunmaktadır. Bununla birlikte artık reklam ve promosyon amaçlı gönderilecek iletilerde öncesinde tüketicilerden yazılı izin alınması gerekmektedir. Ayrıca ilgili elektronik posta içeriğinde o sistemden çıkarılması amacı ile bilgilendirme ve yönlendirmesi yapılması zorunludur. Ancak ticari amaçlı gönderilen elektronik postalar için önceden izin alma zorunluluğu bulunmamaktadır.

---

[39] http://www.ekizer.net/bilisimsuclari-sibersuclar/ Son Erişim 01.03.2015

[40] DÜLGER M. Volkan, 2004 s 71.

[41] MEMİŞ Tekin; "Hukuki Açıdan Kitlelere E-posta Gönderilmesi", Atatürk Üniversitesi. Erzincan Hukuk Fakültesi Dergisi, Sayı 1-4 Erzincan, 2001, s 432–433.

[42] MEMİŞ Tekin, s.432–433.

[43] http://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm (Erişim: 14.11.2014).

Tüketicilere yazılı izin alınmaksızın gönderilen elektronik postalar sebebi ile ilgili işletmecilere idari para cezası uygulanacaktır. Bunun haricinde; e-postanın içeriğinde tehdit, hakaret veya yasal olmayan propagandalar varsa bu takdirde bunlar ayrıca ceza davalarının konusunu oluştururlar. Bunun yanında istem dışı alınan elektronik postalar, sistemi engelleyecek boyuta ulaştığı takdirde bu, 5237 sayılı TCK'nın 244. maddesinde düzenlenen "bilişim sisteminin engellenmesi" kapsamında değerlendirilebilecektir[44].

Diğer yandan spam sorununun dünya çapında yaygınlık kazanması ve internetin kullanımının da artması dolayısıyla çeşitli ülkeler konu ile ilgili yasal düzenleme yapmak durumunda kalmışlardır. Özellikle bu konudaki en etkili ve kapsamlı yasal düzenleme Avusturya'da yapılmış ve Avusturya Telekomünikasyon Yasası'nın 101'inci maddesinde, spam açık bir hükümle yasaklanmıştır. Telekomünikasyon Yasası'nın 101'inci maddesine göre, bir elektronik postanın birden fazla kimseye veya reklâm amaçlı olarak gönderilebilmesi için alıcının önceden bir onayı gereklidir. Alıcı, istediği her zaman da bu onayını geri alabilmektedir. Kanun iki problem alanını kurala bağlamaktadır. Bunlardan biri, birden fazla insana gönderilen e-posta, diğeri de reklâm amacıyla gönderilen e-posta problemleridir. Bu şekilde e-postalar için 500 bin Şili'ne kadar ceza öngörülmüştür[45].

İstenmeyen e-postalar konusunda ABD'li Sophos kuruluşunca gerçekleştirilen bir araştırmaya göre, dünyanın en çok "spam" (istenmeyen) mesajlarını üreten 12 ülke arasında yüzde 15.6′ lık bir payı ile ABD birinci oldu. "Kirli Düzine" olarak adlandırılan söz konusu 12 ülke listesinde Türkiye yüzde 5.2 payı ile üçüncü sırada bulunuyor. 2009 yılının Nisan-Haziran döneminde dünyada oluşturulan "spam" e-posta mesajlarının yüzde 15.6'sı, ABD'den kaynaklanıyor. ABD'yi yüzde 11.1′lik payı ile Brezilya ve yüzde 5.2′lik payı ile Türkiye izliyor. "Kirli Düzine" listesinde yer alan diğer ülkeler ve payları söyle: Hindistan (yüzde 5), Güney Kore (yüzde 4.7), Polonya (yüzde 4.2), Çin (yüzde 4.1), İspanya (yüzde 3.4), Rusya (yüzde 3.2), İtalya (yüzde 2.8), Arjantin (yüzde 2.5) ve Vietnam (yüzde 2.3). Diğer ülkelerin ise, Nisan-Haziran dönemindeki toplam "spam" mesajlarının ancak yüzde 35.9′undan sorumlu olduğu bildirildi[46].

[44] KURT Levent, 2005 s 72.

[45] MEMİŞ Tekin, 2001 s 434-435.

[46] http://www.milliyet.com.tr/spam-mesajlarda-dunya-ucuncusuyuz--internet-1119939/ (Erisim: 17.09.2011)

l) Oltalama yöntemi

İngilizce bir kelime olarak kullanılan Phishing terimi, "Password Harvesting Fishing" ifadesi temel alınarak "password" ve "fishing" kelimelerinin bir araya gelmesinden oluşmuştur. İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünün 'f' harfinin yerine 'ph' harflerinin konulması suretiyle oluşmuş bir kavramdır. Phishing, *"Sosyal Mühendislik" teknikleri kullanılarak, kurbanın Kredi, Debit/ATM Kart Numaraları, Şifreler ve Parolalar, Hesap Numaraları, İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri gibi büyük önem arz eden ve çok iyi korunması gereken bilgilerini, kurbanı aldatarak elde etme yöntemi* olarak tanımlanabilir. Başka bir ifadeyle Phishing**;** *kişileri, yasal bir şirket, ajans veya organizasyon olduğuna inandırarak, kişisel ve finansal bilgilerini ele geçirme yöntemidir.* İngilizce fishing (balık tutma) kelimesinden türetilen bir kelime olması hasebiyle Phishing kurbanlarına "Phish" (fish–balık) denilmektedir. Balık tutma faaliyeti esnasında, balık tutan kişi balıkları tutabilmek için farklı çeşitlerde oltalar kullanır. Farklı çeşitlerde olan bu oltaları, balıkların çok olduğu ve yakalayabileceğini umduğu yerlere balıkların cinsine göre yerleştirir ve avını beklemeye başlar. Phishing dolandırıcılığında da sistem benzer şekilde işlemektedir. Phishing'in oluşturduğu tehdidin büyüklüğünü anlayabilmek adına verilecek şu örnek çok yararlı olacaktır. Phishing yüzünden ABD'de Mayıs 2004 ila Mayıs 2005 arasında 1.2 milyon bilgisayar kullanıcısı zarara uğramış ve toplam 929 Milyon Dolar kaybetmişlerdir, bu da şirketlere 2 milyar dolara yakın bir zarar teşkil etmiştir. İngiltere'de 2004′de 12.2 Milyon pound olan banka dolandırıcılığı, 2005′de 23.2 milyon pounda çıkmıştır. Phishing dolandırıcıları, özel ve ciddi güvenlik isteyen kişisel veya kurumsal bilgileri çalmak için, bireylerin kullandığı, toplumda belirli bir saygınlık ve güvenilirlik oluşturmuş, popüler ve müşterisi fazla olan hizmet sunucularının taklitleri kullanılmaktadır. Yani gerçek süsü verilmiş sahte mesajlar ile kazanılan güven kötüye kullanılarak kişiler aldatılmaktadır. Taklidi veya sahtesi oluşturulan mesajlar; bankalar, internet üzerinden hizmet sunan, satış yapan firmalardan geliyormuş gibi gösterileceği gibi devlet kurumlarından gönderilmiş mesajlar olarak da sunulabilmektedir. Kişilere ilgili kurum ve kuruluşça, belirli istekler sunulur ve bunun önemi belirtilir, yapılmaması durumunda karşılaşılacak sorunlar ve dezavantajları belirtilir. Örneğin X bankasının internet bankacılığını kullanan bir kullanıcıya, 2014 yılında gerçekleşen bankaya gerçekleşen bir siber saldırı sebebiyle tüm kişisel ve finansal bilgilerinin de güncellenmesi gerektiği bilgisini içeren bir e-mail gönderiliyor. Bu elektronik posta sanki bankadan gelmiş gibi orijinal bir şekilde benzetilmeye çalışılıyor. Elektronik mailde belirtilen bu güncelleştirmenin yapılmaması durumunda ise, hesabın tehlike altında kalacağı gibi

olumsuzluklar ve dezavantajlar ile karşılaşılabileceği söyleniyor. Bu blöf sayesinde müşteri kandırılmış oluyor. Kişi özel ve güvenlik gerektiren bilgilerini yazılan sahte siteye girdiğinde ise artık tüm kontroller tuzağı kuran kişiye geçiyor. Bununla birlikte, hesaba girilebilmesi için cep telefonuna gönderilen tek kullanımlık şifre ise ***"Zeus ve Zitmo"*** adı verilen yöntemler ile ele geçiriliyor. Aynı şekilde hesap sahibinin sisteme cep telefon numarasını yazması üzerinde, cep telefonuna gönderilen linki tıklayarak, güvenlik sebebi ile zorunlu olduğunu zannettiği programı yüklemesi ile birlikte, gerçekten bankadan gelen tek kullanımlık şifre, hesap sahibinin cep telefonuna gelmekte ancak ekranda gözükmeyerek, bilişim korsanlarının yazılım programı ile yönlendirdiği cep telefona otomatik olarak gönderilmektedir[47].

§ V. Dijital delil

A- Dijital delil nedir

Ceza yargılamasında delil kavramının önemi büyüktür. Zira maddi gerçeğe ulaşılabilmesi için usule uygun elde edilmiş deliller gerekmektedir. Bir başka ifade ile Ceza muhakemesi açısından bir suç soruşturmasına delilin elde ediliş biçimi dahi önemlidir. Delil ceza davasında, maddi gerçeği doğrudan veya dolaylı olarak açıklayan ispat aracıdır[48]. Delile doktrinde, kanıt veya ispat vasıtası da denmektedir[49]. Ceza yargılamasında somut gerçeğin ortaya çıkması için delil türleri sınırlandırılmamaktadır. Bir başka ifade ile delil serbestliği ilkesi benimsenmektedir. Bu ilke hem delillerin serbest değerlendirilmesi hem de vicdani delil sistemini oluşturmaktadır[50].

Bilişim teknolojilerinin gün geçtikçe yaşamımızın her alanına girmesi üzerine, ortaya yeni kavramların çıkmasına sebep olmuştur. Bu kavramlar içerisinde dijital delil, elektronik delil, sayısal delil olarak nitelendirilen yeni bir delil türü ile karşılaşılmıştır. Dijital delil kavramı çok farklı şekillerde tanımlanmıştır. Dijital delil; bilişim sistemleri ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delillerdir[51]. Bu bağlamda olay yerinden elde

---

[47] http://www.chip.com.tr/haber/internet-bankaciliginda-zeus-virusu-panigi_39240.html (Erişim: 17.09.2014)

[48] CENTEL Nur – ZAFER Hamide; Ceza Muhakemesi Hukuku; Yenilenmiş ve Gözden Geçirilmiş 5. Bası Beta Yayınları 2008 s 211.

[49] CENTEL Nur - ZAFER Hamide, Ceza Muhakemesi Hukuku, s 211.

[50] ÖZTÜRK Bahri – ERDEM Mustafa Ruhan, Uygulamalı Ceza Muhakemesi Hukuku, 9. Bası, Ankara 2006 s 388.

[51] HENKOĞLU Türkay, Adli Bilişim Dijital Delillerin Analizi, 1. Bası Pusula Yayınları, İstanbul 2011 s 5.

edilen bilgisayar donanımları ile bu bilgisayar donanımının içindeki veriyi de ifade etmektedir[52]. Bir başka tanıma göre; elektronik bir cihaz üzerinde saklanabilen veya bu cihazlar aracılığıyla iletilebilen muhakeme bakımından değeri olan bilgi veya veriler şeklinde tanımlanmıştır[53].

Herhangi bir fiziki bilgi veya veri de aynı şekilde dijital ortamda yer alabilir. Söz konusu verilerin ceza muhakemesinde delil olma niteliğine sahip olması halinde ise somut olayı çözecek olması ve gerçek olması hallerinde dijital delil olacaktır. Bununla birlikte bir verinin delil olabilmesi için sahip olması gereken ortak özellikler vardır[54].

B- Dijital delil nerede bulunur

Dijital delil diğer delil türlerine göre bir hayli farklıdır. Öncelikle fiziki olarak gözükmezler[55]. Anlam ifade edebilmesi için ise söz konusu veriye uygun donanımların bulunması gerekmektedir. Dijital deliller; bilgisayar veri depolama donanımlarında(sabit disk, flash bellek, optik disk, manyetik teyp, floppy disk, zip/jazz disk), faks ve fotokopi makinaları, modemler, router, cep telefonları, gprs aygıtları, akıllı kartlar, silinmiş dosya, tahsis edilmemiş ve tahsisli kullanılmamış alanlardan kurtarılan veriler, geri dönüşüm kutusundan kurtarılan veriler, link dosyaları, tarayıcı makinalar, registry kayıtları, e-posta kayıtları, uzak sunucu bilgisayara erişim kayıtları ve sohbet programları, sosyal ağ hesapları, internet tarayıcı geçmişi, erişim sağlayıcı kayıtları, kablosuz internet bağlantı noktaları, ağ veri depolama ve internet bağlantı kayıtları, işletim sistemine ait kayıtlar, dijital fotoğraf ve videolar, CD-DVD kayıt bilgileri, veri dosyaları elektronik imza, yedekleme sunucuları ve benzeri yerlerde yer almaktadır[56].

Dijital delillerin bulunduğu ortamlar, haliyle teknolojinin gelişmesine bağlı olarak farklılık gösterecektir. Nitekim yeni teknolojik gelişmeler karşısında, insanların ihtiyaçları değişerek, farklı donanımlar ile ileride henüz öngöremediğimiz farklı dijital deliller ortaya çıkacaktır. Örneğin önceleri sabit disklerde yer alan veriler artık sabit disklerde değil sanal

---

[52] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, Adli Bilişim ve Elektronik Deliller 1. Bası Seçkin Yayınları, Ankara 2014, s 145

[53] ÖZOCAK Gürkan, Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması, İzmir 2. Uluslararası Bilişim Hukuku Kurultayı 17-19 Kasım 2011, Bildiriler Kitabı (Editörler: MEMİŞ Tekin, KOLTUKSUZ Ahmet, AKKAN Mine) s 114.

[54] DEĞİRMENCİ Olgun, Ceza Muhakemesinde Sayısal (Dijital) Delil 1. Bası Seçkin Yayınları Ankara 2014 s 127.

[55] DEĞİRMENCİ Olgun, 2014 s 132.

[56] HENKOĞLU Türkay, 2011 s 6.

sunuculardа saklanmaktadır. Doktrinde bulut bilişim olarak adlandırılan bu husus gün geçtikçe farklı niteliklerde gelişeceği şüphesizdir[57].

C- Dijital delil kapsamı ve özellikleri

Dijital delillerin maddi gerçeğe ulaşma aşamasında delil vasfında sayılabilmesi ve adli makamlara sunulabilmesi için teknik açıdan birçok unsuru bünyesinde barındırması gerekmektedir. Bu unsurları Akla uygunluk, kabul edilebilirlik, gerçeklik, eksiksiz olması, güvenilirlik, manipülasyona uğramamış olması ve tekrar edilebilirlik üst başlıklarında toparlayabiliriz[58].

Dijital deliller yapısı itibarı ile hassas niteliktedir. Bir başka ifade ile kasıtlı veya kasıtsız hareketlerle bozulabilme niteliğine sahiptir[59]. Dijital delillerin en önemli özelliklerinden biri ise kolay bir şekilde yok edilememesidir. Daha doğru bir ifade ile çeşitli teknik yöntemler ile silinmiş veriler geri getirilebilir. Bunların yanı sıra; dijital deliller kolaylıkla kopyalanabilir ve çoğaltılabilir, manyetik alan, sıcaklık ne gibi sebeplerle bozulabilirler, üzerinde işlem yapılmak suretiyle kolayca değiştirebilirler, tekrar geri getirilemeyecek şekilde silinebilir, şifrelenmiş, gizlenmiş başkaca veriler üzerinde barındırılabilirler[60].

D- İmaj alma ve yöntemleri

Dijital deliller niteliği gereğince hassas olması sebebi ile analiz işlemleri de örnek üzerinde yapılmalıdır. Söz konusu örnek tüm diskin komple yedeklenmesi şeklinde olmalıdır. Disk üzerinde, bit bazında, örnek alma ile silinen, zarar gören, değiştirilen ve gizlenen tüm dosyalar elde edilebilir. Aynı zamanda verinin orijinalliği doğrulanabilir. İmaj alma olarak tabir edilen bu yöntemle diskin tümünün bire bir kopyası alınarak teknik açıdan adli bilişim standartlarına uygun bir yöntemle çalışılmalıdır[61].

[57] DEĞİRMENCİ Olgun, 2014 s 141.

[58] HENKOĞLU Türkay, 2011 s 7.

[59] TANRIKULU Cengiz, 2014 s 53.

[60] ÇAKIR Hüseyin Çakır - KILIÇ Mehmet Serkan, 2014 s 146.

[61] ÇAKIR Hüseyin Çakır - KILIÇ Mehmet Serkan, 2014 s 172.

E) Hash değeri ve önemi

Hash değeri (dijital mühürleme) uygulamada çok tartışılan ve sorun yaşanan bir hususdur. Tartışılmasının nedeni, tezimizin ilerleyen bölümlerinde açıklanacağı üzere Türk Ceza Muhakemesi Hukukunda uygulanmasına ilişkin bir kanun maddesi bulunmamaktadır. Ancak Yargıtay içtihatlarında özellikle dijital delillerin bütünlüğüne ve güvenirliğine sıkça vurgu yapılmakta ve deliller toplanırken tartışmaya mahal vermeyecek güvenirlikte saklanması gerektiği belirtilmektedir.

Elektronik deliliğin bütünlüğü ve güvenirliği, yedeğinin alınmasından mahkemeye gidene kadar geçirdiği aşamada sonuna kadar değişmediğinin doğrulanması demektir. Adli bilişim incelemelerinde uygulanan yöntemin delili değiştirmediğini ispatlaması için *"bütünlük algoritması"* kullanılır. Dijital delilin elde edilmesi sırasında oluşturulan hash algoritması fiziksel delil ile bağlantılı olarak, delilin temelini ve bütünlüğünün idamesini meydana getirir[62].

Hash Algoritması için bir dijital belgenin DNA'sı şeklinde benzetme yapılmaktadır[63]. Hash değeri alınırken oluşan belli bir uzunluktaki şifreli özet tek yönlü olması sebebi ile eski haline çevrilmesi mümkün değildir. Bir başka ifade ile hash değeri alınmış bir belgeyi açarak tek bir nokta eklenmesi sonrasında tekrar hash değeri alınmasında aynı sonuç çıkmayacaktır. Çünkü parmak izinde olduğu gibi, hash algoritması da ait olduğu dosya ya da diske özel ve tektir. Hash algoritması standardı olarak birçok seçenek olmasına karşın, en çok kabul gören iki standart 128 bit MD5 (Message-Digest algorithm 5) ve 160 bit SHA-1 (Secure Hash Algorithm)'dir[64].

(İkinci Bölüm)

TÜRK HUKUKUNDA BİLİŞİM SUÇLARI

§ I. Genel olarak

Ülkemizde bilişim suçları, 1990'lı yılların başlarından itibaren kanunlarımızda düzenlenmelere konu olmuştur. 765 sayılı Türk Ceza Kanunu'na, 06.06.1991 tarihli ve 3756 sayılı Kanun ile *"Bilişim Alanında Suçlar*" adıyla 525/a, 525/b, 525/c ve 525/d maddelerinin eklenmesiyle yasal boyut kazanmıştır. Bilişim suçlarıyla ilgili bu değişiklik 1989 Türk Ceza

[62] ÇAKIR Hüseyin Çakır - KILIÇ Mehmet Serkan, 2014 s 176.

[63] HENKOĞLU Türkay, 2011 s 54.

[64] HENKOĞLU Türkay, 2011 s 55.

Kanunu Tasarısındaki düzenlemelerle yapılmıştır. 1989 Türk Ceza Kanunu Tasarısındaki düzenlemeler ise Fransız Ceza Kanunun 'dan alınmıştır[65].

1990 Yıllarda 765 sayılı TCK'daki değişiklikle yer alan suç tipleri; "verilerin ele geçirilmesi suçu (525a/1), başkasına zarar vermek için verilerin kullanılması, nakledilmesi veya çoğaltılması suçu (525a/2), verilere veya veri işleme zarar verilmesi suçu (525b/1), Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlanması suçu (525b/2) ve verilerde sahtekârlık yapılması suçlarıdır (525c)." O tarihlerde daha internet ve bilgisayar kullanımı yaygınlaşmadığından ilk etapta bu maddeler gerek uygulamada gerekse doktrinde tam olarak algılanamamıştır. Fakat 1995 yılından sonra hızla yükselen internet ve bilgisayar kullanımı, kanunlarımızda da zorunlu olarak değişikliklere gidilmesine sebep olmuştur. Zira bu süreç zarfında gerek Ceza kanunumuzda gerekse birtakım özel kanunlarda bilişim suçları ile ilgili birçok değişiklik yapılmıştır.

§ II. 5237 Sayılı Türk Ceza Kanunu'ndaki bilişim suçları

A- Genel olarak

5237 Sayılı Türk Ceza Kanunu 29.04.2004 tarihinde kabul edilmiş ve 01.06.2005 tarihinde de yürürlüğü girmiştir. 5237 sayılı yasada bilişim suçları onuncu bölümde "Bilişim Alanında Suçlar" başlığı altında, Kanunun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında yer almaktadır.

Bilişim alanında suçlar bölümünde; hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu (m. 243), bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m. 244/1–2), bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m. 244/4), banka veya kredi kartlarının kötüye kullanılması suçu (m. 245) yer almaktadır.

B- 5237 Sayılı TCK'da "Bilişim alanında suçlar" bölümünde düzenlenen suç tipleri

1. 5237 sayılı TCK'nın 243. maddesi "hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu"

[65] DÖNMEZER Sulhi, " Sempozyumun Genel Değerlendirilmesi" Uluslar arası İnternet Hukuku Sempozyumu, 21-22 Mayıs 2001, İzmir, 2002, s 552.

“Bilişim sistemine girme” kenar başlıklı TCK 243. Maddesi şöyledir;

“(1) 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.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.”

Görüldüğü üzere 243/1. Maddede, bir bilişim sistemine hukuka aykırı olarak erişim başlı başına yeterli görülmemiş ve orada kalmaya devam etme fiiliyle suç gerçekleşmektedir.

Hukuka aykırı olarak bilişim sistemlerine girme ve sistemde kalma suçunda korunan hukuksal değer, bilişim sistemlerinin güvenliği, özel hayatın gizliliği ve sırrın masumiyeti olarak belirtilebilir. Bir bilişim sistemine hukuka aykırı bir şekilde girilmesi ve orada kalmaya devam edilmesi bir kişinin veya bir kuruluşun çıkarlarına, menfaatlerine zarar vermekte bu da o kişi veya kurumun verilerinin gizliliği, özel hayatın dokunulmazlığı gibi hukuksal değerlerini ihlal edilebilmektedir. Tüm bunlarda o sistemin güvenliğini etkilemektedir[66].

243. Maddedeki *“Girme”* kelimesinin kullanımı, bilişim sistemlerine özgü bir kelime değildir. Burada hedeflenen aslında *“erişim”* kelimesidir. Özellikle, suç işleyen bakımından fiil, sisteme yetkisiz “erişim” ile gerçekleştirilmektedir[67].

Bir başka tartışma konusu ise madde metni suçun oluşması için orada kalmaya devam eyleminin de gerçekleşmesini şart koşmuştur. Fakat sisteme hukuka aykırı girildikten sonra, ne kadar süre ile sistemde kalınması sonucu suçun tamamlanacağı, madde metni ve gerekçesinde somut olarak tespit edilmemiştir.

Zira her suç için geçerli bir kalmaya devam etme süresi belirlemek sıhhatli bir yaklaşım olmayacaktır. Çünkü suça konu her bilişim sisteminin özelliği ve güvenlik yapısı aynı değildir. Bu durum bazen birkaç saniye bazen birkaç saat olarak ifade edilebilir. Bir başka deyişle somut olayın şartlarına göre bir değerlendirme yapılması gerekmektedir.

---

[66] DÜLGER M. Volkan; “Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi” , İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını (İstanbul, 2004), s 214.

[67] KARAGÜLMEZ Ali, 2009 s 169.

Hukuka aykırı olarak bilişim sistemlerine girme ve sistemde kalma suçu düzenlenirken suçu işleyecek kişi açısından herhangi bir özellik belirtilmemiş ve "kimse" sözcüğü kullanılmıştır. O halde bu suçu herkes işleyebilmektedir. Failin bu suçu işlerken hangi amaçla hareket ettiğinin bir önemi yoktur[68]. İşlenen suç dolayısıyla özel hukuk tüzel kişileri hakkında, tedbir niteliğinde yaptırımlara hükmedilecektir. Bu yönde, 5237 sayılı TCK 246. maddesinde; bilişim alanında suçlar bölümünde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlayan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir.

Bu suç tipinde yetkisiz erişim ve orada kalmaya devam etme unsuru arandığından burada temadi niteliğinde bir suç söz konusudur.

Bu suç tipinde, teşebbüsten bahsedebilmek için, hukuka aykırı erişimden sonra, sistemde kalmaya başlanmış ve fakat henüz suçun tamamlanmasını sağlayacak kadar süre geçirilmemiş olması gerekmektedir. Sonuç olarak, şayet bilişim sistemine girdikten sonra, orada kalmayı başaramamak, anlık olmuşsa (kanunun aradığı makul süre olmamışsa), yine suça teşebbüsten bahsetmek güçtür. Fakat sistemde kalmaya başlandıktan sonra, sistemde kalma başarılamamışsa bu takdirde suça teşebbüs ihtimali gündeme gelebilecektir.

Bilişim sistemlerine girme ve sistemde kalma suçu genel kastla işlenebilmektedir. Fakat 5237 sayılı TCK'nın 243. maddesinin üçüncü fıkrasında, fail tarafından fiillerin gerçekleştirilmesi sırasında sistemin içerdiği verilerin taksirle yok edilmesi veya değiştirilmesi hali düzenlenmiştir. Bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekmektedir.

243. maddenin 2. fıkrasında ise konun koyucu bir hafifletici neden öngörmüştür. Buna göre verilecek cezanın yarı oranında azaltılacağını belirtmiştir. Fakat bu madde metni değerlendirildiğinde, kanun koyucunun maksadının, hafifletici nedenin gerekçesinin ne olduğu kafalarda soru işareti olarak kalmıştır. Çünkü 1. fıkradaki suçun bedeli karşılığı yararlanılan bir site olması halinde cezanın yarı oranda azaltılacağı belirtilmektedir. Örneğin; ücretli olarak kullandığınız bir e-posta hesabınızın olduğunu varsayalım, şayet bu e-posta hesabınıza hukuka aykırı olarak girilir ve orda kalmaya devam edilirse birinci fıkrada

[68] DÜLGER M. Volkan, 2004 s 218.

tanımlanan suç oluşacaktır. Fakat bedeli karşılığında yararlandığınız bir sistem olmasından ötürü fail, yarı oranında cezalandırılacaktır. Ancak bedava alınan bir e-posta hesabında aynı durum gerçekleşmesinde, faile ceza indirimi uygulanmayacaktır. Bedeli karşılığında yararlanılan sistemler denilirken sadece bedel para olarak anlaşılmamalı bir hizmet karşılığı yararlanılıyor olması da bedel olarak sayılmalıdır. Fakat maddenin bu bendi kanımca hafifletici neden olarak düzenlenememeli aksine ağırlaştırıcı neden olarak düzenlenmelidir. Çünkü; bu suçun mağduru bir bilişim sisteminden belirli bir bedel ödeyerek yararlanmaktadır. Bir başka deyişle; mağdur o sistemin herhangi bir özelliğine güvenmiş, beğenmiş ve bunun karşılığı ödeyerek o sistemi satın almıştır. Fakat; benzer bir sistemi bedava kullanan ile bedeli karşılığında kullanana aynı suçun işlenmesi durumuna yaptırımı, mantık ilkelerine ters bir şekilde bedel ödeyerek sistemi kullanan mağdurun aleyhe yönündedir.

243. Maddenin 3. fıkrasında, *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."* hükme yer almaktadır.

Maddenin gerekçesinde ise;

"Üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaştırılmış hali düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değiştirilmesi halinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır."

denilmektedir.

Buna göre fıkrada suçun neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Fakat bu fıkranın uygulanabilmesi için failin verileri yok etme kastıyla hareket etmemesi, taksirle verileri yok etmesi gerekmektedir.

2. 5237 sayılı TCK'nın 244 maddesi "Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu"

Sistemi engelleme, bozma, verileri yok etme veya değiştirme kenar başlıklı TCK madde 244. maddesi şöyledir;

"*(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

Madde gerekçesinde 1 numaralı fıkrasıyla ilgili olarak, *" Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir. Aracın fizik varlığı ve işlenmesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir."* denilmiştir.

Madde gerekçesinde birinci fıkradan söz edildiği halde, getirilen açıklama 244. maddedeki 1 ve 2 numaralı fıkraları kapsamaktadır. TBMM Adalet komisyonu tarafından kabul edilen tasarı metninde 244. maddenin 1 ve 2 numaralı fıkralı, *"(1) Bir bilişim siteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir"* şeklindeydi ve TBMM Genel kurulunda bu fıkra 1 ve 2 numaralı fıkra olarak iki parçaya bölünmüştür[69]. Fakat bu durum iki fıkranın içeriği incelendiğinde, ikiye ayırarak farklı cezai yaptırımlar öngörmenin ve çok isabetli olmadığı kanısındayım.

Ayrıca 244. maddenin 1. fıkrasında yer alan suç tipine 5237 sayılı TCK'da yer vermekle, Avrupa Siber Suç Sözleşmesinin 5. maddesinde öngörülen "sisteme etki" ve 244. maddenin 2. fıkrasında yer alan suç tipine 5237 sayılı TCK'da yer vermekle de Avrupa Siber

[69] KARAGÜLMEZ Ali, 2009 age s 185.

Suç Sözleşmesinin 4. maddesinde öngörülen "verileri etkileme" düzenlemelerine paralellik sağlanmaya çalışılmıştır[70].

244. maddenin 1. Fıkrasında, doğrudan bir bilişim sisteminin çalışmasına yönelik fiiller engellenmek istenmektedir. Bir görüşe göre ise, bu fıkrada "daha önce düzenlenmemiş olan sabotaj fiili düzenlenmektedir. Bununla bir bilişim sisteminin işleyişinin engellenmesi veya bozulması müeyyide altına alınmaktadır"[71].

244. maddenin 1. ve 2. fıkrasına ilişkin korunan hukuki yararı konusunda doktrinde farklı görüşler mevcuttur. Buna göre, korunan hukuki yarar, karma nitelikte olduğu yönündedir[72]. Bir diğer görüş; 244. maddede bilişim sisteminin ve bu sistem içerisindeki verilerin dokunulmazlığı korunan hukuki yarardır. Suçun konusu ise bilişim sisteminin soyut ve somut bileşenleri ile sistem içinde yer alan verilerdir. 1 numaralı fıkrada, bilişim sistemi sahibinin mülkiyet hakkı, zilyedinin ise bilişim sisteminin dokunulmazlığı, iletişim kurma, teknolojik gelişim özgürlüğü de korunmaktadır. 2 numaralı fıkrada ise bazen mülkiyet hakkı, bazen de verilerin içeriğine göre, fikri mülkiyet hakkı, özel hayatın gizliliği, ticari sırlar da korunmaktadır[73]. Bir diğer görüşe göre, 244. madde kapsamındaki bir suç, kimi zaman zimmete yada hırsızlığa veya dolandırıcılığa ya da güveni kötüye kullanmaya, suçuna çok benzeyebilir. Bu suçlardan, hırsızlığın mal üzerinde işlenmesi zorunlu iken, verinin mal olmaması; aynı şekilde dolandırıcılıkta da hile ve desise ile mağdurun kandırılması gerekirken, bilişim sistemlerinin ise kandırılmasının söz konusu olmaması sebebiyle klasik hırsızlık ve dolandırıcılık suçları hiçbir zaman gerçekleşmeyecektir[74].

244. maddenin 1. fıkrasında seçimlik bir hareket söz konusudur. Buna göre; bilişim sisteminin işleyişini "engelleme" veya "bozma" hareketlerinde birinin gerçekleşmesi gerekmektedir. Aynı zamanda bu suç taksirle değil, kasıtla işlenmesi gerekmektedir. Bir bilişim sisteminin işleyişinin engellemesi, sistemin geçici veya sürekli olarak çalışmasının

[70] DEĞİRMENCİ Olgun; Bilişim Suçları, 2002 age s 129.

[71] YAZICIOĞLU Yılmaz; Bilgisayar ağların ile ilgili suçlar konusunda Türk Ceza Konunu 2000 Tasarısı, Uluslararası İnternet ve Hukuku Sempozyumu, 21-22 Mayıs 2001, DEÜ. Yayını, İzmir, 2002, s 468.

[72] DÜLGER Volkan Murat, 2004 s 231.

[73] KURT Levent; Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, TODAİE Kamu Yönetimi Bölümü, (Yayınlanmamış Yüksek Lisans Tezi) Ankara 2005 s 185.

[74] YAZICIOĞLU R. Yılmaz, 1997 s 144.

kesintiye uğratılmasıdır. Burada, sistemin genel olarak yapısı bozulmamakta fakat işleyişi herhangi bir şekilde engellenmektedir[75].

Avrupa Konseyi Siber suç sözleşmesinin *"sistemin bütünlüğü ihlali" başlıklı 5. Maddesinde, "Her taraf, iç hukukuna uygun olarak, bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle bir bilişim sisteminin işletilmesine kasten ve haksız olarak engel olunmasını suç haline getirmek için gerekli görülen koruma tedbirleri ve diğer tedbirleri kabul eder."* denilmektedir. Nitekim sözleşmenin 5. Maddesinde çok net bir biçimde görüldüğü üzere, buradaki seçimlik hareketler, sonuçta sistemin işleyişini engellemektedir[76].

Madde fıkrasında yer alan sistemin işleyişini bozma eylemi ise şu şekilde açıklanabilir. Buna göre; yetkisiz bir müdahale ile sistemin sıhhatli bir şekilde işleyişini geçici veya sürekli ortadan kaldırılmasıdır. Bu hareket direk olarak sisteme olabileceği gibi, sistemin işleyişine etki eden veya katkısı olan herhangi bir unsurun tahrip edilmesiyle de olabilir. Sonuç olarak; sistemin işleyişinin kısmen veya tamamen bozulmuş olması yeterlidir.

244. maddenin 2. fıkrasında ise, aslında birinci fıkradan biraz daha ayrıntılı olarak düzenlenmiştir. Bunun nedeni ise; 244. maddenin 1 ve 2 numaralı fıkraları tek fıkra iken TBMM Genel Kurulunda kabul edilen önergeyle iki fıkra haline getirilmiştir. Bunun gerekçesi ise *"suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiilin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür."* denilmiştir[77].

Buna göre 1. fıkrada daha ağır bir yaptırım öngörülmüş çünkü doğrudan bir bilişim sisteminin işleyişinin engellenmesi ve bozulmasından bahsetmektedir. Fakat ikinci fıkrada sistemdeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişiye altı aydan üç yıla kadar hapis cezası öngörülmüştür.

244. maddenin 1. ve 2. fıkralarında ki suçun manevi unsuru genel suç işleme kastıdır. Fail burada suç işleme kastıyla hareket etmesi gerekmektedir. Bu suçlar, taksirle işlenemez.

---

[75] KARAGÜLMEZ Ali, 2009 s 187.

[76] AKSOY Eylem; Avrupa Konseyi Siber Suçluluk Sözleşmesi, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi Sayı 1, İstanbul 2002 s 872.

[77] YILMAZ Zekeriya; Gerekçe ve Tutanaklarla Yeni Türk Ceza Kanunu, Seçkin Yayınevi Ankara 2004 s 330.

Böylece 243. maddenin 3. fıkrası ile 244. maddenin 1 ve 2 numaralı fıkralarının uygulanmasında, faildeki manevi unsur belirleyici olmaktadır. Bir başka deyişle; 243. maddenin 3 numaralı fıkrasının uygulanabilmesi için öncelikle 244. maddenin 1 ve 2 numaralı fıkralarının uygulanmasında, faildeki manevi unsur belirleyici olmaktadır. Bu durumda 243/3. maddenin uygulanabilmesi için, öncelikle failin 244. maddenin 1 ve 2. numaralı fıkraları kapsamında bir kastının olmaması gerekmektedir. Ayrıca failin eylemine ilişkin kastının hukuka aykırı olarak sisteme girip orada kalmaya devam etme şeklinde olması gerekmektedir. Son olarak da failin bu kast ile işlediği fiilinin sonucunda sisteminin içerdiği verilerin yok olması veya değişmiş olması koşullarının gerçekleşmesi gerekmektedir[78].

244. maddenin 3. fıkrasındaki "bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında " hükmüyle, 1 ve 2. fıkranın suça tesir eden ağırlaştırıcı nedeni düzenlenmiştir. Bu hüküm, hükümet taslağında yer almasa da, TBMM adalet komisyonu çalışmalarında eklenmiştir.

244. maddenin 4 numaralı fıkrasında *"Yukarıda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur"* kuralıyla 1 ve 2 numaralı fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, cezai yaptırımı altına alınmıştır.

Madde gerekçesinde, "bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunun oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilecektir" denilmekle 4 numaralı fıkra ile çelişmektedir[79]. Burada *"başka bir oluşturmaması"* ibaresi *"daha ağır başka bir suç oluşturmaması"* şeklinde gerekçeye uygun olarak düzeltilmesi gerekmektedir.

Yaptırım olarak; 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

[78] KARAGÜLMEZ Ali, 2009 age s 190.

[79] KARAGÜLMEZ Ali, 2009 s 190.

sağlamaktadır. Bu sebeple madde metnine göre hapis cezası ile birlikte adli para cezasına da hükmedilecektir. 5237 sayılı TCK'nın 246. maddesinde bu suçun işlenmesinden dolayı tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara 5237 sayılı TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.

3. 5237 sayılı TCK'nın 245 maddesi "Banka veya kredi kartlarının kötüye kullanılması suçu"

Banka veya kredi kartlarının kötüye kullanılması kenar başlıklı TCK 245. Maddesi Şöyledir;

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz." denilmektedir.

29.06.2005 tarihli, 5377 sayılı "Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanun"un 27. maddesi ile "banka veya kredi kartlarının kötüye kullanılması"nı düzenleyen

5237 sayılı TCK'nın 245. maddesinde değişiklik yapılmıştır. Bu durumda, 5237 sayılı TCK'nın 245. maddesi ile başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme gibi eylemlerle, banka ve kredi kartlarının haksız, hukuka aykırı olarak kullanılması yoluyla bankaların ve kart sahiplerinin zarara sokulması ve bu suretle hukuka aykırı yarar sağlanması önlemek istenmiştir[80]. Maddenin gerekçesinde de "madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi kartları sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır" denilmiştir[81].

245. Maddedeki, aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının işlenme şekillerinin tümünü de içeren fiiller, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirilmiştir[82].

Bir görüşe göre ise, 245. Maddedeki suç, bir bilişim sistemi olmaksızın işlenemeyeceği için, bir bilişim suçudur. Korunan hukuki yarar, mağdurun malvarlığının korunmasıdır[83].

245. maddenin 1 numaralı fıkrasında ayrıntılı düzenlemede, 765 sayılı eski TCK'nin uygulandığı dönemdeki tartışmaların ve uygulamada özellikle Yargıtay'ın verdiği kararların etkisi olduğu açıktır. O dönemde konu, 765 sayılı TCK'nin 525b/2 maddesindeki suç ile hırsızlık ya da dolandırıcılık gibi suçlar arasında farklı içtihatlara neden olmuştur[84].

Zira, kanun metnindeki *"Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse"* şeklindeki yoruma açık kanun lafzı Yargıtay tarafından farklı içtihatlar oluşmasına sebep olmuştur. Fakat bir ceza normunun bu kadar geniş tutulması uygulamada şüphesiz sorunlara sebep olacaktır. Burada "her ne suretle olursa olsun ele geçirme" tanımlaması aslında suçun bilişim sistemlerinin her geçen gün yenilenen teknolojisinin önüne geçmek için konulduğu kanısındayım. Fakat bu tanım yüzünden bilişim suçu ile ilgisi olmayan birtakım fiiller, Yargıtay tarafından 245/1.

[80] DEĞİRMENCİ Olgun, Bilişim Suçları, 2002 s. 158.

[81] ÖZGENÇ İzzet; Türk Ceza Hukuku Genel Hükümler, 2. Bası Seçkin Yayınları Ankara, 2007 s 1005.

[82] www.tbmm.gov.tr Tck 245. Maddenin gerekçesinden (Erişim 11.09.2009).

[83] KURT Levent, 2005 s 205.

[84] KARAGÜLMEZ Ali, 2009 s 206.

Maddesine girmesine sebep olmuştur. Örneğin; Gasp ederek elde ettiği kredi kartıyla ATM'den para çekme failin hareketi, Yargıtay tarafından bilişim suçu olarak algılanmıştır[85].

Maddenin 2. fıkrasında düzenlenen "başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme" eyleminin gerçekleştirilmesi halinde ise faile üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası verilecektir.

Bu suçun getirilme amacı TBMM Adalet komisyonu raporunda, "Başkalarına ait banka hesaplarıyla ilişkilendirilerek üretilen sahte banka veya kredi kartlarının ticari amaçlı olarak piyasaya sürülmesi karşısında, bu fiilleri yaptırıma bağlamak amacıyla maddeye yeni ikinci fıkra eklenmiştir" şeklide belirtilmiştir.

Bu suçun manevi unsuru, başkasına ait banka hesabıyla ilişkilendirerek banka veya kredi kartı üretmek kastı gerekli ve yeterlidir.

Maddenin 3. fıkrasında ise sahte oluşturulan veya sahtecilik yapılan banka veya kredi kartından haksız yarar sağlanması ayrı bir suç sayılmıştır.

Madde gerekçesinde, "birinci fıkrada belirtilen fiillerin, oluşturulmuş sahte bir banka veya kredi kartını kullanmak suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektirmektedir. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir" denilmektedir.

Bir görüşe göre ise; maddede bu ibarenin yer almasının, TCK 44. Madde hükmü karşısında sonuca bir etkisi yoktur. Böyle bir ibare yer almasa bile, şayet fiil daha ağır cezayı gerektiren bir suç oluşturmakta ise 44. Madde gereğinde, 245/3 'ün değil, daha ağır cezayı gerektiren ilgili maddenin uygulanması gerekmektedir[86].

245/3. Maddende suçun neticesi, failin sahte oluşturulan veya üzerinde sahtecilik yapılan bir kart kullanarak haksız bir yarar elde etmiş olmasıdır.

Maddenin 4. fıkrasına göre birinci fıkrada yer alan suçun cezasızlık sebepleri öngörülmüştür. Buna göre; a) Haklarında aykırılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya

[85] Yargıtay 6.CD. 05.02.2002, 16231E, 1149K; www.kazanci.com (Erişim 11.09.2014).

[86] KARAGÜLMEZ Ali, 2009 age s 220.

evlatlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.

C- TCK'da yer alan bilişimle ilgili diğer suçlar

1. TCK'nın 135. maddesi "Kişisel verilerin kaydedilmesi suçu"

5237 sayılı TCK'nın 135. maddesinin 1. fıkrasında, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi suç haline getirilmiştir. 2. fıkrasında ise, kişilerin siyasal, felsefi ve dinsel görüşlerinin, ırksal kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak yerleştirilmesi eylemleri suç tipi olarak düzenlenmiştir[87].

Madde gerekçesinde *"Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedir. Bu bakımdan, kişilerle ilgili bireylerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır..."*

Bu suçun konusu madde gerekçesinde; Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak tanımlanmıştır. Fakat kişisel verinin, ne olduğu konusunda açıklayıcı bir ifade yer almamaktadır. Kişisel verilerin korunmasına ilişkin kanun tasarısı halen meclistedir. Uygulamada her ne kadar Emniyet teşkilatının, kişisel verileri hukuka aykırı olarak kayıt altına aldığına dair yaygın bir kanı varsa da aslında Türkiye'de birçok Özel ve Tüzel kişiler, şirketler kişisel verileri hukuka aykırı kaydedip bunları kullanmaktadırlar. Özellikle, daha kolay ve erişilebilir olduğundan, daha çok internet kullanıcılarının kişisel verilerinin kayıt altına alındığı bilinmektedir. Bunun için de kişisel verilerin korunması kanun tasarısı mutlaka çıkartılmalıdır. Bu kanunun yasalaşması Avrupa Birliği standartlarının yakalanması için de şarttır. AİHS ve AİHM uygulamalarında kişisel veriler;

* Cinsiyet, medeni hal, doğum yeri, diğer kişisel bilgiler ile ilgili bilgileri içeren uygulamalar (Nüfus sayımı).

[87] DEĞİRMENCİ Olgun, Bilişim Suçları, 2002 age s 156-157.

* Polis kayıtları gizli olsa bile polis tarafından parmak izi, fotoğraf ve diğer kişisel bilgilerin kaydedilmesi,

* Tıbbi verilerin toplanması ve tıbbi kayıtların tutulması,

* Vergi makamlarının kişisel harcamaların detaylarını (ve böylece özel hayatın detaylarını) açıklama zorunluluğu getirmesi,

* Sağlık, sosyal hizmetler ve vergi gibi idari ve sivil konuları ele alan bireysel kimlik belirleme sistemi kişisel veriler kapsamında değerlendirilmiştir.

Kişisel veri; belirli veya kimliği belirlenebilir kişiye ilişkin tüm verileri kapsar.

Yargıtay ise bir kararında; "*kişinin yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak sınırlı bir çevre ile paylaştığı nüfus bilgileri(T.C kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi) adli sicil kaydı, yerleşim yeri, parmak izi, DNS'sı, etnik kökeni, siyasi, felsefi, dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir; ancak herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler, yasal anlamda "kişisel veri" olarak değerlendirilmez, aksinin kabulü; anılan maddelerin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsiz ve hemen her eylemin suç oluşturması gibi olumsuz sonuçlar doğurur"*[88]. Şeklinde görüşü bulunmaktadır.

Hukuka aykırı olarak kişisel verilerin kaydedilmesinde maddi unsur kaydetmek verilerin işlenmesi anlamına geleceği için kişisel verilerin kaydedilmesinde öngörülen kıstaslar ayrımcılık esası getirilmeyerek yapılması gerekir. Nitekim TCK md.135/2'de kişilerin siyasi, felsefi, dini görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendika bağlantılarına ilişkin kişisel bilgileri veri olarak kaydeden kişinin cezalandırılacağı öngörülmüştür. Burada dikkat edilirse kişisel verilerin siyasi, felsefi veya dini görüşlerine, irkî kökenlerine göre kayıt yapılması her halükarda suçtur. Oysa diğer verilerin kayıt işlemi kişisel verilerin korunması kanundaki kıstaslara aykırı olarak yapılması halinde suçtur.

[88] T.C Yargıtay 12. Ceza Dairesi 2012/22781 Esas, 2013/22719 Sayılı Yayınlanmamış Kararı.

Kişisel bilgilerin bilimsel ortama geçirilip kaydedilmesi ve kullanılması günümüzde yaygın bir şekilde yapılmaktadır. Örneğin sigorta şirketleri, hastaneler, bankalar, büyük alışveriş merkezleri, müşterilerine ait kişisel bilgi kayıtlarını tutmaktadırlar. Bu bilgiler ancak sınırlı bir şekilde amacına uygun olarak kullanılması lazım. Eğer bu amacın dışında kullanılırsa veya üçüncü kişilerin yaralanmasına ya da kullanılmasına sunulduğu takdirde kişilerin hak kaybına veya zarara uğraması mümkündür. Bu nedenle bu kişilere ait bilgilerin amaç dışında hukuka aykırı olarak kayda alınması ve kullanılması suç olarak düzenlenmiştir[89].

Madde metninde kişisel verilerin "hukuka aykırı olarak kaydedilmesi" aranmakta, ancak verilerin sır olarak nitelendirilen ve sahibinin diğer kişilerin erişimine ve öğrenmesine izin vermediği veri niteliğinde olması aranmamaktadır. Bu nedenle bu suçun hukuksal değerini sırrın korunması oluşturmamaktadır[90].

Kişisel verilerin kaydedilmesi suçunu işleyecek kişi açısından madde metninde herhangi bir özellik belirtilmemiştir. Bu nedenle bu suçun faili herkes olabilir. Suçun mağduru ise sadece gerçek kişiler olabilir, tüzel kişiler bu suçun mağduru olamazlar.

Ancak 137 maddenin 1. fıkrası a bendine göre, bu suçların kamu görevlisi tarafından görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında arttırılacaktır.

Yine 5237 sayılı TCK'nın 137. maddenin 1. fıkrası b bendine göre belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde de verilecek ceza yarı oranında arttırılacaktır.

Kişisel verilerin kaydedilmesi suçunda fail bilerek ve isteyerek hareket etmelidir, yani kastı olmalıdır. Fail kanunda belirtilen eylemi gerçekleştirirken hukuka aykırı şekilde hareket ettiğini bilmelidir. Kanunda bu suç için failin bilerek ve isteyerek hareket etmesi arandığı için bu suç tipinin taksir ile işlenmesi mümkün değildir.

[89] DOĞAN Yusuf Hakkı, Antalya Cumhuriyet Savcısı (www.ceza-bb.adalet.gov.tr/makale/146.doc).

[90] DÜLGER M. Volkan, 2004 age s 268,269.

2. TCK'nın 136. maddesi "Verileri hukuka aykırı olarak verme veya ele geçirme suçu"

5237 Sayılı TCK'nın 136. Maddesi "Kişisel verileri, hukuka olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." Şeklindedir. Madde gerekçesinde ise *"hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır."*

Madde kenar başlığında "veriler" ibaresi kullanılarak başlanması ile madde metninde "kişisel verileri" ifadesiyle uygun düşmemektedir. Çünkü "veri" kelimesi ile "kişisel veri" kelimesi farklı anlamları ifade etmektedir. Kişisel veri, gerçek kişilere ait olan verileri anlatır; oysa "veri" kelimesi, kişisel verileri de kapsayan, gerçek olmayan kişilere ait olan verileri ve diğer her türlü veriyi içermektedir[91].

Günümüzde hemen hemen bütün kişilerin kişisel bilgileri, kendi rızaları ile internette yer alan, bazı sitelerde bulunmaktadır. İşte bu verilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da verilerin üçüncü kişiler tarafından ele geçirilmesinin önüne geçebilmek için kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri bağımsız bir suç tipi olarak 5237 sayılı TCK'nın 136. maddesinde düzenlenmiştir.

Madde metninde fail açısından bir özellik belirtilmemiştir. Bu sebeple suçun faili herkes olabilir. Aynı şekilde suçun mağduru için de bir özellik belirtilmemiştir. Bu yüzden suçun mağduru herkes olabilir.

Ancak 137 maddenin 1. fıkrası a bendine göre, bu suçların kamu görevlisi tarafından görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında arttırılacaktır.

Yine 137. maddenin 1. fıkrası b bendine göre belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde de verilecek ceza yarı oranında arttırılacaktır.

İnternet üzerinde işlenen suçların faili bu işlemleri rahatlıkla yapabilir, bilgi aktarımları gerçekleştirebilir, bunların delillendirme aşaması ise kolay değildir. Zira sınırı

[91] KARAGÜLMEZ Ali, 2009 s 253.

aşan bir durum varsa bunu ispatlamak daha da zor olmaktadır. Bu nedenle kanundaki vermek, yaymak, ele geçirmek nasıl ve hangi durumlarda hukuka aykırı olacağı konusunda düzenleme yapılması zorunludur.

5237 sayılı TCK'nın 140. maddesi gereğince bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara 5237 sayılı TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.

3. TCK'nın 138 maddesi "Verilerin yok edilmemesi suçu"

5271 sayılı TCK'nın 138. Maddesi " Kanunun belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir." Şeklindedir. Madde gerekçesinde ise *"hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, bağımsız bir suç olarak tanımlanmıştır."*

Verileri yok etmeme suçunun faili, verileri sistem içinde yok etmekle görevli olan kişidir. Fail, kamu görevlisi sıfatını taşımak zorunda değildir. İnceleme konusu suç tipi "özel türde, kendine özgü bir görevi ihmal suçu" olduğu için failin kamu görevlisi olması aranmamıştır. Kamu görevlisi olmayanlar açısından bir örnek vermek gerekirse, belli sürede veriyi yok etme görevi olan özel bir kurumdaki, örneğin hastanedeki görevli bir kişi de bu suçun faili olabilir. Ancak bu kişi, o hastanedeki verileri sistem içinde yok etmekle yükümlü olan kimse olmalıdır. Suçun mağduru için bir özellik aranmamıştır. Ancak genellikle bu suçun mağduru toplumdur.

Bu suçun faili, kanunda belirtilen eylemi gerçekleştirirken hukuka aykırı şekilde hareket ettiğini bilmelidir. Fail, suçun kanuni tanımındaki unsurları bilerek ve isteyerek gerçekleştirmiş olmalıdır. Kanunda bu suç tipinin kasten işlenmesi arandığı için, taksir ile işlenmesi mümkün değildir. Bu suç tipiyle kamu idaresine karşı duyulan güven korunmaktadır. Çünkü kanunda verileri yok etmekle görevlendirilen kişi bunu, kamu görevi olarak yapmaktadır[92].

[92] DÜLGER M. Volkan, 2004 s 282.

4. TCK'nın 124. maddesi "Haberleşmenin engellenmesi suçu"

5271 sayılı TCK'nın 132. Maddesi "*(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.*

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur" şeklindedir.

Bu suçun bilişim sistemleri aracılığıyla işlenmesi mümkündür. Günümüzde daha hızlı ve ucuz olduğu için klasik yöntemlere nazaran daha fazla kullanılan internet aracılığıyla elektronik posta, telefon görüşmeleri vb. gibi araçlar ile haberleşme sağlanmaktadır. Bu sebeple bilişim sistemleri aracılığıyla haberleşmenin engellenmesi eylemleri, 5237 sayılı TCK'nın 124. maddesinde suç tipi haline getirilmiştir. Kişiye veya herhangi bir kamu kurumunun elektronik hesabına gelen iletilerin muhatabı tarafından ulaşılmasından önce ulaşımın engellenmesi maddede yazılı suçu oluşturacaktır. Ancak engellemenin hukuka aykırı olarak yapılması gerekecektir[93].

5. TCK'nın 125. maddesi "Hakaret suçu"

5271 sayılı TCK'nın 125. Maddesi *"(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir. (2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.*

(3) Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

[93] KURT Levent, 2005 s 282.

c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,

İşlenmesi halinde, cezanın alt sınırı bir yıldan az olamaz.

(4) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır. Şeklindedir.

(5) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır."

Kişilerin şeref, namus ve haysiyetine karşı işlenen hakaret suçunun oluşabilmesi için somut bir fiil ya da olgunun isnat edilmesi gerekmektedir. Mesela kişinin bilişim sistemine "hırsız", "kel", "topal" , "sahtekâr" gibi hakaret içeren bir iletinin gönderilmesi halinde bu madde hükümleri uygulanacaktır. Bu isnatların bir internet sitesinde yayınlanması halinde ise, hükmolunacak ceza aynı maddenin 4. fıkrası gereğince altıda bir oranında arttırılacaktır. Çünkü hakaret suçunun alenen işlenmesi, bu suçun nitelikli şekli olarak kabul edilmiştir. Madde gerekçesinde de; "aleniyet için aranan temel ölçüt, fiilin, gerçekleştiği koşullar itibariyle belirli olmayan ve birden fazla kişiler tarafından algılanabilir olmasıdır" denilmiştir[94].

6. TCK'nın 132. Maddesi "Haberleşmenin gizliliğini ihlal suçu"

5271 sayılı kanunun 132. Maddesi *(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, (Değişik ibare: 6352 - 2.7.2012 / m.79/a) "bir yıldan üç yıla kadar hapis" cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, (Değişik ibare: 6352 - 2.7.2012 / m.79/a) "verilecek ceza bir kat artırılır"* .

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, (Değişik ibare: 6352 - 2.7.2012 / m.79/b) "iki yıldan beş yıla kadar hapis" cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın (Ek ibare: 6352 - 2.7.2012 / m.79/c) "hukuka aykırı olarak" alenen ifşa eden kişi, (Değişik ibare: 6352 - 2.7.2012 / m.79/c) "bir yıldan üç yıla kadar hapis" cezası ile cezalandırılır.(Ek cümle: 6352 - 2.7.2012 / m.79/c) "İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur." şeklinde düzenlemiştir.

Maddenin gerekçesinde, kişiler arasında haberleşmenin ne şekilde yapıldığının öneminin olmadığı, bu haberleşmenin örneğin mektupla, telefonla, telgrafla, elektronik posta

[94] ÖZGENÇ İzzet, 2007 s 855.

yoluyla yapılabileceğine işaret edilmiştir. O halde bilişim sistemi aracılığıyla gerçekleştirilen bu haberleşme yöntemleri de, inceleme konusu madde ile koruma altına alınmakta ve bu şekilde haberleşmeyi ihlal edenler cezalandırılmak istenmektedir. Bu maddede haberleşme hürriyeti ve haberleşmenin gizliliğinin korunması amaçlanmaktadır[95].

7. TCK'nın 142. maddesi'nin 2. fıkrası "e" bendi "Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu":

5237 sayılı TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 142. maddesinde nitelikli hırsızlık halleri düzenlenmektedir. Bu maddenin 2. fıkrasının "e" bendinde ise "bilişim sisteminin kullanılması suretiyle işlenen hırsızlık suçu" yer almaktadır. Görüldüğü üzere korunan hukuki değer göz önüne alınarak düzenlenen bu suç tipi, ilgili olduğu bölümde yer almaktadır.

5237 sayılı TCK'nın 141. maddesindeki genel tanıma göre hırsızlık, zilyedinin rızası olmadan başkasına ait taşınır bir malın, failin kendisine veya başkasına yarar sağlamak maksadıyla bulunduğu yerden almasıdır. 5237 sayılı TCK'nın nitelikli hırsızlık suçunu oluşturan 142. maddesinin 2. fıkrasının e bendinde, hırsızlık suçunun "bilişim sistemlerinin kullanılması suretiyle" işlenmesi halinde" üç yıldan yedi yıla kadar hapis cezasına hükmolunur" denilmektedir.

Teoride ve Yargıtay içtihatlarında en çok tartışılan konulardan biri ise, TCK'da düzenlenen Bilişim alanındaki suç tipleri ile hırsızlığın nitelikle halinde yer alan bilişim sistemlerinin kullanılması suretiyle meydana suçların birbiri ile karışmasıdır. Örneğin; *" Sanığın, evrakı tefrik edilen suç ortaklarıyla birlikte fikir ve eylem birliği içinde ..... Tekstil sanayi ve Ticaret Ltd. Şti adına .... Kayseri Ticari şubesinde bulunan .... Nolu YTL hesabına internet üzerinden girerek, mevduatta bulunan 7.250.00 YTL parayı, aynı bankanın Konya .... Şubesinde kendi fotoğrafının yapıştırıldığı ve V.T'ye ait kimlik bilgileri içeren sahte nüfus cüzdanı ile açtırdığı .... Nolu banka hesabına havale edip, bu şekilde hesaba yatan paradan 5.000YTL yi bankadan çektikten ve bakiye parayı çekmek isterken yakalandığı oluşa uygun şekilde kabul edilmiş olmasına göre, eylemin 5237 sayılı TCK'nın 244/4 maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden suçun nitelendirilmesinde yanılgıya düşülerek hırsızlık suçundan yazılı şekilde hüküm kurulması yasaya aykırıdır"*[96].

[95] KARAGÜLMEZ Ali, 2009 age s 236.

[96] Yargıtay 11.CD.,16.09.2007, E. 6122, K. 5897; www.kazanci.com (Erişim 13.09.2014).

Yargıtay'ın bu kararına göre failin bilişim sistemlerini kullanarak bir hesaptan bir başka hesaba para aktarma işlemini, TCK 244/2 bir bilişim sisteminde var olan verileri "başka bir yere gönderme" ve (3) numaralı fıkrasındaki "Bu fiillerin bir bankaya ait bilişim sistemi üzerinde işlenmesi halinde" hükümlerine uymaktadır. 244/4 fıkrasındaki yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin yararına haksız bir çıkar sağlaması hükümlerine girmektedir. Nitekim Yargıtay bu olayın hırsızlık suçu tanımına girmediğine kanaat etmiştir.

Bir başka tartışılan hususlardan biri de TCK 245/1'in uygulanması sorunudur. Şöyle ki TCK 245/1'e göre "başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse…" ibaresi yer almaktadır. Bu da hırsızlık suçunun tanımı ve bilişim sistemleri kullanılması suretiyle işlenmesi halinde hangi maddenin uygulanacağı sorununu gündeme getirmektedir. Örneğin; Sanığın şifresiyle birlikte çaldığı kredi kartıyla ATM'den para çekmesi fiillini[97] veya müştekinin bulunmadığı sırada işyerine girerek onun çantasından banka ve kredi kartlarını çalma filleri[98] hırsızlık suçundan değil, 765 Sayılı TCK'nın 525b/2 maddesinin uygulanmasını öngördüğü bazı fiillerdir. Fakat yukarıda örneklere baktığımızda aslında ortada saf bir bilişim suçu olmadığı gözlenmektedir. Nitekim Kişinin çantasının içerisindeki kredi kartıyla çalınması, hırsızlık suçunu oluşturmaktadır. Paranın ATM'den çekilmesi ise bu suçun nitelikli halini oluşturacaktır. Yani TCK 142/e maddesi uygulanması gerekmektedir. Fakat ATM'den para çekilirken veya çekilmeden önce bir takım bilişim yöntemleri ile kredi kartı şifresi ele geçiriliyor ise bu sefer TCK 245/1 'in uygulama alanı bulacağı kanaatindeyim. Zira TCK 245/1'teki "her ne suretle olursa olsun ele geçirme" ifadesi bilişim sistemlerinin kullanılması ile meydana gelebilecek farklı olaylar için yorumlanmalıdır. Yoksa kredi kartının fiziki olarak çalınması yada unutulan bir kredi kartın ele geçirilmesinde TCK 245/1 in uygulanması kanunun ruhuna uygun düşmeyecektir. Çünkü 245/1 Bilişim Alanında Suçlar Başlığı altındadır. Bu durumda Kanun koyucunun bu maddeyi tekrar ele alması gerektiğini düşünüyorum. Çünkü aynı durum kredi kartının şifrelerinin ele geçirilmesi durumunda da meydana gelmektedir. Kanun maddesi şifrenin ele geçirilmesini o kartın ele geçirilmesi olarak belirtmemiştir. Gerekçede de böyle bir düzenleme yoktur. Bu durumda, failin elde ettiği kredi kartlarının şifrelerini kullanarak menfaat elde etmesinde, TCK 245/1 in uygulanması, TCK'daki genişletici yorum yasağını akla getirmektedir.

[97] Yargıtay 6. CD.,11.04.2002, E.2418, K4937; www.kazanci.com (Erişim 13.09.2014).

[98] Yargıtay 6.CD., 01.02.2002, E.17027,K.1016; www.kazanci.com (Erişim 13.09.2014).

8. TCK'nın 158. Maddesinin 1. fıkrasının "f" bendi "Bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu"

5237 sayılı TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 158. maddesinde nitelikli dolandırıcılık halleri düzenlenmektedir. Bu maddenin 1. fıkrasının "f" bendinde "bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu" yer almaktadır. Görüldüğü üzere suçla korunan hukuksal değer göz önüne alınarak bu suç tipi de, ilgili olduğu bölümde düzenlenmiştir.

5237 sayılı TCK'nın 157. maddesinde dolandırıcılık, "hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamak" şeklinde tanımlanmıştır. Nitelikli dolandırıcılık suçunun düzenlendiği 158. maddenin 1. fıkrasının f bendinde dolandırıcılık suçunun, "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesi halinde iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur, denilmektedir.

Görüldüğü üzere f bendinde birden fazla nitelikli hal belirtilmiştir. Birincisi bilişim sistemlerinin ikincisi banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılıktır. Esasen bilişim sistemlerinin dolandırıcılık suçunda en çok kullanıldığı alanların başında banka ve kredi kurumlarının gelmiş olması etkilidir[99].

Nitekim bu suç tipi de, TCK'nın bilişim alanında düzenlenen suç tipleri ile uygulamada karıştırılmaktadır. Bu hususta verilmiş yargı kararları ise şu şekildedir. *"Dolandırıcılık suçunun oluşabilmesi için 765 sayılı TCK'nın hile ve desise ile 5237 Sayılı TCK'daki hilenin gerçek kişiye yöneltilerek aldatılması ve bu işlemeler sonucunda onun veya başkasının zararına olarak sanığın veya bir başkasının lehine haksız yarar sağlanması gerekli olup, somut olayda; sanığın şikayetçiye ait kredi kartı bilgilerini ele geçirip kendisine ait cep telefonu faturasını iletişim hiz. A.Ş nin web sayfasına girerek interaktif ortamda ödediğinin iddia ve kabul olunması karşısında, gerçek kişiye yöneltilen hile ve desise bulunmadığından yüklenen fiilin suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2 (5237 sayılı yasanın 244/4) maddesinde öngörülen bilişim suçunu oluşturulduğu*

[99] KARAGÜLMEZ Ali, 2009 age s 181.

gözetilmeden vasıfta hataya düşülerek banka vasıtası kılınarak nitelikli dolandırıcılık suçunu oluşturduğunun kabulü ile yazılı şekilde hüküm kurulması bozmayı gerektirmiştir"[100].

9. TCK'nın 226. maddesi "Müstehcenlik suçu"

5237 sayılı TCK'nın topluma karşı suçlar baslıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 226. maddesinde "müstehcenlik suçu" düzenlenmektedir. Bu suç tipi de bilişim sistemleri aracılığıyla işlenebilecektir. Bu madde, veri iletim ağları ile gerçekleştirilen müstehcen yayın eylemlerine uygulanabilecektir. Başka bir ifade ile bu maddede tanımlanan birçok suçu oluşturan hareketlerin, bilişim sistemleri vasıtasıyla gerçekleştirilmesi mümkündür.

Özellikle maddenin ikinci fıkrasında, müstehcen görüntü, yazı veya sözlerin basın ve yayın yolu ile yayınlanması veya yayınlanmasına aracılık edilmesi ve beşinci fıkrasında, maddenin üçüncü ve dördüncü fıkralarındaki suçların konusunu oluşturan ve müstehcenlik bakımından mutlak yasak kapsamına giren ürünlerin içeriğinin basın ve yayın yoluyla yayınlanması veya yayınlanmasına aracılık edilmesi ya da çocukların görmesinin, dinlemesinin veya okumasının sağlanması hallerinde, bilişim sistemleri kullanılmak suretiyle müstehcenlik suçu işlenebilecektir. Örneğin, bir okulun öğrencilerinin elektronik posta adreslerine pornografik mesaj, metin ve görüntülerin atılması olayında 226. madde uygulanacaktır. Maddenin 4. fıkrasında ise "Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır." Fakat kanun koyucu, doğal olmayan yoldan yapılan cinsel davranışın ne olduğu hususunda, gerekçede bir açıklama yapmamıştır. İnsanın doğası gereği oluşturduğu cinsel davranışlardan hangisi doğaldır, hangisi doğal değildir? Cinsel davranışların doğal olup olmadığına kim karar verecektir? Örneğin, Yargıtay'ın çok yeni bir kararında[101] kadın kadına sevişme, anal, oral ve grup seks görüntülerinin 226/4. Maddedeki "doğal olmayan yoldan yapılan cinsel davranışlara girdiği düşünülmüş, görevsizlik kararı verilerek dosyanın üst derece mahkemesine gönderilmesi yönünde bozma kararı verilmiştir. Bu kararla, Yargıtay'ın bu konudaki görüşü ortaya

[100] Yargıtay 11. CD., 23.01.2007, E. 8415, K. 87; www.kazanci.com (Erişim 13.09.2014).

[101] Yargıtay 5. CD. 2008/14636, 2009/1404; www.kazanci.com (Erişim 13.09.2014).

çıkmıştır. Mahkemelerin ve Yargıtay'ın, doğal olmayan cinsel davranışlar konusundaki bilirkişiliğini bazen de "Çocukları Muzır Neşriyattan Koruma Kurulu" yapmaktadır. Bir çok dosyada, görüntüler ve yazılar bu Kurul'a gönderilmektedir.

1117 sayılı kanunla kurulan kurulun görevi, bir olayda veya durumda sadece müstehcenlik olup olmadığını belirlemektir. Görevleri arasında doğal olmayan cinsel davranışların ne olduğunu tespit etmek yoktur. Kurul 10 kişiden oluşmaktadır: 2 bürokrat, 1 hakim veya savcı, 2 eğitimci, 1 doktor, 1 güzel sanatlar uzmanı, 1 akademisyen, 1 gazeteci ve 1 diyanetçiden kuruludur. Görüldüğü üzere, psikolog, psikiyatır veya seksolog yoktur. Kanun koyucular, diyanetçi ve bürokratlar varken, bu meslek gruplarını kurula almak ihtiyacı hissetmemişlerdir[102].

10. TCK'nın 228. maddesi "kumar oynanması için yer ve imkân sağlama suçu"

5237 sayılı TCK'nın topluma karşı suçlar başlıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 228. maddesinde "Kumar oynanması için yer ve imkân sağlama suçu" düzenlenmektedir. Bu suç tipi de bilişim sistemleri aracılığıyla işlenebilecektir. İnternette oluşturulan sanal gazinolarda kumar oynatılması durumunda, unsurları oluştuğu takdirde sanıklar aleyhine 5237 sayılı TCK'nın 228. maddesi uyarınca ceza verilmesi mümkün olacaktır. Söz konusu suçun oluşabilmesi için aleniyet şartı aranmamıştır. Bu durum madde gerekçesinde de ifade edilmiştir.

D- Fikir ve sanat eserleri Kanunu'nda düzenlenen bilişim suçları

Mobil teknolojilerin kullanımının giderek artması ile birlikte, günümüzde internet her zaman ve her yerde daha hızlı bir şekilde kullanılmaktadır. İnternetin bu denli yayılması sonucunda, müzik, film, dizi, şiir gibi eserlerin bedava paylaşılması, fikri eserlerin korunmasını güçleştirmektedir.

5846 Sayılı FSEK'da, 07.06.1995 tarih ve 4110 sayılı Kanun ile değişiklik yapılarak kanunun 2. maddesinde eser kavramının tanımı yapılırken bilgisayar programları da bu kavram içinde sayılmış ve kanunun koruma kapsamına alınmıştır. Kanunun 71. 72. ve 73.

[102] AHİ Gökhan; "Doğal olmayan yoldan yapılan cinsel davranışlar" ne demektir?" (http://www.bilisimhukuk.com/2009/08/%e2%80%9cdogal-olmayan-yoldan-yapilan-cinsel-davranislar%e2%80%9d-ne-demektir/) (Erişim: 17.09.2014).

maddelerinde eser sahibinin haklarının korunması açısından düzenlenen suç tiplerinin konusuna bilişim yazılımları da dahil edilmiştir.

FSEK'nın 71. maddesinde manevi haklara tecavüz, 72. maddesinde mali haklara tecavüz, 73. maddesinde ise diğer suçlar başlığı altında üç farklı suç tipi düzenlenmiştir. Böylece FSEK'in 2. maddesinde yapılan değişiklik ile bilişim yazılımlarının hukuka aykırı olarak çoğaltılması ve kullanılması eylemleri suç tipi olarak düzenlenmiştir[103].

5846 Sayılı Kanun'un 6. Maddesine, 4110 sayılı kanun ile eklenen (10) numaralı bende göre ise "Bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması" da fikir ve sanat eseri sayılmaktadır. Kanun 71. maddesinden itibaren, özellikle fikir ve sanat eserlerine yönelik olarak düzenlenmiş olan suçlar açısından, eser niteliği olan bilgisayar programları da suç kapsamında değerlendirilmektedir[104].

Ayrıca FSEK madde EK4'e göre *"Eser ve eser sahibi ile, eser üzerindeki haklardan herhangi birinin sahibi veya eserin kullanımına ilişkin süreler ve şartlar ile ilgili olarak eser nüshaları üzerinde bulunan veya eserin topluma sunulması sırasında görülen bilgiler ve bu bilgileri temsil eden sayılar veya kodlar yetkisiz olarak ortadan kaldırılamaz veya değiştirilemez. Bilgileri ve bu bilgileri temsil eden sayıları veya kodları yetkisiz olarak değiştirilen veya ortadan kaldırılan eserlerin asılları veya kopyaları dağıtılamaz, dağıtılmak üzere ithal edilemez, yayınlanamaz veya topluma iletilemez.*

Yukarıdaki fıkra hükümleri fonogramlar ve fonogramlarda tespit edilmiş icralar bakımından da uygulanır.

(Değişik fıkra:03/03/2004 - 5101/25.mad) Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlâlin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik

[103] AKINCI Hatice - ALIÇ, Emre/ER, Cüneyd; "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk Derleyen: Yeşim M. ATAMER; İstanbul Bilgi Üniversitesi Yayınları, 1. Bası (İstanbul, 2004), s. 264.

[104] KARAGÜLMEZ, 2009 s 150.

sağlayıcısına verilen hizmetin durdurulması istenir. İhlâlin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır. Servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür. Bu maddede belirtilen hususların uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından çıkarılacak bir yönetmelikle belirlenir".

Hükmü ile de Cumhuriyet Savcılarına re'sen internet sitesini erişime engelleme kararı verebilme yetkisi getirilmiştir. Buna göre Ek 4. maddede belirtildiği gibi, fikri mülkiyeti ihlal eden içerik (Örn. İllegal biçimde müzik, video, oyun, yazılım paylaşımı) bulunduran siteler, uyarılmalarına rağmen ihlale konu içerikleri kaldırmadığında erişim engelleme kararı verilebilmektedir[105].

E- Elektronik imza kanunu'nda düzenlenen bilişim suçları

Elektronik imza, bir tür şifreleme programıdır. Öncelikle bir yazılım ve şifreleme programıdır. Bu sayede güvenlikli haberleşme imkanı sağlanmaktadır. Elektronik imzanın kullanılmasının artması ile internetteki anonimliğin ortadan kaldırılması gündeme gelecektir[106].

5070 Sayılı Elektronik İmza Kanunu, TBMM tarafından 15.01.2004 tarihinde kabul edilmiş ve yayım tarihinden itibaren altı ay sonra yürürlüğe girmiştir. EİK'da, AB Direktifi doğrultusunda hazırlanmış ve güvenli elektronik imza, güvenli elektronik imza doğrulama araçları, bu imzanın hukuk alanında doğurduğu sonuçlar, elektronik sertifika hizmet sağlayıcı gibi elektronik imzayla ilgili araçlar ve hizmet sağlayıcılarının hukuki yetki ve sorumlulukları düzenlenmiştir[107].

EİK'nın 16. maddesinde "elektronik imza oluşturma verilerinin izinsiz kullanımı suçu", 17. maddesinde ise "elektronik sertifikalarda sahtekârlık suçu" düzenlenmiştir. Bu

---

[105] AHİ Gökhan; "İnternet Sitelerinin Erişime Kapatılmaması İçin Bazı Hukuki Tavsiyeler" (http://www.bilisimhukuk.com/2009/07/internet-sitelerinin-erisime-kapatilmamasi-icin-bazi-hukuki-tavsiyeler/) (Erişim 17.09.2014).

[106] BERBER Leyla Keser; "Elektronik İmza Kanunu Yönetmelik Çalışmaları" Bilişim Hukuku, Türkiye II. Bilişim Hukuku Sempozyumu; Derleyen Mete Tevetoğlu; Kadir Has Üniversitesi Yayınları s 19.

[107] DÜLGER Volkan. M, 2004 age s 307.

suçlar ile korunan hukuksal değer, evrakta sahtecilik suçlarında korunmak istenen hukuksal değerle aynıdır, yani devlet tarafından fertlere yüklenilen hukuk alanında inandırıcılığı olan bu tür verilere karşı güven korunmak istenmektedir.

Elektronik imza oluşturma amacıyla imza oluşturma verisi veya imza oluşturma aracının elde edilmesi, verilmesi, kopyalanması, bu araçların yeniden oluşturulması ile izinsiz elde edilen imza oluşturma araçlarının kullanılarak elektronik imza oluşturulması eylemlerinin yetkili kişilerin izni olmaksızın gerçekleştirilmesi halinde, EİK'nın 16. maddesinde düzenlenen elektronik imza oluşturma verilerinin izinsiz kullanımı suçu gerçekleşmiş olacaktır. Tamamen veya kısmen sahte elektronik sertifika oluşturulması, geçerli olarak oluşturulan sertifikaların taklit edilmesi, geçerli olarak oluşturulan sertifikaların tahrif edilmesi, yetkisiz olarak elektronik sertifika oluşturulması veya bu sahte elektronik sertifikaların kullanılması hallerinde ise EİK'nın 17. maddesinde düzenlenen elektronik sertifikalarda sahtekârlık suçu gerçekleşmiş olacaktır.

Kanunda düzenlenen suçların faili açısından her hangi bir özellik rastlanmamıştır. Bu nedenle bu suçları herkes işleyebilmektedir. Ayrıca her iki suçun da konusunu genel olarak veriler oluşturmaktadır. Bu suçların mağduru da daima devlettir. Ancak aynı eylemler dolayısıyla zarar gören kişiler ise bu suçun mağduru olamamakta ancak kamu davasına müdahale edebilmektedirler.

EİK'nın 16. maddesinde düzenlenen suç tipi açısından failin bilerek ve isteyerek hareket etmesi ve bunun yanında elektronik imza oluşturma amacının bulunması gerekmektedir. 17. maddesinde ise, failin bilerek ve isteyerek hareket etmesi suçun manevi unsurunu oluşturacaktır. Ancak her iki suç tipinin de taksirle işlenmesi mümkün değildir.

EİK'nin 16. maddesinde hapis cezasının alt sınırı olarak bir yıl, üst sınırı olarak üç yıl öngörülmüştür, para cezasının ise yalnızca alt sınırı belirtilmiş ve bu miktar beş yüz Türk lirası olarak öngörülmüştür. Kanunun 17. maddesi için ise, hapis cezasının alt sınırı olarak iki yıl, üst sınırı olarak beş yıl öngörülmüştür, para cezasının ise yalnızca alt sınırı belirtilmiş ve bu miktar bin Türk lirası olarak öngörülmüştür.

(Üçüncü Bölüm)

ADLİ BİLİŞİM

§ I. Adli bilişim kavramı

Gelişen teknolojik gelişmeler ışığında, bir takım suç işleme araçları süreç içerisinde değişiklik göstermiştir. Günümüzde işlenen suç tiplerinin bazılarında bilişim sistemleri bir hayli öneme sahiptir. Bazı durumlarda doğrudan suçun unsuru olurken bazı hallerde suç işlenmesinde aracı konumundadır. Bilişim sistemleri üzerinde gelişen olaylar akabinde yapılan çalışmalar aslında adli bilişim disiplinin ortaya çıkması için zemin hazırlamıştır[108]. Sayısal delillerin analizi ile ilgili bilimsel adlandırmada hiyerarşik yapı analiz edildiğinde, doktrinde ağırlıklı olarak Adli bilişim kavramı Adli bilimler kavramının altında yer almaktadır[109]. Adli bilimler, kimya, fen ve diğer sosyal bilimler alanlarında elde edilen bilgilerin, delillerin hukuk sistemi içerisinde kullanılması amacı ile ilgilenen bilim dallarının tümüdür[110].

A)- Tanım ve amaç

Adli bilişim kavramı gerek uygulamada gerekse doktrinde son yıllarda sıkça kullanılmaktadır[111]. İngilizce *"computer forensic"* olarak bilinen bu kavram, Türkçe'ye adli bilişim, bilgisayar incelemesi, bilgisayar kriminalistiği, adli bilgisayar incelmesi şeklinde çevrilmektedir[112]. Adli bilişim çeşitli şekillerde öğretide tanımlanmaktadır. Adli bilişim dijital delillerin usulüne uygun bir biçimde el konularak çeşitli ekipmanlar aracılığı ile delile zarar vermeden incelenmesi ve analiz edilmesidir. Bir başka ifade bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette

[108] TANRIKULU Cengiz, 2014 s 71.

[109] HENKOĞLU Türkay, 2014 s 1.

[110] HENKOĞLU Türkay, 2014 s 1.

[111]TANRIKULU Cengiz, 2014 s 71; BERBER Leyla Keser 2004 s 39.

[112] ÇAKIR Hüseyin Çakır, KILIÇ Mehmet Serkan, 2014 s 139.

kullanılıp kullanılmadığının tespiti amacıyla yapılan çalışmaların olarak açıklanmıştır[113]. Adli bilişim "potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama şeklinde tanımlanmıştır[114].

B- Adli bilişim alanına gerek duyulmasının sebepleri

Dijital delillerin en büyük özelliklerinden biri herhangi bir suç işlenmesinde iz bırakmasıdır. Bu sebeple herhangi bir suç işlenmesinde, bilişim sistemlerinde delil, iz ve emarelerin % 100 yok edilmesi her zaman mümkün değildir[115].

Bu sebeplerle; günümüz çalışma hayatı ve ihtiyaçlarının tamamının bilişim sistemleri üzerinde kayıt altına alınması sonucunda, ortaya çıkan hukuki sorunlarda ilgili sistemlerin analiz edilmesi gündeme gelmektedir. Örneğin; Dolandırıcılık, yetkisiz erişim, çocuk pornografisi, bilişim sistemleri aracılığı ile işlenen tüm suçlarda maddi gerçeğin ortaya çıkabilmesi için kriminal incelemenin yapılması gerekmektedir[116].

§ II. Adli bilişim evreleri

A- Olay yeri ve incelemesi

Olay yeri incelemesinin her suç tipinde, gerçek faillere ulaşabilme ve gerçek faillerin Ceza Kanun'un öngördüğü usul ve yasalar çerçevesinde cezalandırılabilmesi bir hayli önemlidir. Bilişim teknolojilerinin her geçen gün gelişmesi neticesinde ortaya çıkan suç tiplerinde, teknolojik gelişmelerin izleri görülmektedir.

Usule uygun bir olay yeri incelemesi özellikle dijital delillerin manipülasyona açık olması sebebiyle önem arz etmektedir. Adli Bilişim modelleri incelendiğinde, olay yeri inceleme ilk müdahale aşamasının safhaları şunlardır; olayın öğrenilmesi ve tespiti, olay yerine gitmeden önce yapılacak hazırlıklar, olay yerine ilk müdahale, elektronik delil tespiti, toplanması ve belgelenmesi ile elektronik delillerin güvenli taşımaya hazırlanması[117].

---

[113] HENKOĞLU Türkay, 2014 s 1.

[114] BERBER Leyla Keser; Adli Bilişim, Güncel Hukuk Dergisi, 6.Sayı İstanbul, Haziran 2004 S 19.

[115] DÜLGER Volkan Murat; Bilişim Suçları ve İnternet İletişim Hukuku Seçkin Yayınları, 2012 2. Bası, Ankara, s 661.

[116] HENKOĞLU Türkay, 2014 s 3.

[117] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, 2014 s 181.

1. Somut olayın tespiti ve olay mahalline gitmeden önce yapılması gereken hazırlıklar

Suç eyleminin öğrenilmesi akabinde olay yerine yapılacak müdahale sırasında adli bilişim uzmanlarının bulunması daha verimli ve etkin bir inceleme yapılmasını sağlayacaktır. Ancak ülkemizde özellikle uygulama aşamasında olay yerine müdahale sırasında çok fazla yetkin personel bulunmaması sebebi ile teknik bilgisi oldukça sınırlı adli kolluk görev almaktadır. Bu durumda uygulama aşamasında birçok sorunu doğurmaktadır. Bilişim sistemleri aracılığı ile işlenen sahtecilik, dolandırıcılık, yetkisiz erişim gibi suçların elektronik ortamda delillerinin yer aldığı gibi adam öldürme, adam yaralama, hakaret, vb suç türlerinde de elektronik ortamda delilleri bulunabilmektedir. Olayın türüne göre şüphelinin bilişim bilgisi tespit edilebilir. Bu halde; olay yeri ilk müdahale ekibinin karşılaşabileceği risk unsurları değerlendirebilir[118].

Soruşturmayı yürüten adli kolluk görevlileri olay yerindeki kişilerin ve olay yerinin mutlaka güvenliğini sağlayarak, elektronik delillerin bütünlüğünün sağlanması için gereken önlemleri almalıdırlar. Olay yerinde gerçekleştirilecek tüm işlemeler usule uygun yapılmalıdır. Gerekli güvenlik önlemleri alındıktan sonra ilk bakışta görünebilen delillerin dökümü yapılmalı ve bozulabilecek nitelikteki delillerin koruma altına alınmasına öncelik verilmelidir[119].

Yapılacak plan dahilinde olay yerine götürülecek cihaz ve yazılımlar belirlenmelidir. Söz konusu yazılımlar belirlenirken elektronik verilerin mahkemeler tarafından delil vasfını kaybetmeyecek, manipülasyona uğramamış, delil bütünlüğüne zarar vermeyecek programların kullanılması gerekmektedir. Olay yerine götürülmesi gereken araçlar genel olarak elektronik delil toplama, muhafaza, belgeleme araçlarıdır. Aşağıdaki ekipmanlar olay yerine gitmeden hazırlanmalıdır[120];

- ✓ Bilgisayar kasaları ve diğer cihazları sökmek için kullanılacak aletler,

[118] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, 2014 s 181.

[119] ÖZDİLEK Ali Osman, s 220.

[120] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, 2014 s 163.

- ✓ Elektronik delillerin ve olay yerinin belgelenmesi için kullanılacak kamera, fotoğraf makinası, delil numaralandırma etiketleri, renkli fosforlu kalemler, kroki şablonu, elektronik delil formları, mesafe ölçüm araçları,
- ✓ Elektronik ve fiziki delillerin bütünlüğünü korumak için elektrostatik deşarj ekipmanları, tek kullanımlık lateks eldivenler,
- ✓ Elektronik delilleri usulüne uygun elde etmek için kullanılacak adli bilişim cihazları ve boot-DVD'leri, delillerin alınacağı(adli bilişim açısından steril) sabit diskler, donanımsal yazma koruma araçları, dizüstü bilgisayarlar, cross-over kablo,
- ✓ Elektronik delillerin güvenli taşınması için darbeye dayanıklı, antistatik ve antimanyetik çantalar, delil torbaları, radyo frekansına karşı korumalı çantalar,
- ✓ Olay yerinden elektronik delil toplamaya yardımcı olarak kullanılabilecek güç kaynakları, çevirici ve bağlantı aparatları, elektronik çoklama/uzatma cihazları network kabloları.

2. Olay yeri incelemesi ve ilk müdahale

Bilişim sistemleri aracılığı ile işlenen suçlarda deliller, diğer deliller gibi dikkatlice ele alınmalı ve delillerin bütünlüğünü koruyacak şekilde hareket edilmelidir. Bu zorunluluk sadece donanımın fiziksel bütünlüğünün korunması değil, aynı zamanda içerdikleri dijital delillerin bütünlüğünün korunması gerekmektedir. Bu sebeple, bilişim sistemlerine ilişkin delillerin bazı tiplerinin özel olarak toplanması, paketlenmesi ve nakledilmesi gerekmektedir. Dijital delillerin toplanması işine başlamadan önce, dokümantasyon ve konum tespiti işinin bitilmiş olması gerekmektedir. Öncelikle iz, biyolojik veya görünmezler izler gibi diğer delil çeşitlerinin mevcut olabileceğinin bilincinde olmak gerekmektedir[121].

Olay yerinin güvenliğinin sağlanması aşağıdaki adımlardan oluşmaktadır[122];

- ✓ Olay yerinin bütün giriş ve çıkışının belirlenmesi,
- ✓ Olay yerinde bulunan şüphelilerin elektronik delillerin yanından ve çevresinden hızla uzaklaştırılması,

[121] ÖZDİLEK Ali Osman, s 221.

[122] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, 2014 s 164.

- ✓ Olay yerinin sınırlarını belirleyen şeritlerin çekilmesi,
- ✓ Diğer kolluk personeli ve şüphelinin elektronik delillerin bulunduğu ortamdan çıkarılması,
- ✓ Yetkili olmayan kimselerden gelen teknik yardım taleplerinin reddedilmesi,
- ✓ Kişisel ve taşınabilir cihazlar dahil tüm elektronik cihazların güvenliğinin alınması,
- ✓ Elektronik cihazlara yetkisiz personelin erişiminin engellenmesi,
- ✓ Hiçbir elektronik cihazın yerinin ve durumunun değiştirilmesine müsaade edilmemesi,
- ✓ Kapalı olan bilgisayar veya elektronik cihazların açılmaması,
- ✓ Açık olan bilgisayar veya elektronik cihazların kesinlikle kapatılmaması, gerekirse çalışmaya devam edebilmeleri için gerekli elektrik gücünün sağlanması.

Olay yerinde ilk müdahale esnasında şüpheli veya şüphelilerden ön bilgi almak bazı hallerde fayda olabilecektir. Ancak burada aramaya giden adli kolluk personelinin uzmanlığı da çok önemlidir. Zira şüpheliler delillere ulaşılmaması açısında adli kolluk personeline yanıltıcı bilgilerde verebilir. Bu kapsamda olay yerinde bulunan şüphelilerden, konunun elverdiği ölçüde, elektronik delillere yönelik aşağıdaki konuları kapsayan bilgiler alınabilir[123];

- ✓ Cihazların kimlere ait olduğu ve kullanıcı adları,
- ✓ Bilgisayar ve internet(Sosyal ağ hesapları vb) kullanıcı bilgileri,
- ✓ Bütün oturum açma isimleri, şifreleri ve kullanıcı hesaplarının detayları,
- ✓ Elektronik cihazların kullanım amacı,
- ✓ Yazılım, hesap veya veri erişiminde kullanılan şifreler (BIOS, oturum açma, e-posta, PGP vb şifreleri)
- ✓ Kullanımda olan otomatik uygulamalar,
- ✓ İnternet erişim tipi,
- ✓ Olay yeri haricinde bulunan veri depolama birimlerine ait bilgiler,

[123] ÇAKIR Hüseyin - KILIÇ Mehmet Serkan, 2014 s 164.

- ✓ İnternet servis sağlayıcı bilgileri,
- ✓ Olay yerinde bulunan verilerin erişimine yönelik kısıtlamalar,
- ✓ Kullanımda olan yok edici, zarar verici donanım ve yazılım bilgileri.

Adli bilişim incelemelerinde, olay yeri esnasından incelemenin sonuna kadar oluşan sürecin belirli bir disiplin altında yürümesi gerekmektedir. Buna göre adli bilişim incelemesini 4 ana başlık altında sınıflandırabilir.

a) Delil toplama

Yukarıda izah edildiği üzere, delil toplama aşaması, dijital delillerin niteliği gereğince aşırı derecede dikkat edilmesi gerekmektedir. Türkiye'de henüz delil toplama sürecinde kullanılması gereken ekipman ve donanımlar ile ilgili olarak geliştirilen ve yasa ile desteklenen ve kullanılan bir standart bulunmamaktadır. Adli bilişim alanın geliştirilen ISO/IEC 27037[124], 27041, 27042[125] ve 27043[126] standartları, bilgi güvenliği ISO/IEC 27000 olarak geçer ve ISO (International Organization for Standardization) ve IEC (International Electrotechnical Commission) şeklinde tanımlanmaktadır[127]. Ancak söz konusu standartlar ile bu alandaki eksikliğin giderilmesine çalışılmış olsa da uygulama aşamasında belli bir standardın geliştirilmediği görülmektedir. Ancak adli kolluk birimleri gerek doktrinde gerekse de uluslararası standartlarda geliştirilen standartlar dahilinde dijital delillerin bütünlüğü bozmayacak şekilde delil toplama aşamasını yürütmektedir.

Uluslararası standartlarda belirtilen ilkeler gereğince değerlendirme yapıldığında sayısal delillerin elde edilmesinde göz önüne alınacak ilkeler şunlardır[128];

- ✓ Toplanılan, muhafaza edilen, incelenen ve nakledilen delilin, delil güvenliği ve doğruluğunun uygun bir şekilde sağlanması için kolluk kuvvetleri ve adli bilim organizasyonları etkili kalite kontrol sistemleri oluşturulmalıdır,
- ✓ Dijital delili inceleyen ve el koyan tüm birimler, uygun standart yönetim süreçlerine bağlı kalmalıdır,

---

[124] http://www.iso27001security.com/html/27037.html Son Erişim 07.03.2015

[125] http://www.iso27001security.com/html/27042.html Son Erişim 07.03.2015

[126] http://www.iso27001security.com/html/27043.html Son Erişim 07.03.2015

[127] http://www.leylakeser.org/search/label/Adli%20Bilişim "Iso/Iec'in Adli Bilişim Standartlari" Son Erişim 07.03.2015)

[128] DEĞİRMENCİ Olgun, 2014 s 195.

- ✓ İlgili birimlerin yönetimi, yıllık bazda söz konusu standart yönetim süreçlerini, uygunluğunu ve etkinliği sağlamak için gözden geçirmelidirler,
- ✓ Kullanılan süreçler, alanda genel olarak kabul görmeli veya veri toplanması veya kaydedilmesinde bilimsel yöntemlerle desteklenmelidir,
- ✓ İlgili birimler, uygun teknik süreçlerin yazılı nüshalarını muhafaza etmelidirler,
- ✓ Elkoyma ve inceleme süreçleri için etkili ve uygun donanım ve yazılımlar kullanılmalıdır.
- ✓ Sayısal delile elkonulması, delilin muhafazası, incelenmesi ve nakledilmesi ile ilgili tüm işlemler, daha sonraki gözden geçirme ve tanıklık işlemleri için yazılı şekilde kaydedilmelidir.
- ✓ Esas delili herhangi bir şekilde değiştirecek, ona zarar verecek veya yok edecek potansiyel eylemler, bu alanda nitelikli personel tarafından yerine getirilmelidir.

b) İnceleme

Bilişim sistemleri aracılığı ile işlenen suçlarda elde edilen deliller, ilgili birimler tarafından işleme tabi tutulmadan önce bir takım işlemlere tabi tutulular. Silinmiş verilerin geri getirilmesi, şifrelenmiş alanlara girilmesi için yapılan çalışmalar örnek gösterilebilir[129]. Tüm bu işlemler için adli kolluk birimleri olan yerinde var olan delilin *"bit by bit"* zaman damgalı hash değerli bir yedeğini alması gerekmektedir. Akabinde ise o yedek üzerinden tekrardan bir *"bit by bit"* yedek çıkartılması ve tüm çalışmanın *"best copy"* diye tabir edilen bu disk üzerinde yapılması gerekmektedir. Böylece inceleme esnasında diske veya içerisinde verilere herhangi bir zarar gelmesi halinde, tekrardan yedek kopyadan bir örnek çıkarılarak inceleme eksiksiz ve usule uygun bir biçimde gerçekleştirilebilecektir.

İnceleme esnasında ise somut olayın şartlarına göre çeşitli yöntemler gerçekleştirilecek, delilin bütünlüğüne zarar vermeyecek ve güvenirliği uluslarası standartlarda kabul görmüş programlar kullanılmalıdır. Bu aşamada, somut olaya göre şüpheli kelimelerin aranması yapılabileceği gibi, şifrelenmiş verilerin geri getirilmesi, silinmiş verilerin disk üzerine geri getirilmesi, diskte tanımlanmış veya tanımlanmamış alanlarda bulunan gizli verilerin bulunması vb çalışmalar yapılmaktadır.

[129] DEĞİRMENCİ Olgun, 2014 s 254.

c) Çözümleme

Verinin analiziyle, toplanan verilerin birbiri ile irtibatlandırılarak onlardan muhakemede kullanılacak sayısal delillerin elde edilmesi sağlanır. Sağlıklı bir inceleme ve inceleme sonrasında maddi gerçeği ortaya çıkaracak sayısal delillere ulaşabilmesi için olay yerinden elde edilen delillerin incelenmesini yapacak cihaz ve konusunda uzman personelin bulunduğu laboratuvar ortamına gerek duyulabilmektedir[130]. Verinin çözümlenmesi aşamasında işlenecek yollardan biri de bir zaman dizgesine sokulması suretiyle, suç içeren eylemler dizesinin yeniden yapılandırılmasıdır. Örneğin elektronik posta mesajları veya ağdaki konuşma kayıtlarının hepsi, kaydın alındığı veya gönderildiği zaman damgasını içermektedir. Adli bilişim uzmanı maddi olayı yeniden yapılandırırken iki temel analiz sistemi kullanmaktadır. Bunlardan birisi günlük dosya analizi (log file analysis) diğeri ise dosya sistem analizi (file system analysis)'dir. Günlük dosya analizi, zaman damgalarının kontrolü, günlük kayıtlarına girdi yapan sürecin tanımlanması ve girdinin yaratılma nedenlerinin kontrolünü içermektedir. Zaman damgalarının kontrolünde, sistem saatinin zaman damgasının yaratıldığı sistemlere göre farklılık arz edebileceği gözden kaçırılmamalıdır[131].

d) Raporlama

Raporlama ve çözümlenen verilerin belgelenmesi adli bilişim aşamalarında, mahkemelerin gördüğü kısım olması sebebi ile bir hayli önemlidir. Bir başka ifade ile konunun teknik olması sebebi ile Mahkeme Hakimi, savcısı veya sanık müdafi, katılan vekili adli bilişim uzamanın verdiği raporu analiz ederek dosyanın hukuka uygun bir şekilde tekâmül etmesini sağlayacaklardır. Bu sebeple; teknik bir raporda anlatılmak istenenler bir hukukçunun da anlayabileceği yalınlığa sahip olması gerekmektedir. Adli bilişimci, süreç içerisinde karşılaştığı tüm detayları belgelemek zorundadır. Bu belgeleme bazı durumlarda video kamera ile kaydetme, bazı durumlarda fotoğraflama şeklinde olabileceği, bazı durumlarda kayıt tutma şeklinde de gerçekleşebilmektedir. Bir adli bilişim raporunda şu hususların bulunmasına dikkat edilmelidir[132];

---

[130] DOKURER Semih; Adli Bilimlerde Seçilmiş Konu Başlıkları Ses, Görüntü ve Data İncelemeleri (Editör Levent Bayram), Ankara 2008 S 243.

[131] DEĞİRMENCİ Olgun, 2014 s 267.

[132] DEĞİRMENCİ Olgun, 2014 s 268.

- ✓ Olay tarihi, zaman, adres bilgileri,
- ✓ Donanımların üretici, seri numarası, modeli, unsurları gibi sisteme ait bilgiler,
- ✓ Verilerin toplanması esnasında sistemin durumuna ilişkin bilgiler,
- ✓ Olaya ilişkin dosya numarası, şikayetçi veya şüpheli gibi bilgiler,
- ✓ Verinin analiz edilmesi esnasında tüm aşamalar ve özellikle kullanılan araçlar araçlar, süreçler, konular, hata mesajları gibi bilgiler,
- ✓ Olay yerinden toplanan fotoğraflar ve fiziksel deliller varsa tanık bilgileri.

Mahkemeye sunulacak bu tür raporlarda, tespitlere nasıl ve nereden ulaştığını ifade etmeli, incelenen cihaz, araç ve diğer bulgular üzerinde ne gibi incelemeler yaptığına raporunda yer vermelidir. Raporun sonuç kısmında; kanaat, tespit veya bilgi niteliğinde araştırma sonuçlarını gösterilmesi gerekmektedir. Kanaat, tespit veya bilginin kesinlik dereceleri birbirinden farklı olduğundan, mahkeme tarafından eylemin sübuta erip ermediğini konusunda göz önüne alınma dereceleri de farklı olacağından raporda bu hususlara özen gösterilmelidir[133].

Bilirkişi raporunda, dijital delillerin, diğer delillerle desteklenmediği sürece bir kişi ile irtibatlandırmasının mümkün olmadığı noktası unutmamalıdır. Dolayısıyla, sayısal delillerin bir kişiye ait olup olmadığı noktasında, kesinlik düzeyinde bilgi mevcut değilse yargıda bulunmaktan kaçınılmalıdır[134].

[133] BALI Yunus, Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırabilirliği; Adli Bilimlerde Seçilmiş Konu Başlıkları Ses, Görüntü ve Data İncelemeleri (Editör: Levent Bayram) Ankara 2008, S 231.

[134] BALI Yunus, Rapor Metinleri s 235.

(Dördüncü Bölüm)

CEZA MUHAKEMESİ HUKUKUMUZDA BİLİŞİM SİSTEMLERİNE ARAMA VE EL KOYMA

§ I Türk ceza muhakemesi hukukunda koruma tedbirleri

A- Kavram

Ceza muhakemesinde hukuku niteliklerine göre maddi gerçeğe ulaşılabilmesi için yargılamanın yapılabilmesi veya ileride verilecek hükmün infazının mümkün olabilmesi amacıyla bazı önlemlere başvurulması gerekebilir. Bu önlemler, şüpheli kişinin ve/veya sanığın hazır bulunmasını veya delillerin karartılmamasını önlenmesini güvence altına alınmasını sağlanması hususu başta gelmektedir. Bu tedbirlerin gerçekleştirmesi ise ceza muhakemesi süjelerine, özellikle bir suç işlemiş olmakla suçlanan kişiye ya da eşyaya karşı zor kullanılmasını zorunlu kılmaktadır. Söz konusu tedbirler her biri bir ya da daha çok temel hakka dokunan bu tedbirlere koruma tedbirleri denir[135].

Türk öğretisinde koruma tedbirleri terimi hakkında bir birlik yoktur. Bunlara Taner, ihtiyati tedbir; Erem, usul tedbirleri; Yüce, zorlayıcı önlem; Yurtcan, ceza yargılaması önlemi; Tosun, Kunter, Yenisey ve Centel de koruma tedbirleri terimini kullanmaktadır[136].

Koruma tedbirlerinin amacı, ceza muhakemesini yapılabilir kılmak ve yargılama sonucunda verilecek hükmün infaz edilebilmesini güvence altına almaktır. Delillere ulaşmak ve delillerin karartılmasını önlemek, şüpheli veya sanığın muhakeme sırasında veya hükmün infazı için hazır bulundurulmasını sağlamak üzere bu tedbirlere başvurulabilir[137].

---

[135] CENTEL Nur - ZAFER Hamide, Ceza Muhakemesi Hukuku, 6. Bası, s 302.

[136] ÖZTÜRK Bahri, Uygulamalı Ceza Muhakemesi Hukuku, 12. Bası, s 537.

[137] ŞAHİN Cumhur, Ceza Muhakemesi Hukuku I, 2. Baskı, s 197.

B- Koruma tedbirlerinin ortak özellikleri

Koruma tedbirleri, kişinin suçlu olup olmadığı hüküm altına alınmadan önce kişinin temel bir hakkının sınırlanmasına sebebiyet verir. Bu sınırlama geçici, yalnız yasayla düzenlenebilen ve yargı kararının verilmesi açısından araç niteliği taşır[138].

1. Yasayla düzenlenmiş olması

Bütün koruma tedbirleri temel bir hakka müdahale niteliğinde olduğundan bu temel haklara müdahalenin sınırlarının yasayla belirlenmesi şarttır. Koruma tedbirleri bu niteliği gereği Anayasa, Avrupa İnsan Hakları Mahkemesi Kararları ve usulüne uygun yürürlükte bulunan taraf olduğumuz uluslar arası sözleşmelere uygun bir biçimde düzenlenmiş olması gerekmektedir. Yasayla düzenlenmemiş bulunan bir koruma tedbiri kıyas yoluyla uygulanamayacağı gibi, yasada yer alan bir koruma tedbiri için aranan şartlar ve sebepler de kıyas yoluyla genişletilemez[139].

2. Suç şüphelerinin belli bir yoğunlukta olması

Koruma tedbirlerinde genel olarak kuvvetli şüphe aranır. Yakalama, tutuklama, zorla getirme gibi koruma tedbirlerinde kuvvetli şüphe aranır. Ancak arama, el koyma gibi bazı koruma tedbirlerinde makul şüphenin varlığı koruma tedbirine başvurmak için yeterli görülmüştür. Bazı istisnai durumlarda ise basit şüphenin varlığı ile de yetinilebilmektedir. Burada somut olay ile şüphe derecesinin orantılılığı esas alınarak hareket edilmelidir[140].

3. Hükümden önce temel bir hakkı sınırlaması

Koruma tedbirlerinin kanunla düzenlenmesinin zorunlu olması ve diğer ortak özelliklerinin bulunmasının aranması asıl sebebi ilgili kişi hakkında henüz verilmiş bir mahkeme kararı olmamasına rağmen çeşitli şekillerde sahip olduğu mutlak hakkın kısıtlanmasıdır. Daha suçlu olup olmadığını bilmediğimiz; başka bir ifade ile suçlu olduğu bir yargı kararıyla sabit hale gelmeyen bir kimse hakkında yakalama ve/veya tutuklama yaparak kişi özgürlüğünü sınırlandırmakta; arama ve/veya el koyma yapmak suretiyle mülkiyet

[138] KAPILI Kübra; Bilgisayarlarda ve Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama, El Koyma 2013 Bilgi Üniversitesi Sosyal Bilimler Enstütüsü s 2 (Yayınlanmamış Proje).

[139] ŞAHİN Cumhur, s 200.

[140] KAPILI Kübra, 2013 s 2.

hakkını kısıtlamakta; telefonlarını dinlemek suretiyle özel hayatına müdahale edilmektedir. Bu özellik tüm koruma tedbirlerinden doğrudan veya dolaylı olarak vardır[141].

4. Geçici nitelikte olması

Koruma tedbirleri araç niteliğindedir. Uygulaması hüküm verilinceye kadar sürmez, amacının gerçekleştiği noktada son bulması gerekmektedir. Koruma tedbiri ile ulaşılmak istenen amaç gerçekleştikten sonra tedbire devam edilmesi tedbiri hukuka aykırı hale getirir. Çoğunlukla kanun bu amacın ne zaman gerçekleşmiş sayılacağını, süreler öngörmek suretiyle belirtmektedir[142].

Koruma tedbirleriyle delillere ulaşılmakta ve ulaşılan deliller korunmaktadır. Örneğin, yakalama tutuklamaya; tutuklama ise sanığın muhakemede hazır bulunmasının sağlanmasına, delillerin ortaya konulabilmesine veya muhtemel hapis cezasının infazının sağlanmasına yardımcı olmaktadır[143].

5. Gecikmede sakınca bulunması

Hükümden önce temel hak ve özgürlüklere müdahale edildiği için, ancak zorunluluk bulunduğunda koruma tedbirine başvurulabilir[144]. Bu itibar ile gecikmesinde sakınca bulunmadığı hallerde bu tür koruma tedbirlerine başvurulmasına gerek görülmemelidir. Bu çareler başvurulmadığında veya geç başvurulduğunda, muhakeme yapılamaz, hüküm infaz edilemez ve/veya muhakeme masrafları karşılanamaz duruma girecekse gecikmesinde tehlike olduğu kabul edilebilir[145]. Gecikmede tehlike bulunup bulunmadığı, her somut olayda olayın özelliklerine göre takdir edilir.

---

[141] ÖZTÜRK Bahri, s 540.

[142] ŞAHİN Cumhur, s 201.

[143] CENTEL Nur - ZAFER Hamide, s 304.

[144] ŞAHİN Cumhur, s 201.

[145] ÖZTÜRK Bahri, s 540.

6. Hakim, gecikmesinde sakınca bulunduğu hallerde savcı kararının bulunması

Kanunda öngörülen bir çok durumda gecikmede sakınca varsa koruma tedbirlerine savcılık karar vermekte yetkili olabilmektedir. Bazı durumlarda kolluk (CMK md. 119) ve hatta bazı istisnai durumlarda herkes (CMK md. 90) yetkili olabilmektedir.

Ceza Muhakemesi Kanunu madde 119[146].- *"(Değişik 1. fıkra: 5353 - 25.5.2005 / m.15) (1) Hakim kararı üzerine veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri arama yapabilirler. Ancak, konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama, hakim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile yapılabilir. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhal bildirilir."*

Ceza Muhakemesi Kanunu madde 90[147]. "*(1) Aşağıda belirtilen hallerde, herkes tarafından geçici olarak yakalama yapılabilir: a) Kişiye suçu işlerken rastlanması. b) Suçüstü bir fiilden dolayı izlenen kişinin kaçması olasılığının bulunması veya hemen kimliğini belirleme olanağının bulunmaması. (2) Kolluk görevlileri, tutuklama kararı veya yakalama emri düzenlenmesini gerektiren ve gecikmesinde sakınca bulunan hallerde; Cumhuriyet savcısına veya amirlerine derhal başvurma olanağı bulunmadığı takdirde, yakalama yetkisine sahiptirler. (3) Soruşturma ve kovuşturması şikayete bağlı olmakla birlikte, çocuklara, beden veya akıl hastalığı, malullük veya güçsüzlükleri nedeniyle kendilerini idareden aciz bulunanlara karşı işlenen suçüstü hallerinde kişinin yakalanması şikayete bağlı değildir. (Değişik 4. fıkra: 5353 - 25.5.2005 / m.7) (4) Kolluk, yakalandığı sırada kaçmasını, kendisine veya başkalarına zarar vermesini önleyecek tedbirleri aldıktan sonra, yakalanan kişiye kanuni haklarını derhal bildirir. (Değişik 5. fıkra: 5353 - 25.5.2005 / m.7) (5) Birinci fıkraya göre yakalanıp kolluğa teslim edilen veya ikinci fıkra uyarınca görevlilerce yakalanan kişi ve olay hakkında Cumhuriyet savcısına hemen bilgi verilerek, emri doğrultusunda işlem yapılır. (6) Yakalama emrine konu işlemin yerine getirilmesi nedeniyle yakalama emrinin çıkarılma*

[146] http://www.kazanci.com/kho2/ibb/giris.htm Erişim 13.12.2014

[147] http://www.kazanci.com/kho2/ibb/giris.htm Erişim 13.12.2014

amacının ortadan kalkması durumunda mahkeme, hakim veya Cumhuriyet savcısı tarafından yakalama emrinin derhal iadesi istenir."

7. Orantılılık ilkesinin bulunması

Failin eylemin ağırlığı ile başvurulacak önlemin ağırlığı arasında bulunması istenen dengedir. Bu bakımdan ne kadar ağır bir suç söz konusu olursa o kadar ağır önlemlere başvurulabilecektir[148]. Bir başka ifade ile söz konusu eylem sebebi ile faile uygulanacak koruma tedbirinin değerlendirilmesi gerekmektedir. Örneğin; internet üzerinden bir kimseye hakaret eden bir kişi hakkında, salt söz konusu eylemi sebebi ile CMK md. 100 gereğince Tutuklama kararı verilemez. Zira bir kimseye hakaret suçu TCK 125. Maddede düzenlenmiş olup, üç aydan iki yıla kadar hapis veya adli para cezasına hükmolunmaktadır. Fail üst sınırdan ceza alsa bile mevcut indirimler ve yasal düzenlemeler gereğince hapis cezası infaz edilemeyecektir. Ancak söz konusu eylem sebebi ile failin Tutuklanmasına karar verilmesi durumunda, ortada çok açık bir hukuka aykırılık bir başka ifade ile tipik bir orantılılık ilkesine aykırılık gündeme gelecektir.

C- Koruma tedbirlerinin çeşitleri

Gecikmede tehlike bulunması hali, haklı görünüş hali ve orantı bulunması halinin varlığından koruma tedbirlerine başvurulabilir. Bu ön şartlar gerçekleşmeden bir koruma tedbirine başvurulamaz. Ceza Muhakemesi Kanunu'nda düzenlenen koruma tedbiri çeşitlerini şu şekilde sıralayabiliriz[149];

"Yakalama, gözaltı, tutuklama, zorla getirme, adli kontrol, güvence gösterilmesi, arama, elkoyma, şirket yönetimi için kayyım tayini, telekomünikasyon yoluyla yapılan iletişimin dinlenmesi, beden muayenesi, fizik kimliğin tespiti, gizli soruşturmacı görevlendirme, teknik araçlarla izleme, tanık koruma - gizli tanık".

Tez konusunun, koruma tedbirlerinden "Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar" olması dolayısıyla Ceza Muhakemesi Kanunu 134. Maddesinin konu başlığı olan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma koruma tedbirine yer verilecektir.

---

[148] YURTCAN Erdener, Ceza Yargılaması Hukuku, 10. Bası, s 405.

[149] ŞAHİN Cumhur, s 201.

§ II Bilişim suçları açısından ceza muhakemesi koruma tedbirleri

A- Kavram ve hukuki niteliği

Ceza muhakemesi hukukunun soruşturma tedbirlerinin maddi ceza hukukuna farklı şekillerde etkisi bulunmaktadır. Ceza muhakemesi hukuku tedbirleri uygulanırken maddi gerçeğe usulüne uygun bir şekilde ulaşma hedefi yerine getirilmektedir. Bu sebeple; arama ve el koyma hukukuna sadece ceza muhakemesi prensipleri değil aynı zamanda anayasa ve maddi ceza hukuku prensipleri ve kuralları da dikkate alınmaktadır[150].

Bilişim Sistemleri Aracılığı ile işlenen suçlarda ise ceza muhakemesi hukukunda ayrı bir düzenlemeye gidilmiştir. CMK 134. maddesinde adli aramanın özel bir şekli olup, ceza muhakemesi anlamında genel arama müessesi bilindiği üzere hukukumuzda CMK'nun 116. ve devamı maddelerinde düzenlenmiştir. Bu halde; bilişim sistemlerinde aramalarda öncelikle CMK 134. maddede yazılı hükümler uygulanacak, bu maddede düzenlenmeyen hususlarda ise bu maddede yazılı hükümlere aykırı olmamak üzere genel arama ve el koymaya ilişkin hükümler uygulanabilecektir[151].

B- Bilişim sistemlerinde arama, kopyalama ve el koyma işlemine ilişkin hukuki mevzuat

Bilişim Sistemleri üzerinde Arama ve El Koyma kararı, Temel Hak ve Özgürlükleri Kısıtlayıcı bir işlemdir. Bu sebeple; T.C Anayasası Madde 20/2[152] *"(Değişik: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."* gereğince koruma altına alınmıştır. Bu sebeple; bilişim sistemleri üzerinde arama ve el koyma yapılabilmesinin çok katı kurallara bağlanmasının temel sebebi vatandaşlara Anayasa ile tanınmış temel hakkının kısıtlanmasıdır. 1 Haziran 2005 tarihinde

[150] TANRIKULU Cengiz, 2014 s 350.

[151] TANRIKULU Cengiz, 2014 s 350.

[152] www.kazanci.com Son Erişim 06.03.2015

yürürlüğü giren, 5271 sayılı Ceza Muhakemesi Kanunu'nun 2. Maddesinin (1) numaralı fıkrasının (e) bendine göre, "Soruşturma: Kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi" ifade etmektedir.

CMK'nın 134. Maddesinde, " Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma", 135. Maddesinde "iletişimin tespiti, dinlenmesi ve kayda alınması", 140. Maddesinde "Teknik araçlarla izleme" konularında, birtakım farklı hükümlere yer verilmiştir. CMK'nında yer alan bu düzenlemeler, ağırlıklı olarak, bilişim suçları dışında yer alan önem arz eden suçların, dillendirilmesin de bilişim alanına yönelebilmeye ilişkindir.

Söz konusu kanun düzenlemelerinin yanı sıra aşağıda yer alan ve çok fazla ayrıntıya yer verilmemiş yönetmelik hükümleri bulunmaktadır.

Adlî ve Önleme Aramaları Yönetmeliği[153] *"Madde **17** - Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir. Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır. İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir."*

[153] http://www.resmigazete.gov.tr/eskiler/2005/06/20050601-15.htm Erişim 15.11.2014

Ayrıca el konulan delillerin ne şekilde muhafaza edilmesi gerektiği konusunda Suç Eşyası Yönetmeliği Madde 9/2. fıkrasının bulunmaktadır[154]. *"Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir."*

Tüm bunlar ile birlikte Türkiye Cumhuriyeti Devleti'nin imzaladığı ve onay kanunu çıkartması sebebi ile iç hukuk bakımından bağlayıcılığı bulunan Siber Suçlar Sözleşmesi'nde uygulanmaktadır. Söz konusu Uluslararası sözleşme siber suçlar ile mücadele edilebilmesi açısından taraf devletlerin yeknesak iş birliği ve kendi iç hukuklarını bu şartlara uydurmalarını düzenlemektedir. Bilişim sistemlerine arama ve el koyma hususunda sözleşmenin 19. Maddesinde hükümler bulunmaktadır. Siber Suçlar Sözleşmesi Madde *"19[155]; Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara El Konulması*

1. Taraflardan her biri kendi ülkesindeki yetkili makamların;

a) Bir bilgisayar sisteminin tamamının veya bir kısmını ve içerisinde depolanmış bilgisayar verilerini; ve

b) Bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtını arama ve benzer şekilde bunlara erişme yetkisine sahip olmalarını için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

2. Taraflar her biri paragraf 1a uyarınca makamlarının özel bir bilgisayar sisteminin tamamını veya bir kısmını araması veya benzer şekilde bunlara erişim sağlaması söz konusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğunda inanmak için gerekçeleri bulunduğunda ve söz konusu veriler yasalara uygun biçimde ilk sistemden erişebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama ve diğer tedbirleri kabul edecektir.

---

[154] http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.8200&sourceXmlSearch=&MevzuatIliski=0 Son Erişim 15.11.2014

[155] http://www2.tbmm.gov.tr/d24/1/1-0676.pdf Son Erişim 15.11.2014

3. Taraflardan her biri, yetkili makamlarına, paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koymaya veya benzer güvence altına almaya yetki tanımak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Bu tedbirler:

a) Bir bilgisayar sisteminin tamamına veya bir kısmına veya bilgisayar verileri depolama aygıtına el koymaya veya bunları benzer şekilde güvence altına almaya;

b) Söz konusu bilgisayar verilerin bir kopyasını oluşturmaya ve bunu muhafaza etmeye;

c) İlgili depolanan verilerin bütünlüğünü korumaya;

d) Erişim sağlanan bilgisayar sistemindeki bilgisayar verilerini erişilemez hale getirmeye veya kaldırmaya yönelik yetkileri içerecektir.

4. Taraflardan her biri paragraf 1 ve 2'de belirtilen tedbirlerin tatbik edilmesine olanak sağlanması amacıyla kendi yetkili makamlarına bilgisayar sisteminin işleyişi veya içerisindeki bilgisayar verisinin korunması için uygulanan tedbirler hakkında bilgisi olan herhangi bir kişiden makul ölücüde gerekli bilgileri temin etme konusunda yetki tanınması için gerekli olabilecek yasama tedbirleri ve diğer tedbirleri kabul edecektir.

5. İş bu maddede atıfta bulunan yetki ve usuller madde 14 ve 15'e tabi olacaktır.

Yürürlükte bulunan Adli Arama Yönetmeliği Madde 17 incelendiğinde CMK 134'ün tekrarı niteliğinde olduğu görülmektedir. Bu halde; ilgili yönetmeliğin getirdiği bir fayda bulunmamaktadır. Burada kanun maddesine aykırı olmamak ve çok aşırı genişletmemek kaydı ile CMK 134'ün ne şekilde uygulanması gerektiği ayrıntılı olarak belirlenmelidir. Ancak bu sayede, Türkiye genelinde adli kolluk birimleri tarafından yeknesak bir uygulamaya gidilebilir. Aynı şekilde Suç Eşyası Yönetmeliği madde 9'un genişletilmesi, uluslar arası standartlar çerçevesinde dijital delillerin muhafazasının ne şekilde yapılması gerektiği detaylandırılmalıdır.

C- Bilişim sistemlerinde arama, kopyalama ve el koyma işleminin şartları

Bilişim sistemlerine karşı veya bilişim sistemleri kullanılmak suretiyle bir suç işlendiğinde yapılması gereken en önemli işlemlerden biri söz konusu sistem üzerinde inceleme yapmaktır. Ancak bu inceleme yapılırken tıpkı ev veya iş yerlerinde yapılan aramalar gibi bir yasa normuna dayanılarak yapılması gerekmektedir. Zira bu temel hak ve özgürleri kısıtlayan bir işlemdir. Aksi halde keyfi ve hukuksuz uygulamaların gerçekleşmesi

kaçınılmazdır. Bu ise hem maddi gerçeğin ortaya çıkarılmasına zarar verecek hem de elde edilen deliller gerçeği yansıtsa da hukuka aykırı elde edildiği için yasak delil olacak ve soruşturmada ve kovuşturmada hükme esas teşkil etmeyecektir[156]. Bu sebeple; söz konusu kanun metninden yola çıkılarak gerçekleştirilecek soruşturmalarda savcılık makamının ve adli kolluğun Kanun'un amir hükümlerine uygun hareket etmesi gerekmektedir.

1. Suç dolayısıyla yürütülen bir soruşturmanın bulunması

CMK'nın 134. Maddesinin 1. fıkrası **"*(1) Bir suç dolayısıyla yapılan soruşturmada*** *(Ek ibare: 6526 - 21.2.2014 / m.11) "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve" , başka surette delil elde etme imkanının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine hakim tarafından karar verilir."*

Bu halde CMK'nın 134. Maddesinin uygulanabilmesi için Kanun'un tarif ettiği amir hükmü gereğince ortada öncelikle bir suç dolayısı ile var olan bir soruşturma olmalıdır. Bir başka ifade ile soruşturması tamamlanmış ve kovuşturma aşamasında gelmiş dosyada, artık CMK 134/1 gereğince arama ve el koyma kararı verilemeyeceği anlaşılmaktadır. Burada kanun koyucu bilinçli bir şekilde, soruşturma aşamasına vurgu yapmıştır. Burada soruşturma ne zaman başlamış sayılır sorusu akla gelebilir. CMK'nun 2. Maddesinde *"Soruşturma: Kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi[157]"* tanımından anlaşılacağı gibi söz konusu sürenin başlangıcı yetkili mercilerce suç şüphesinin öğrenilmesi ve/veya şikayete tabi suçlar açısından mağdur yada yakınanın durumu yetkili mercilere bildirmesi ile başlayacaktır. Bir başka husus ise kovuşturma aşamasına gelindiğinde, sanığa ait bir bilişim sisteminin CMK 134 gereğince el konularak tekrardan analiz edilmesi teknik açıdan maddi gerçeğe ulaşabilmek adına sıhhatli olmayacaktır. Zira o aşamaya kadar sanık kendi aleyhine olacak delillerden kurtulmuş olabilme veya mahkemeye farklı bir delil sunma ihtimali vardır.

[156] DÜLGER Volkan Murat, 2012 s 656.

[157] www.kazanci.com Son Erişim 18.02.2015

Ancak kovuşturma aşamasında mağdurun veya sanığın rızası ile bilişim sistemleri üzerinde inceleme yapılabilmesi hukuken mümkündür[158].

2. Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı

CMK'nın 134. Maddesinin 1. fıkrası "*(1) Bir suç dolayısıyla yapılan soruşturmada (Ek ibare: 6526 - 21.2.2014 / m.11)* ***"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*** *ve" , başka surette delil elde etme imkanının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine hakim tarafından karar verilir."*

Buna göre kanun koyucu; CMK md. 116'da aranan makul şüpheden farklı olarak daha katı ve sert bir şartın var olması gerektiğini belirtmiştir. Bu bağlamda Yasa Koyucu, CMK md. 134'ün uygulaması bakımından kuvvetli şüphe aranması gerektiği yönünde tercihini açık bir şekilde ortaya koymuştur.

Tedbire karar verilebilmesi için ayrıca kuvvetli şüphenin somut delillere dayandırılması gerekmektedir. Burada somut delilden kanun koyucunun kastının ne olduğu açıklanmalıdır. Somut delil, soruşturma konusu suça ilişkin mi olacak, yoksa CMK md.134 gereğinde karar verebilmek için şüphelinin kullandığı bilişim sisteminde delil bulunabileceğine yönelik mi olacaktır. TBMM Adalet komisyonu Raporu'nda da haklı olarak ifade edildiği üzere somut delil, ancak suçla ilgili olabilecektir[159].

Soruşturma makamının arama ve el koyma kararı verebilmesi için kanun maddesi gereğince, soruşturma yapılan suçun, şüpheli/ler tarafından işlendiğine ilişkin kuvvetli şüphe ve somut deliller bulunması gerektiğidir. Örneğin; bir soruşturmada mağdurun bilişim sistemlerine girildiği ve müşteri bilgilerinin çalındığını ve aynı zamanda şirkete şantaj mailleri atıldığını düşünelim. Adli kolluk tarafından yapılacak ilk analiz sonrasında mağdurun bilişim sistemi üzerinde tespit edilen IP numarası ile şirketin mail sunucularında tespit edilen IP numarası ve ilgili hizmet sağlayıcının verdiği abonelik bilgilerinin aynı kişiye ait olduğunun

---

[158] http://www.hukukihaber.net/e-posta-takibi-ve-cmk-m134un-kapsami-makale,3524.html Son Erişim 18.02.2015 " E-Posta Takibi ve CMK m.134'ün Kapsamı" Prof. Dr. Ersan ŞEN

[159] DEĞİRMENCİ Olgun, 2014 s 352.

tespiti halinde, artık suçun o fail/ler tarafından işlendiğine ilişkin somut delillerin bulunduğu ve bu sebeple, failin kullandığı bilişim cihazları üzerinde suçun %100 kimin tarafından işlendiğinin ortaya çıkabilmesi için CMK 134 gereğince arama ve el koyma kararı verilmesi mümkün olabilecektir.

Ancak bu şartların her soruşturma dosyasında mevcut olması ihtimali hemen hemen imkansızdır. Zira bilişim sistemleri aracılığı ile işlenen suçların yapısı gereğince somut delile ulaşılması bir hayli sıkıntılıdır. Çoğu zaman suç işlendikten sonra faile ulaşılması aşamasında soruşturma aşamasının elinde tek bir IP numarası bulunmaktadır. Bu halde; söz konusu arama ve el koyma tedbirinin uygulanması için somut deliller ve kuvvetli şüphe şartının aranması yerinde değildir. Ceza Mahkemesi'nde kuvvetli şüphenin arandığı diğer koruma tedbirlerine bakıldığında, (Gözaltı kararı, Tutuklama Kararı, İletişimin Tespiti, Taşınmazlara hak ve alacaklara el koyma) gibi tedbirlerin kişinin Temel Hak ve Hürriyetini açıkça sınırlandıran işlemler olduğu görülmektedir. Burada; şüphesiz bir kimsenin bilişim sistemine, cihazlarına el koyulması temek hak ve özgürlüklerini kısıtlayan bir işlemdir. Ancak Ceza Muhakemesi Kanun'un kuvvetli şüphe sebebinin varlığını aradığı diğer koruma tedbirlerinin sistematiği gereğince aynı şartlar açısından CMK 134'ün uygulanmasının ağır olduğunu düşünülmektedir. Burada kanımızca CMK 134 maddesinde yeni bir düzenleme yapılarak, yapılan suç soruşturmasında *makul şüphenin* bulunduğu durumlarda, şüphelinin bilişim sistemlerinde *arama ve kopya çıkartma* kararı verilebilmeli, ancak somut delillere dayanan kuvvetli şüphenin var olduğu durumlarda ise *arama ve el koyma* kararı verilebileceğine ilişkin düzenlenme yapılmalıdır. Aksi halde; mevcut durumda, soruşturma aşamasında benzer suç tiplerinde somut delillere dayanan kuvvetli şüphenin olması ihtimalinin bir hayli az olması sebebi ile verilecek çoğu arama ve el koyma kararları hukuka aykırı olacaktır.

a) Şüphe kavramı

Şüphe kelimesinin anlamı zihnin birçok düşünce arasında bir tercih yapmasında duraksamasıdır. Buna göre bir kanıyı destekleyen nedenler karşıt kanıyı destekleyen nedenlerle eşit değerde olunca veya bize eşit değerde görününce, bu nedenler arasında seçim yapamaz, ortada kalırız; yani şüphe duyarız[160]. Ceza muhakemesi hukukunda söz konusu olan şüphe ise, soruşturmanın başında, yetkililerin delillere dayanan bir tahmininden ibarettir. Demek oluyor ki, hukuk devleti ilkesi esasları çerçevesinde yapılan bir ceza muhakemesinde

[160] KAPILI Kübra, s 16.

delil olmadan şüpheden söz edilemez; o halde delil olmaya ceza muhakemesinin çarkları dönmeye başlayamaz; hiçbir ceza muhakemesi işlemi yapılamaz. Çünkü bir ceza muhakemesi yapılmasının ve böyle bir ceza muhakemesinin varlık sebebi suç şüphesidir. Bir hukuk devletinde böyle bir şüphe ancak delillere tarif edilebilir[161].

Şüphenin içerisinde daima yanılma payı vardır. Yanılma payının derecesine göre şüphe, basit, makul, yeterli veya kuvvetli olur. Muhakemenin değişik aşamalarında değişik işlemlere göre şüphenin de yoğunluğu değişmektedir[162].

b) Şüphe türleri

aa) Basit şüphe

Soruşturmayı başlatan şüphe olmasından dolayı başlangıç şüphesi olarak da bilinir. Basit şüphe dayandığı deliller basit, yetersiz ve/veya sayıca az olan şüphedir. Soruşturmaya başlanabilmesi için, belli ve yaşanmış somut olayların, en azından belirti şeklinde ortada bulunan delillerin belli bir suçun işlendiği yolunda bir şüphe ortaya koyması şarttır. Belirli olaylara ve belirti şeklindeki delillere dayanmayan ve sadece tahminden ibaret bulunan şüphe soruşturmaya başlanabilmesi için yeterli değildir; yeterli sayılırsa keyfiliğin önlenebilmesi mümkün olmaz.

bb) Makul şüphe

5271 Sayılı Ceza Muhakemesi Kanunu ile ceza muhakemesi hukukuna girmiş olan makul şüphe kavramından kanunun 116. Maddesinde şu şekilde bahsedilmiştir;

"Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir."

Makul şüphe tanımına ise Adli ve Önleme Aramaları Yönetmeliği'nin 6. Maddesinde yer verilmiştir. Yönetmeliğe göre makul şüphe;

"Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir. Makul şüphe, aramanın yapılacağı zaman, yer ve ilgili kişinin veya onunla birlikte

[161] ÖZTÜRK Bahri, s 538-539

[162] CENTEL Nur - ZAFER Hamide, s 76.

olanların davranış tutum ve biçimleri, kolluk memurunun taşındığından şüphe ettiği eşyanın niteliği gibi sebepler göz önünde tutularak belirlenir. Makul şüphede, ihbar veya şikâyeti destekleyen emarelerin var olması gerekir. Belirtilen konularda şüphenin somut olgulara dayanması şarttır. Arama sonunda belirli bir şeyin bulunacağını veya belirli bir kişinin yakalanacağını öngörmeyi gerektiren somut olgular mevcut bulunmalıdır."

cc) Yeterli şüphe

Ceza Muhakemesi Kanunu'nun 170. Maddesinin 2. Fıkrası şu şekildedir; "Soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturuyorsa; Cumhuriyet savcısı, bir iddianame düzenler." Kanundan da anlaşılacağı üzere bir kamu davasının açılabilmesi için yeterli şüphenin varlığı aranmaktadır.

Mevcut delillere göre yapılacak muhakemede sanığın mahkum olması ihtimali beraat etmesi ihtimalinden daha kuvvetli ise yeterli delilden veya başka bir anlatımla yeterli şüpheden söz edilir[163].

dd) Kuvvetli şüphe

Somut delillere nazaran, yapılacak bir duruşmada sanığın mahkum olması kuvvetle muhtemel ise, kuvvetli şüphe var demektir[164].

Ceza Muhakemesi Kanunu'nun koruma tedbirlerine ilişkin maddelerini incelediğimizde karşımıza genellikle kuvvetli şüphenin koruma tedbirleri için bir ön şart niteliği taşıdığını görmekteyiz. (bkz. Md.74, 100, 128, 133, 134 135, 139, 140) Tez konumuz olan bilişim sistemleri üzerinde arama ve el koymaya ilişkin olarak CMK 134'te de 6526 sayılı kanun ile değiştirilmesi sonrasında somut delillere dayanan kuvvetli şüphe sebebinin varlığı aranması gerekmektedir. Kanun koyucunun, bilgisayar ve sair donanımlarda arama yapılmasında kuvvetli şüphe sebebini araması teorik olarak çok katı kurallara bağlandığı yorumlanmaktadır. Ancak bu maddenin uygulama aşamasında getireceği sonuçlar bir hayli tartışmalıdır. Zira bilişim sistemleri aracılığı ile işlenen suçlarda her zaman soruşturma aşamasında ilk etapta somut delillere ulaşabilmek imkansızdır. Bu tür suçlarda en kuvvetli delil gibi gözüken emare IP numarasıdır. Bir başka ifade ile soruşturma aşamasında çoğu

[163] ÖZTÜRK Bahri, s 540.

[164] CENTEL Nur - ZAFER Hamide, s 79.

zaman bir IP adresinden yola çıkarak devam etmektedir. Hali ile sadece tespit edilen bir IP numarası başlı başına faili işaret etmeyecektir. Daha doğru bir ifade ile bu IP numarasının yan deliller ile de doğrulanması sonrasında somut delilin varlığından söz edilebilir.

3. Başka surette delil elde etme imkanının bulunmaması

CMK'nın 134. Maddesinin 1. fıkrası "*(1) Bir suç dolayısıyla yapılan soruşturmada (Ek ibare: 6526 - 21.2.2014 / m.11)* ***"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*** *ve" , başka surette delil elde etme imkanının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine hakim tarafından karar verilir."* denilmektedir.

Buna göre bilişim sistemlerinde delil elde etmek için araştırma yapılabilmesi için öncelikle "başka surette delil elde etme imkanın bulunmaması" gerekmektedir. Şayet bu şart gerçekleşmeden arama kararı verilmiş ise bu açıkça hukuka aykırı olacaktır. Başka surette delil elde etme imkanının neden bulunmadığı ve bu yola başvurulmasının sebebi hem savcılık talep yazısında hem de mahkeme kararında açıkça belirtilmelidir. Tabi böyle bir şartın uygulama açısından yaratabileceği sıkıntılar üzerinde de durmak gerekmektedir. Nitekim bu tür suçlarda suçun niteliği gereğince tüm deliller bilişim sistemleri üzerindedir. Bilişim sistemleri üzerinde bulunan veriler çabuk yok olmaya veya manipülasyona uğramaya müsaittir. Bu halde soruşturma makamının bir an evvel delillere ulaşması gerekmektedir. Bu durumda ilk olarak bilişim sistemleri üzerinde arama yapmak yerine diğer yan delilleri toplamaya yönelmesi soruşturmanın gidişatını ve özellikle maddi gerçeğe ulaşılması açısından oldukça zorlayacaktır[165].

Bu sebeple; öğretide bir kısım yazarlar bazı suç tiplerinde "TCK'nın bilişim alanında suçlar bölümünde 135 Kişisel Verilerin Kaydedilmesi, 136 Verileri Hukuka aykırı olarak verme veya ele geçirme, 138 Kişisel Verileri Yok Etmeme, 142/2-e Bilişim sistemleri aracılığı ile hırsızlık ve 158/1-f bilişim sistemleri aracılı ile işlenen dolandırıcılık suçları açısından bu unsurunun aranmaması gerektiğini belirtmektedirler[166].

[165] DÜLGER Volkan Murat, 2012 s 657.

[166] DÜLGER Volkan Murat, 2012 s 657.

Bir diğer görüşe göre Kanun'un bu maddesinin çok dar yorumlanmaması olayın ve soruşturmanın yeterince delil elde edilmemesi olarak anlamak gerekmektedir. Aksi dar yorum, devam eden soruşturmada zayıfta olsa dosyada bulunan bir delil nedeniyle artık başkaca bilişim sistemlerinde arama ve el koyma kararı verilemeyeceği anlamına geleceği ve bunun da kanun koyucu tarafından amaçlanmadığı belirtilmiştir[167].

Söz konusu kanun metninde açıkça belirtildiği üzere başka suretle delil etme imkanın bulunmaması gerekmektedir. Bu tür soruşturmalarda suçun niteliği gereğince, soruşturma makamı tarafından değer delillerin tüketildikten sonra bu yönteme başvurulması soruşturmanın sıhhatini ciddi şekilde etkileyecektir. Çünkü; Ceza hukukunda bir sanığın iddia olunan suçtan dolayı cezalandırılabilmesi için hukuka uygun deliller ile suçun işlendiğine ilişkin %100 ispat aranmaktadır. Soruşturma aşamasında, bu tür suç tiplerinde bilişim sistemleri ise, suçun kimin tarafından işlendiğine ilişkin en önemli kati delillerin bulunabileceği alanlardır. Bu halde; soruşturma makamı suçun aydınlatılmasında, CMK 134'te belirtilen şart gereğince, son aşamada dijital delillerin tespitine yönelmesi durumunda delillerin yok olması ile karşı karşıya kalabilecektir. Örneğin; Sosyal ağlar aracılığı ile gerçekleştirilen hakaret, tehdit ve şantaj suçlarına ilişkin olarak; müşteki tarafından yapılan savcılık şikayeti sonrasında, bilişim şube tarafından şüpheli tespiti üzerine, soruşturma makamı önce şüphelinin ifadesine sonrasında ise CMK 134 gereğince arama ve el koyma tedbirine yönelmesi durumunda tüm delillerin yok olma ihtimali ile karşı karşıya kalabilecektir. Bu durumda; şüphelinin ifadesinin alınmasından önce bilişim cihazlarında uygulanacak bir arama, kopya çıkartma ve el koyma kararı sonucunda suça konu delillere ulaşılabilecektir. Ancak mevcut hukuki düzenlemeler ışığında, soruşturma makamının hiçbir delil araştırma yöntemine başvurmadan doğrudan CMK 134 gereğince arama ve el koyma işlemi için hakimde talepte bulunması açıkça hukuka aykırı olacaktır.

4. Cumhuriyet savcısının istemi ve Hakim kararı olması

CMK'nın 134. Maddesinin 1. fıkrası "*(1) Bir suç dolayısıyla yapılan soruşturmada (Ek ibare: 6526 - 21.2.2014 / m.11) "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve" , başka surette delil elde etme imkanının bulunmaması halinde,* ***Cumhuriyet savcısının istemi üzerine*** *şüphelinin kullandığı bilgisayar ve bilgisayar programları ile*

[167] TANRIKULU Cengiz 2014 s 390.

bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine ***hakim tarafından karar verilir.”*** denilmektedir.

Bilişim sistemlerinde arama, kopyalama ve el koyma tedbirine karar verebilecek merci mahkemedir. İlgili kanun maddesi hükmü açık bir şekilde kararın hakim tarafından verilebileceği belirtmiştir. Buna ilişkin herhangi bir istisnai durum belirtmemiştir. Bir başka ifade ile gecikmesinde sakınca bulunan hallerde savcılık veya adli kolluk kendi aldığı karar ile bir kimsenin bilişim sistemleri üzerinde arama ve el koyma tedbiri uygulayamaz.

Bununla birlikte Kanun maddesinde belirtildiği üzere tedbir kararının verilebilmesi için Cumhuriyet Savcısının istemi bulunmalıdır.

5. Şifrenin çözülememesinden dolayı bilgisayara girilememe veya gizlenmiş bilgilere ulaşılamama hallerinden birisinin varlığı

CMK’nın 134. Maddesinin 2. Fıkrası *“(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere* ***elkonulabilir****.* ***Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.”*** denilmektedir.

Bu halde; CMK 134 gereğince adli kolluğun olay yerinde bilişim sistemlerinin şifrelenmiş olması veya gizlenmiş bilgilere ulaşamaması halinde tüm araç ve gereçlere el koyabilecektir. Ancak uygulamada hem donanımsal yetersizlikler hem de fiziki imkanlardan ötürü çoğu arama kararlarında bilişim sistemlerine el koyulmakta ve şube müdürlüklerinde incelemeleri yapılmaktadır. Lakin burada Kanun’un amir hükmüne aykırı davranıldığının tespiti halinde elde edilecek delillerin hukuka aykırı delil statüsünde olması gerekmektedir. Bir başka ifade ile olay mahallinde, bilişim sistemlerine el koyma uygulanmasını gerektirmeyecek hallerde, adli kolluk tarafından el koyma kararı uygulanması durumunda elde edilecek delillerin akıbetinin tartışılması gerekmektedir. İlgili kanun maddesinde yer alan düzenleme maalesef somut olay üzerinde uygulanması durumunda, bazı hallerde yoruma açık ve adli kolluğun takdirine bırakabilecek durumlar ortaya koyabilecektir. Özellik bilişim sistemleri üzerinde gizlenmiş bilgilerin bulunması ihtimali her olayda adli kolluğun karşına çıkabilecek bir durumdur. Bu halde; adli kolluk tarafından el konulma işlemi yapılmak istendiği takdirde, el konulacak bilişim sistemi şifrelenmiş olmasa bile, bir takım verilerin

gizlenmiş olması ihtimaline binaen kolluk tarafından bir gerekçe oluşturulması halinde, mahkemenin el koyma kararı uygulanması, hukuka aykırılığı ortadan kaldıracaktır.

Bir diğer husus ise ilgili maddeden çok açık bir şekilde anlaşılacağı üzere bilişim sistemlerine arama ve el koyulmasına ilişkin kararlarda, **ana kural kopyalama yapılması, istisna ise el koymanın uygulanmasıdır**. Ancak olay mahallinde, adli kolluğun canlı sistemler üzerinde bir başka ifade ile çalışır durumda olan bilişim sistemleri ile karşılaşması halinde ne şekilde davranması gerektiği konusunda hukuki düzenleme bulunmamaktadır. Halbuki yeni gelişen teknolojik gelişmeler ışığında artık bir çok veri, bilişim sistemlerinde geçici kayıt tutan *"RAM"* üzerinde bulunmaktadır. Bu halde; canlı sistemler üzerinde analizin yapılması gerektiği durumlarda, adli kolluğun olay anında inceleme yapmak yerine sistemini çeşitli yöntemler ile kapatması durumunda çok ciddi veri kaybı yaşanabileceği kuşkusuzdur. Burada yapılması gereken soruşturma konusu olayın özelliğine göre olay mahallinde canlı sistemler mevcut ise gerekli ekipman ve donanım ile gidilerek analizin çalışır durumdaki sistem üzerinde yapılmasıdır.

6. El koyma işlemi sırasında sistemdeki verilerin yedeklemesinin yapılması

CMK'nın 134. Maddesinin 3. Fıkrası "*(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır."* denilmektedir.

Madde metninden açıkça anlaşılacağı üzere, bilişim sistemlerine **el koyma işlemi sırasında** sistemdeki bütün verilerin bir yedeğinin alınması zorunlu tutulmuştur. Bir başka ifade ile bilişim sistemlerine el koyma işleminin yapıldığı an itibarı ile sistemdeki yedeklerin bir kopyası çıkartılması gerekmektedir. Olay mahallinde canlı sistemler bir başka ifade ile çalışır durumda bulunan bilişim sisteminin bulunması durumunda ise ne şekilde bir yol izlenmesi gerektiği belli değildir. Canlı sistemler üzerinde bulunan veriler, teknik açıdan bilişim sisteminin kapatılması veya enerji kaynağının çekilmesi durumunda yok olma tehlikesi ile karşı karşıya kalabilir. Bu durumda adli kolluk canlı bir bilişim sistemi ile karşılaşması durumunda, mevcut ekipmanı ile sistemin çalışır durumda bir yedeğini alması daha sıhhatli olacaktır. Kanun koyucu bununla ilgili bir ayrım yapmamıştır. Bu halde; ister canlı sistemler ister kapalı sistemler olsun el koyma işlemi sırasında sistemdeki verilerin yedeklemesi olay mahallinde yapılması gerekmektedir. Maalesef Kanun maddesinin bu hükmü uygulama aşamasında usule uygun bir biçimde kullanılmamaktadır. Özellikle teknolojik gelişmeler ışığında sistem kapasitelerinin artması ve olay mahallinde, çok ciddi

kapasiteli bilişim sistemlerine el konulacak olması dolayısı ile kimi yedeklemelerin günlerce sürecek olması sebebi ile tüm işlemler adli kolluk merkezlerinde yapılmaktadır. Bunun haricinde, yedekleme işlemini gerçekleştirecek kalifiye personelin yeterli sayıda istihdam edilmemesi ve kimi zaman el koyma işlemini uygulamaya gelen adli kolluk personelinin teknik kapasitesinin bulunmaması sebebi ile de sistem verilerin yedeklemesi yine kanuna aykırı bir biçimde merkezlerde gerçekleştirilmektedir. Olay mahalline gidildiğinde, hangi kapasitede ve kaç adet bilişim sistemi ile karşılaşılacağı bilinmediğinden, bazı durumlarda donanımsal sıkıntılar yüzünden el koyma işlemi sırasında verilerin yedeklemesi alınmamaktadır. Bu ve buna bağlı sebepler uygulama kısmında daha da arttırılabilmektedir. Ancak hangi sebep gösterilir ise gösterilsin, mevcut kanun maddesi gayet sarihtir. Bu sebeple; el koyma işleminden sonra sistem verilerinin yedeklemesi yapılması hukuka aykırılık teşkil edecektir.

Bir başka sorun ise el koyma işlemi sırasında yedekleme yapılırken hangi kriterlere uyulması gerektiğidir. Kanun koyucu gerek CMK 134'te gerekse yönetmeliklerde belirtilen bir program veya usul öngörmemiştir. Adli kolluk birimlerinin olay mahallinde kullandığı donanımların hangi sertifikasyonlardan geçtiği veya uluslararası açıdan uygun olduğu belirtilen yedekleme programlarının Türk Kanun koyucusu tarafından hangi kriterlerde kabul edileceği hususları şu an için düzenlemenin ayrıntılı olarak bulunmadığı noktalardır. Bu sebeplerle; ilgili Kanun maddesi haricinde bir yönetmelik veya tebliğ çıkartılarak veya Adli Arama ve Önleme Arama Yönetmeliği'nin 17. Maddesinin geliştirilerek, Türkiye genelinde bu tür suçlar sebebi ile verilen arama ve el koyma kararlarında Adli Kolluğun; olay yeri öncesinde hazırlık aşamasında yapması gerekenler ile olay mahallinde kullanması gereken donanımlar ve programların neler olabileceği, söz konusu donanımların ve programın neden tercih edildiği ayrıntılı bir şekilde belirtilerek yeknesak bir uygulamaya gidilmesi gerekmektedir.

Mevcut hukuki düzenlemeler ışığında, bu tür suçlar sebebi ile yapılan yargılamalarda, Mahkemeler tarafından aranacak kriter ise delillerin hukuka uygun yöntemler ile ele geçirilip, geçirilmediği ve yedeklemesi alınan verilerin dijital bütünlüğüne zarar gelip gelmediği hususudur. Dijital delilin bütünlüğüne herhangi bir zarar gelmediğinin ispatı ise teknik açından zaman damgalı HASH[168] ile ispatlanabilmektedir. Gerek Ceza Muhakemesi Kanunu

[168] Bkz. Birinci Bölüm §V.E.

gerekse de Adli Arama ve Önleme Arama Yönetmeliği'nde dijital delillere el konulurken hash değerinin alınması gerektiği hususunda **herhangi bir düzenleme yoktur**. Uygulamada ise adli kolluk tarafından kullanılan programın özelliğine göre çeşitli algoritmalar ışığında zaman damgalı bir şekilde verinin elektronik olarak değiştirilmediğini ispatlayacak hash algoritmasını almaktadır. Bu sayede; kovuşturma aşamasında, sanık tarafından dijital delillerin manipülasyona uğradığı iddiası sonucunda oluşacak şüphe bertaraf edilebilmektedir. Her ne kadar kanuni düzenleme açısından bir zorunluluk bulunmasa da Yargıtay vermiş olduğu bir kararında HASH değerinin önemi üzerinde durmuştur. T.C. Yargıtay 11. Ceza Dairesi 'sinin E. 2005/6376 K. 2007/2551[169] sayılı kararı ile *"Gerçeğin kuşkuya yer vermeyecek şekilde belirlenebilmesi için; öncelikle e-posta yoluyla virüs gönderilerek sistemine zarar verilmiş bir bilgisayarda incelemenin olaydan hemen sonra yapılması yada inceleme yapılacak bilgisayarın olaydan sonra inceleme anına kadar hiç kullanılmamış olması; bilgisayarda virüslü dosya üzerinden inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir yedeğinin alınması, ikinci olarak birebir yedeğin değiştirilip değiştirilmediğinin tespitine yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi; bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen İP adresinin bulunması, daha sonra da bulunan İP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin talep edilmesi, bulunan İP adresini kullanan abonenin sanıkla bağlantısının araştırılarak tespiti gerekir."* Şeklinde yer alan Yargıtay içtihadı ile bilişim sistemleri aracılığı ile işlenen suçlarda dijital delillerin, delil bütünlüğünün korunması için Zaman damgalı HASH değerlerinin alınması gerektiği hususu belirtilmiştir. Bu sebeple; uygulamada artık adli kolluk çeşitli programlar vasıtası ile kopyalama sırasında delilleri bir nevi mühürleyerek zaman damgalı hash değerini almaktadır.

7. Bilişim sistemlerine arama ve el koyma işlemi sırasında hard diskin bire bir kopyasının şüpheliye veya vekiline verilmesi

CMK'nın 134. Maddesinin 4. Fıkrası **"***(Değişik ibare: 6526 - 21.2.2014 / m.11) "Üçüncü fıkraya göre alınan" yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır*[170]*."* denilmektedir. 5271 sayılı Ceza

[169] www.kazanci.com (Son Erişim: 16.02.2015)

[170] www.kazanci.com Son Erişim 01.03.2015

Muhakemesi Kanun'un 134. Maddesinin 4. fıkrasında 21.02.2014 tarihinde 6526 sayılı kanun ile söz konusu düzenleme yapılmıştır. Düzenleme öncesinde, CMK 134/4 *"İstenmesi halinde yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır*[171]*."* Şeklindedir. Bir önceki kanun metninde isteğe bağlı olan bu husus yeni yapılan değişiklik ile artık zorunlu hale getirilmiştir. Böylece bilişim sistemlerine el koyma kararı uygulanırken, sistem verilerinin yedeklemesinden en az 2 adet yapılması gerekmektedir. Bu durumda bir kopyanın da soruşturma aşamasında delillerin değiştirildiği iddiasında bulunmaması açısından şüpheli veya vekiline verilmesi gerekmektedir. Ancak burada bir diğer sorun çok ciddi kapasitelere sahip olan bilişim sistemleri üzerinde yapılan yedekleme esnasında donanımın kim tarafından karşılanacağıdır. Kanun koyucu bununla ilgili bir düzenleme yapmamıştır. Ortada bir Ceza Soruşturması bulunması sebebi ile ve yedeğin şüpheli veya vekiline verilmesinin zorunlu olmasından dolayı gerekli donanımı soruşturma makamı sağlamak zorunda olacağı kanaatindeyim. Zira kanun koyucu tarafından artık el konulan verilerin bir yedeğinin şüpheli veya vekiline verilmesi hususu el koyma işleminin sıhhatini de etkiyecektir. Bu sebeple; adli kolluk tarafından el koyma işlemi sırasında alınan verilerin bir yedeğinin şüpheli veya vekiline verilmemesi durumunda mutlaka muvafakat yazısı alınması gerekmektedir.

Burada tartışılması gereken en büyük sorun el konulan ve yedeği alınan verilerin suç unsuru taşıması halidir. Bazı hallerde, CMK 134 gereğince el konulan verilerin başlı başına suç unsuru taşıması, bulundurulmasının suç olduğu durumlar olabilir. Bu halde; el konulan verilerin bir yedeğinin şüpheliye veya vekili verilmesi suçun önlenmesi açısından sıkıntı yaratabilecektir. Elde edilen verilen ayrı bir suç olduğunun tespiti halinde izlenecek yol CMK *"Md. 138/1 Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhal bildirilir."* gereğince soruşturma makamına bildirilerek konuya ilişkin ayrıca bir tahkikat yapılması sağlanarak mevcut delilin hukuka uygun hale getirilmesi sağlanabilir. Bunun haricinde ise yedeği alınan ve bulundurulması dahi suç teşkil edecek verinin şüpheliye bir örneğinin verilmesi konusunda sınırlı yasal düzenlemeler gereğince bir çözüm bulunabilir. Öncelikle belirtmek gerekir ki hakkında soruşturma yapılan bir kimsenin aleyhine teşkil edecek delillerin tespit edilmesi ve el koyulması aşamasında savunma yapılabilmesi ve delillerin güvenirliği için şüpheli tarafından da bilinmesi gayet olağandır.

[171] www.kazanci.com Son Erişim 01.03.2015

Zira soruşturma sonrasında, yargılama aşamasına geçildiğinde tüm delillerin alınması serbest olacaktır. Nitekim bu sayede sanık hakkındaki iddiaları görerek savunması gerçekleştirecektir. Soruşturma aşamasında ise CMK 134 gereğince el koyulan delillere suç eşyası müsaderesi şartları gereğince el konulup konulmayacağı hayli tartışmalıdır. Eğer bu şekilde, dijital deliller suç eşyası müsaderesi şeklinde bir el koyma işlemi uygulanır ise CMK 134/4. Fıkrasında yer alan amir hüküm uygulanamayacaktır. Doktrinde ise tartışmaların aynı mahalde yapıldığı görülmektedir. Buna göre mevcut durumun *"CMK md.123 (1) İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır."* ve *CMK md. 127 1) Hakim kararı üzerine veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri, elkoyma işlemini gerçekleştirebilir."* mi, yoksa CMK Md. 134 gereğince uygulanması gerektiği üzerinde durulmaktadır. Bilişim sistemlerinde yer alan verilerin konusunun bizzat suç teşkil etmesi halinde CMK md.134'ün uygulanması gerektiği çünkü bu söz konusu maddenin, bilişim sistemleri aracılığı ile işlenen suçlar bakımından özel bir düzenleme olduğu ve özel bir düzenleme olması münasebeti ile ilgili kanun maddesinin uygulanması gerektiği belirtilmektedir. Bunun karşısında, bilişim sistemleri aracılığı ile işlenen suçlarda el edilen verilerin konusunun suç teşkil ettiği durumda CMK m.134'ün uygulanması yerine, CMK m.123, 127 ve bu kapsamda 138/1'in uygulanması gerektiği ve yargılama sonucunda TCK md.54'ün şartlarının oluştuğunun tespiti kaydıyla kasıtlı suçun işlenmesinde kullanılan veya suçun işlenmesine vasıta olarak bilişim cihazı yönünden müsadere kararının verilmesi gerektiği görüşü ortaya koyulmaktadır[172]. Ancak bu görüşe tam olarak katılmak mümkün değildir. Zira CMK 134 gereğince verilen tüm arama kararlarında el edilen deliller soruşturmanın niteliği sebebi ile suçun konusu teşkil edecektir. Bu durumda CMK 134/4 fıkrasındaki amir hükmün hiçbir mantığı kalmayacaktır. Kaldı ki; bazı hallerde şüphelinin vekilinin doğru savunma yapabilmesi için delilleri görmesi gerekmektedir. Aynı husus yargılama aşamasında da geçerlidir. Örneğin; Çocukların kullanıldığı iddia edilen, müstehcen içerikli görüntülere bu sebeple el konulduğu ve sanık avukatına eşya müsaderesi sebebi ile bir örnek verilmediğini düşünelim. Bu durumda görüntüleri görmeyen savunma makamının müvekkilini hakkaniyetle savunmasının imkanı olmayacaktır. Halbuki, sanık avukatının görüntüleri incelediğini ve her ne kadar görüntülerde çocukların kullanıldığı iddia edilse de yapılan araştırma sonucunda görüntülerde yer alan

[172] http://www.hukukihaber.net/bilgisayar-verilerinin-yedeklenmesi-ve-yasak-veriler-makale,3527.html Son Erişim 18.02.2015 "Bilgisayar Verilerinin Yedeklenmesi ve Yasak Veriler" Prof. Dr. Ersan ŞEN

kişilerin kimliklerinin tespit edilerek on sekiz yaşından büyük olduğunun hukuka uygun bir şekilde mahkeme aşamasında ispatlandığını düşünelim. Bu halde; sanığa isnat edilen suçun niteliği değişecektir. Uygulama açısından bir başka problem ise adli kolluk olay mahallinde el koyma işlemi sırasında bilişim sistemleri üzerinde inceleme yapmamaktadır. Nitekim CMK 134 gereğince bilişim sistemlerine el koyma şartları varsa, el koyma işlemini gerçekleştirmektedir. Adli kolluğun olay mahallinde, el konulacak verileri analiz ederek suç unsuru taşıyıp taşımadığını tespit edebilmesi fiziki şartlar gereğince imkansıza yakındır. Bu durumda, olay mahallinde tespit yapılmadan muhtemel suç unsuru teşkil edecek veriler ışığında CMK 123 veya 127 gereğince bir işlem tatbik edilemeyecektir.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır" şeklindedir. Adli kolluk tarafından, el koyma işlemi yapılmadan bilişim sisteminin yedeğinin alınması durumunda ise şüpheli veya vekiline alınan yedeğin bir kopyasının verilmesi gerekmemektedir. Ancak teknik açıdan delilin manipülasyona uğramadığının ispatı açısından alınan yedeğin zaman damgalı hash değerinin şüpheli veya vekiline verilmesi gerekmektedir. Nitekim adli kolluk tarafından kullanılan bir çok program (Encase, Ftk) diskin yedeğini alırken hash algoritmasını da almaktadır. Kanun'un 5. Fıkrası ile diğer fıkraları arasında ise pek uyum olduğunu söylemek mümkün değildir. Çünkü; CMK 134 gereğince; bilişim sistemleri üzerinde arama ve el koyma kararında, delil elde edilirken ana kural sistemin olduğu yerde arama yapılması ve sistem verilerinin kopyalanmasıdır. Kanun gereğince, bilişim sistemlerine el koyma ise istisnadır. Oysa bu fıkradaki düzenleme sanki el koyma kural, bu tedbir uygulanmadan sistemin olduğu yerde kopyasının alınması istisnaymış gibi bir anlam çıkmaktadır. Dolayısıyla bu fıkranın öğretide olduğu ve anlam karışıklığına yol açan bir düzenleme olduğu belirtilmektedir.[173] Bu sebeplerle; ilgili fıkranın düzenlenmesi tekrardan gözden geçirilmelidir. Özellikle uygulama ile tamamen zıt olan kopyası alınan verilerin kağıda yazılması ve imza altına alınması hususu çıkartılmalıdır. Kanun koyucunun burada amaçladığı hangi verilerin yedeğinin alındığının tutanağa geçirilmesi olabilir. Ancak yedeklemesi yapılan tüm verilerin kağıda yazdırılması mümkün değildir. Bir diğer yapılması gereken değişiklik ise yeni teknolojik gelişmeler ışığında canlı sistemler, mobil sistemler veya bulut bilişim sistemleri üzerindeki veriler ile karşılaşılması hallerinde el koyma işlemi

[173] DÜLGER Volkan Murat, 2012 s 661.

yapılmadan sistem verilerin yedeğinin alınabileceği hususu düzenlenmelidir. Kaldı ki; özellikle bulut bilişim sistemleri üzerinde bulunan verilerde el koyma işleminin yapılması teknik açıdan mümkün değildir. Bu şekilde bir olay ile karşılaşılması halinde, adli kolluğun ayrıca bir izin alarak verilerin bulunduğu yer sağlayıcı (hosting) şirketlerinden temin etmesi gerekecektir. Yer sağlayıcı firmanın yurt dışında bulunması halinde sistem üzerinde yer alan verilere hızlı bir şekilde ulaşılması bir hayli güçtür. Zira fail kendi hesabının şifresini soruşturma aşamasında kolluğu vermek zorunda değildir. Adli kolluk tarafından faile ait olduğu ve suç unsuru taşıyacak bilgilerin bulunduğu bulutta yer alan bilişim sistemin şifresinin kırılarak sistemdeki verilere ulaşılmaya çalışılması ise hukuka aykırı olacaktır.

8. Şüphelinin bilişim sistemleri üzerine yapılan arama el koyma sırasında elde edilen haberleşme içeriklerinin hukuki vasfı, cmk md. 134 ile cmk md. 135'in değerlendirmesi

135. maddeye göre, *"(Değişik: 6526 - 21.2.2014 / m.12) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, ağır ceza mahkemesi veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...) dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl mahkemenin onayına sunar ve mahkeme, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya mahkeme tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır. Bu fıkra uyarınca alınacak tedbire ağır ceza mahkemesince oy birliğiyle karar verilir. İtiraz üzerine bu tedbire karar verilebilmesi için de oy birliği aranır."* Maddenin 8 numaralı fıkrası "Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler" ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

a) Türk Ceza Kanununda yer alan;

1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80),

2. Kasten öldürme (madde 81, 82, 83),

3. İşkence (madde 94, 95),

4. Cinsel saldırı (birinci fıkra hariç, madde 102),

5. Çocukların cinsel istismarı (madde 103),

6. (Ek: 6526 - 21.2.2014 / m.12) Nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149),

7. (*)Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),

8. Parada sahtecilik (madde 197),

9. (...) (Madde 135'in 7. fıkrasının a bendinin 9 numaralı alt bendi, 6.3.2014 tarih ve 28933 sayılı mükerrer R.G.'de yayımlanan, 21.2.2014 tarih ve 6526 sayılı Kanunun 12. maddesi hükmü gereğince yürürlükten kaldırılmıştır.)

10. (Ek: 5353 - 25.5.2005 / m.17) Fuhuş (madde 227(...)(*)),(*)

(*) Madde 135'in 7. fıkrasının a bendinin 10 numaralı alt bendinde yer alan ", fıkra 3" ibaresi, 6.3.2014 tarih ve 28933 sayılı mükerrer R.G.'de yayımlanan, 21.2.2014 tarih ve 6526 sayılı Kanunun 12. maddesi hükmü gereğince madde metninden çıkarılmıştır.

11. İhaleye fesat karıştırma (madde 235),

12. Rüşvet (madde 252),

13. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),

14. (Değişik: 6572 - 2.12.2014 / m.42) Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302),

15. (Ek: 6572 - 2.12.2014 / m.42) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),

16. (*) Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları."

(9) Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz" şeklindedir. **Bunlar arasında bilişim suçlarından söz edilmemiştir.**

CMK 140. Maddede ise sayılan suçların işlendiği hususunda kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilmemesi halinde, şüpheli veya sanığın kamuya açık yerlerde faaliyet gösteren işyerleri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir. Burada bilişim suçlarından bahsedilmemiştir[174].

Bu halde kişilerin bilgisayarlarında ki bu haberleşme verileri, (Msn, Skype, E-Posta Vb.) kanımca 5271 sayılı CMK'nın 135. Maddesi kapsamında değerlendirilmesi gerekmektedir. Bu durumda ancak 135. Maddenin 8 numaralı fıkrasında ki belirtilen suçların gerçekleşmesi halinde, şüphelinin bilgisayarlarında ki bu haberleşme verileri tespit edilebilecektir. Örneğin; 5237 sayılı TCK'nın 243. Maddesi ve devamında yer alan bilişim sistemindeki verilere yetkisiz erişim veya verileri değiştirme, verileri yok etme, verileri bir başka yere gönderme veya banka kredi kartlarının kötüye kullanılmasına ilişkin bir soruşturma olduğunda ise şüphelinin bilgisayarlarında yapılan aramada ortaya çıkan iletişime ilişkin elde edilen veriler (Skype, E-mail vb.. kayıtlar) dava aşamasında hukuka aykırı delil olacağı için kullanılamayacaktır. Bir hakaret suçuna delil olabilecek şüphelinin veya sanığın bilgisayarlarında yapılan aramada elde edilebilecek haberleşme verileri delil olarak kullanılamayacaktır. Çünkü kanun koyucu iletişim tespiti için gerekli gördüğü suç tiplerini tek tek belirlemiştir. Bunun haricinde gerçekleşen suçlar da iletişim tespiti yoluna gidilemeyecektir[175].

Bir diğer görüş ise; Bilişim Sisteminde yer alan haberleşme içeriklerinin, bilişim sistemine ayrıca kayıt edilip edilmediğinin incelenerek tespit edilebilmesi gerektiğidir. Duruma göre CMK 134 veya CMK 135 uygulanması gündeme geleceği belirtilmiştir. Buna göre *"telekomünikasyon yoluyla yapılan iletişim denetlenmesi, sırf telefonla yapılan görüşmelerle sınırlı olmayıp, internet üzerinden yapılan yazılı, sesli veya görüntülü görüşme ve haberleşmeleri de kapsar. Bu nedenledir ki kanun koyucu CMK m.135/4'de "iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkan veren kodu"*

[174] KARAGÜLMEZ Ali, 2009 age s 262.

[175] http://www.bilisimhukuk.com/2010/03/bilgisayardaki-gorusme-kayitlari-sadece-veri-degildir-basli-basina-bir-iletisimdir/2/ Son Erişim 15.11.2014; "Bilgisayardaki görüşme kayıtları sadece "veri" değildir, başlı başına bir "iletişim"dir" Av. Fehmi Ünsal Özmestik

ibarelerine yer vermiştir. Bu anlamda, bilim ve tekniğin sürekli geliştiğini, bu açıdan Ceza Muhakemesi Kanunu'nu da mükemmel bulmamakla, hatta delil toplama ve değerlendirme hususunda yetersiz ve eksik hükümleri olduğunu düşünmekle birlikte, CMK m.135'in bu hali ile de bireylerin e-posta üzerinden yaptığı haberleşmeleri içerdiğini, bu haberleşme türünün bir suçun işlenmesinde kullanıldığı veya işlenen bir suçla ilgili bu haberleşme kayıtlarından delile ulaşılabileceği düşünülmekte ise, yasal şartların oluşması kaydıyla İnsan Hakları Avrupa Sözleşmesi m.8/2, Anayasa m.22/2 ve CMK m.135 uyarınca iletişimin denetlenmesi yoluyla şüpheli veya sanığın haberleşme hürriyetine müdahale edebilmesi mümkün olabilecektir. ***Bireyin e-posta yazışma ve haberleşmeleri CMK m.135 kapsamında değerlendirilirken, kendisine e-posta ile gelen bir yazı, resim, görüntü veya ek dosyayı kullandığı bilgisayara veya taşınır belleğe kaydettiğinde, artık bu belge haberleşme hürriyetinin ve dolayısıyla iletişimin denetlenmesinden çıkıp, CMK m.134 kapsamında bilişim cihazında kayıtlı bilgi ve belgeye dönüşecektir. Burada; bilgi, belge ve dosyanın bireyin kullandığı bilgisayarda mı kayıtlı olduğu, yoksa bu cihazdan bağımsız olarak haberleşme aracı olan e-postasında mı bulunduğu ölçütü dikkate alınmalıdır.*** *Bilgi, belge veya dosyanın bireye e-posta üzerinden ulaşıp ulaşmadığının bu noktada bir önemi olmayacaktır. Dışarıdan, yani başka e-posta kullanıcısından veya başkasından, hatta bireyin kendi e-postası üzerinden aynı e-posta adresine gönderdiği ileti, yani gelen bilgi, belge veya ek dosya, bireyin kendisine ait ve ancak özel şifre ile açılıp kullanılabilen e-postasında durmakta ise, bu unsur haberleşme hürriyetinin ve bu nedenle de CMK m.135 ila 138 konusu sayılacaktır. Bu noktada, bir tür postada elkoyma gibi nitelendirilebilir. Ne zaman bu ileti birey tarafından bilişim cihazına kayda alınır, yani elektronik posta kutusundan çıkarılır, aynı mektubun postadan veya posta kutusundan alınıp çekmeceye veya dolaba koyulmasında olduğu gibi, işte o andan itibaren CMK m.134 devreye girer. Artık bu ileti haberleşme konusu olmaktan çıkıp, bireyin arşivlemek veya kullanmak için bilişim cihazına aldığı bilgi, belge veya dosya özelliğini kazanır*[176]*."*

Bu noktada tartışılması gereken bir başka konu ise bilişim sistemi üzerine yer alacak haberleşme maillerinin şifreli olması hususudur. Soruşturma makamı tarafından CMK 135 gereğince bu şifrelerin kırılarak görüşme kayıtlarına ulaşabilmesi hukuka uygun bir delil mahiyetinde olup olmayacağı üzerinde durulmalıdır. Buna göre; CMK 135'in şartlarına uygun

[176] http://www.hukukihaber.net/e-posta-takibi-ve-cmk-m134un-kapsami-makale,3524.html Son Erişim 18.02.2015 " E-Posta Takibi ve CMK m.134'ün Kapsamı" Prof. Dr. Ersan ŞEN

verilmiş bir iletişimin tespitinde, bilişim sistemi üzerinde karşılaşılan haberleşme metninde şifreli e-mail yazışmaları vb içerikler tespit edilmesi durumunda, CMK 134/2 gereğince adli kolluk tarafından inceleme yapılabilecektir. Ancak burada soruşturma makamı, bilişim sistemleri üzerinde haberleşme metinlerine hukuka uygun yoldan ulaşabilmesi için somut olaya ilişkin hem CMK 134 hem de CMK 135 gereğince karar aldırması gerekmektedir. Aksi halde, elde edilecek delilin hukuka uygunluğundan şüphe duyulacaktır.

Ersan'a göre ise *"CMK m.135'in şartlarının oluşup da şüpheli veya sanığın kullandığı e-postaya girilmesi gerektiğinde, e-posta adresinin şifresi bilinmeksizin, bu gizli bilgi ilgili kişiye sorulup öğrenilemeyeceğine göre, aksini yapmanın iletişim denetlenmesi tedbirinin gizliliğine de aykırı olacağından, adli makama veya kolluğunun şifreyi öğrenmek veya şifreyi kırıp veya etkisiz hale getirmek suretiyle e-posta adresine girip denetim yapıp yapamayacağında sorun çıkabilir. Kimisine göre, kolluk usule uygun şekilde öğrenmedikçe ve bunu da kanıtlamadıkça hukuka aykırı yöntemlerle elde ettiği ve gizlice girdiği e-postadan ulaştığı bilgi, belge, delil veya emareleri hukuka uygun yolla elde edilen delil olarak kullanamaz. Kimisine göre de, esas olan CMK m.135 ila 138'in öngördüğü usul ve şartlara uygun olarak iletişim denetlenmesi kararının alınması olup, CMK m.135/4'de sayılan diğer şartların yanında asıl olarak yüklenen suçun türü, e-posta kullanıcısı şüpheli veya sanığın kimliği ve e-posta adresi yeterli olacak, alınan bu kararla da bireyin e-postasının bağlı olduğu yer veya erişim sağlayıcı üzerinden veya telefon dinlemede olduğu gibi gizli yöntemlerle bireyin e-postasına yargı kararına uygun olarak girilip veri toplanabilecektir. Bu noktada, CMK m.135/4'de geçen "iletişim bağlantısını tespite imkan veren kod" kavramını e-posta şifresi olarak değil e-posta adresi olarak kabul etmek, şifreyi ise iletişimin denetlenmesi kararı alındıktan sonra aşılması gereken bir engel saymak gerekir. Aksi halde, teknik olarak şüpheli veya sanığın kullandığı e-postaya müdahale edebilmek çok zorlaşır. Bununla birlikte, adli makam ve kolluk bireyin e-posta adresini veya şifresini hukuk aykırı yol ve yöntemlerle elde etmişse, bu noktada e-postaya giriş ve bunun sonucu olarak da elde edilen bilgi, belge ve deliller ile emarelerin hukuk aykırılığı gündeme gelecektir*[177].

[177] http://www.hukukihaber.net/e-posta-takibi-ve-cmk-m134un-kapsami-makale,3524.html Son Erişim 18.02.2015 " E-Posta Takibi ve CMK m.134'ün Kapsamı" Prof. Dr. Ersan ŞEN

9. CMK Md. 134 ile CMK Md. 116 ve 123'ün değerlendirmesi

Ceza Muhakemesi Kanunu 116. Şüpheli veya sanıkla ilgili arama *"(1) Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda (Değişik ibare: 6572 - 2.12.2014 / m.40) "makul" şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir*[178]*."* Ve 123. Maddelerindeki *"(1) İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır. (2) Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir*[179]. Genel nitelikteki arama hükümlerine rağmen CMK 134. Maddeye yer verilmesi bunun özel nitelikte bir düzenleme olduğunu göstermektedir. Bu durumda; CMK 116. Maddeye dayanılarak şüphelinin iş yeri ya da konutunda yapılan bir arama sırasında ayrıca 134. Maddeye göre arama yapılmasına ilişkin bir karar alınmamışsa, şüphelinin kullandığı bilişim sistemleri ve bilgisayarlar üzerinde arama ve el koyma kararının uygulanması hukuken mümkün değildir. CMK 116. Maddeye dayanılarak yapılan aramada şüphelinin üzerinden çıkan cep bilgisayarında arama yapılması için dahi 134. Maddeye göre karar alınması gerekmektedir. Buna uyulmaksızın yapılan aramalar hukuka aykırı yöntemle delil elde etme olacak ve elde edilen delilde yasak delil niteliğinde olacaktır[180]. Aynı şekilde CMK 123. Maddesi gereğince; suç unsuru taşıyan verilere el konularak müsadere altına alınıp alınmaması tartışmalıdır. Ancak CMK 134'ün şartlarına bakıldığında, özellike 2. Fıkranın 2. bölümünde açıkça *"Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir."* Hükmü yer almaktadır. Söz konusu özel düzenleme ve CMK 134'ün ortaya çıkardığı metodolojiye göre ana kural sistemin şüpheliye iade edilmesidir.

10. Kovuşturma evresi

Bilişim suçlarının kovuşturma evresine ilişkin hükümler, diğer (klasik) suçlardan farklı değildir. Buna göre CMK'da bilişim suçlarında, kovuşturma evresinde farklı bir düzenlemeye gidilmemiştir.

---

[178] www.kazanci.com Son Erişim 01.03.2015

[179] www.kazanci.com Son Erişim 01.03.2015

[180] DÜLGER Volkan Murat, 2012 s 660.

Bilişim suçlarının kendisine özgü özellikleri, bu suçların ispatında kullanılan elektronik delilin, fiziksel delillerden çok ayrı ve benzersiz yapısı ile özellikle internet ortamında bilişim suçlarında dünyadaki yaklaşım, ilke ve uygulamaların göz ardı edilemeyecek olması karşısında, ülkemizde bilişim suçlarına ilişkin ceza yargılaması kurallarındaki eksikliklerin, belirtilen olguların göz önüne alınarak bir an evvel giderilmesi gerekmektedir.

İnternet aracılığıyla ceza muhakemesinde pek çok işlemin yapılabilmesi olanaklı hale gelmiştir. Bununla birlikte, internette ceza muhakemesi işlemleri yapılırken, bunun insan hakları ve ceza muhakemesi ilkelerine uygunluğu sorunu ile karşılaşılmaktadır[181].

Bilişim suçlarında ortaya çıkan sorunlardan biri de mahkemelerin yetkisi meselesidir. Genel kural gereğince davaya bakma yetkisi, suçun işlendiği yer mahkemesine aittir. (5271 sayılı CMK. m. 12/1.) Bilişim suçlarıyla ilgili açılan davada yetkili mahkeme, bu suçların bünyesi ve işlenme şekillerine göre tartışmalı konular içermektedir. Tüm bunları ele alırken, suçun işlenme şekillerine göre sonuca gitmek gerekmektedir[182].

§ III Şüphelinin bilişim sistemleri üzerinde yapılan arama, el koyma ve inceleme işlemlerinin hukuka aykırı olmasının ortaya çıkardığı sonuç

A- Ceza muhakemesinde hukuku aykırı delil kavramı

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma sonucu elde edilen verilerden, kişinin sadece özel hayatının zedelenmediği ve hukuka uygun şekilde meydana getirildiği durumlarda olayın aydınlatılması veya failin bulunması hususunda yargılama makamlarının kanaatlerinin oluşması için yararlanılacaktır.

Ceza yargılamasının amacının maddi gerçeğe ulaşmaktır ve bu gerçeğe ulaşmak için serbest delil sistemi kabul edilmiştir. Ancak maddi gerçeğin her ne olursa olsun ortaya çıkarılması birçok kişisel değere zarar vereceği için mutlak olarak kabul edilmemektedir. Bunun yanında vicdani delil sistemi de serbest delil sistemine bir istisna oluşturmaktadır. Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir (CMK

[181] ÖZTÜRK Bahri; "Ceza Muhakemesi ve İnternet", Uluslar arası İnternet Hukuku Sempozyumu, 21-22 Mayıs 2001, DEÜ. Yayını, İzmir, 2002, s 506.

[182] KARAGÜLMEZ Ali, 2009 age s 356.

m.217). Bu hükmün zıt anlamına göre, suç, hukuka uygun bir şekilde elde edilmemiş hiçbir delille ispat edilemez[183]. Hukuka aykırı deliller, bir olayın ispatında hükme esas alınamaz. Hukuka aykırılık yasa dışılıktan daha geniş bir içeriğe sahiptir. Hukuka aykırılık en başta ulusal hukuk sistemimiz içinde yürürlükteki tüm hukuk kurallarına aykırılık anlamına gelmektedir. Bu çerçeve içinde, Anayasa'ya, usulüne uygun olarak kabul edilmiş uluslararası sözleşmelere, yasalara, kanun hükmünde kararnamelere, tüzüklere, yönetmeliklere, içtihadı birleştirme kararlarına, teamül hukukuna ve hukukun genel ilkelerine aykırı uygulamaların tümü hukuka aykırılık kavramı içinde yer aldığı belirtilmektedir[184]. Bir delilin hukuk devletinde ceza yargılamasında kullanılması için hukuka uygun yollardan elde edilmiş olması gerekmektedir.

B- Ceza muhakemesi hukukunda delil yasakları

Hukuk devleti esaslarına uygun bir ceza muhakemesinde delil elde edilmesi ve değerlendirilmesi işlemlerine getirilen sınırlamalara Öztürk'e göre delil yasakları, Yenisey'e göre ise hukuka aykırı deliller teorisi adı verilmektedir. Dürüst yargılanma hakkı kapsamına giren temel sanık haklarını sağlamadan elde edilen veya yetki sınırları aşılarak veya kanunun önceden elde edilmesini yasaklamış olduğu halde elde edilen deliller hukuka aykırı yöntemlerle elde edilmiş olmaktadır[185].

Ceza muhakemesinde delil elde edilmesi ve değerlendirilmesi işlemlerine getirilen sınırlamalara delil yasakları denmektedir. Maddi gerçeğin araştırılmasına delil yasakları adı verilen bazı sınırlamalar getirilerek kişisel ve toplumsal değerler korunmaya çalışılmaktadır[186].

Delil yasakları durumları hukukumuzda, aydınlatma yükümlülüğünün yerine getirilmemesi (CMK m. 147), ifade ve sorgu sırasında söz konusu olan delil yasakları (CMK m. 148), ifade ve sorgu dışında söz konusu olan delil yasakları (Örneğin; arama ve elkoyma

[183] KAPILI Kübra, s 30.

[184] Aktaran CENTEL Nur - ZAFER Hamide; AYM, 22.6.2001-2/2, RG 5.1.2002 No.24631 (Mükerrer); Aynı yönde bknz. YCGK, 29.11.2005-7-144/150, YKD XXXII, 3(Mart 2006), s 470.

[185] YENİSEY Feridun; Ceza Muhakemesi Hukukunda Delil, Ceza Hukuku Dergisi, Ağustos 2007.

[186] ÖZTÜRK, Bahri s 487.

için CMK m. 116 vd. söz konusu olan hukuka aykırılıklar), delil aracı yasakları şeklinde ifade edilmiştir.

Ceza Muhakemesi Kanunu'nun 217. Maddesinin 2. Fıkrasında delil değerlendirme yasakları kavramı düzenlenmiş olup, hukuka aykırı delillerin yargılamada kullanılamayacağından bahsedilmiştir. Kanun maddesinden de anlaşılacağı üzere tüm deliller yasaya uygun bir şekilde elde edilmiş olmalıdır, aksi takdirde delil elde etme yasağı ile karşı karşıya kalınacaktır. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemi kararının yasaya uygun verilmiş ve bu işlem ile elde edilen tüm verilerin yasadaki usulüne uygun şekilde elde edilmiş olmaları gerekir. Aksi takdirde değerlendirme yasağı kapsamına girer ve yargılamada değerlendirmeye alınamazlar. Çünkü her türlü takdir yetkisini ortadan kaldıran mutlak bir delil yasağı hukuk sistemimizde mevcuttur. Anayasamızda da yer alan bu düzenleme tüm yargılama hukuku bakımından yasağı ifade etmektedir. Anayasa'nın 38. Maddesinin 6. Fıkrasında, kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez denilmektedir.

5271 Sayılı Ceza Muhakemesi Kanun'unda, hükmün hukuka aykırı yöntemlerle elde edilen delile dayanmasının, hükmün hukuka kesin aykırı olması sonucunu doğuracağı kabul edilmiştir (CMK m. 289). Mahkeme kararında hukuka aykırı delile dayanılması halinde, diğer delillere göre aynı şekilde hüküm kurulabilecek olması, hükmün bozulmasını engellemeyecektir. Hukuka aykırı delilin hükmü mutlaka etkilediği, hükmün bu halde değişebileceği yasal bir karine olarak kabul edilmiştir. Kanun yolu incelemesi yapan mahkeme, hükmün hukuka aykırı delile dayanıp dayanmadığını inceleyebilecektir. Ancak, hükümle hukuka aykırı delil arasında nedensellik ilişkisi kurduktan sonra, hükmün değişebilirliğini değerlendirmeyecektir[187].

C- Hukuka aykırı şekilde verilen koruma tedbirleri nedeniyle tazminat

Ceza muhakemesi hukukunda genel olarak koruma tedbirlerine karşı gidilebilecek üst denetim yolları itiraz ve temyizdir. Ancak bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinden ilgili, kararın yerine getirilmesinden ve gerekli bilgilerin elde edilmesinden sonra bu tedbirden haberdar olunmakta ve öngörülen hukuksal korunma olanaklarından yararlanamamaktadır. Bu sebeple sonrada

[187] KAPILI Kübra, s 33.

başvurulan bu yollar uygulanan tedbirin hukuka aykırılığının tespiti sonucuna yol açabilmektedir[188].

5271 Sayılı Ceza Muhakemesi Kanunu 141. Maddesinin 1. Fıkrasında hangi koruma tedbirlerine ne tür bir hukuka aykırılık olursa tazminat istenebileceğini belirtmiş, tazminat isteyebilecek kişiler sıralanmıştır. Buna göre CMK m. 141/1-j maddesi uyarınca;

"Eşyasına veya diğer malvarlığı değerlerine, koşulları oluşmadığı halde elkonulan veya korunması için gerekli tedbirler alınmayan ya da eşyası veya diğer malvarlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen kişiler, maddî ve manevî her türlü zararlarını, devletten isteyebilirler".

Bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinin uygulanması sırasında elkoyma koşulları oluşmadığı halde elkoyan, elkoyulan cihazları korumak için gerekli tedbirleri almayan veya elkoyulan bu cihazları amaç dışı kullanan veya gerekli veriler elde edilir edilmez ilgilisine iade etmeyen kolluk görevlilerinden bu yolla tazminat istenebilir.

Bu sebepten dolayı, Ceza Muhakemesi Kanunu'na göre tazminat davası açma süresi 3 aydır. Süre, söz konusu mahkeme kararının kesinleşmesi ile başlar ve herhalde kararın veya hükmün kesinleşme tarihini izleyen bir yıl içinde açılması gerekmektedir.

§ IV Sonuç ve değerlendirme

Bilgi teknolojilerinin gelişiminin hızlı bir şekilde ilerlemesi ve bu sayede insanların yaşamlarındaki çeşitli ihtiyaçlarını daha hızlı ve efektif bir şekilde kolaylaştırması, bu alanda karşılaşılan olay tiplerinin çeşitlenmesine ve ihtiyacın da artması sebebi ile sektörün daha hızlı gelişmesine sebep olmaktadır. Özellikle, Türk hukuku açısından çok yeni olan bu alanda, çeşitli sivil toplum kuruluşlarının desteğiyle sürekli seminer ve konferanslar düzenlenerek bilimsel çalışmaların arttırılması gerekmektedir. Zira bu alanda meydana gelen problemlere belli bir mantık çerçevesinden bakmamız gerekmektedir. Bir başka deyişle, nasıl hukuk sisteminin bir mantığı var ise, bilişim sistemlerinin ve internetin de belli bir mantığı vardır.

[188] KAPILI Kübra, s 35.

Bunun yanı sıra, ISO 'IEC' in 27000 "Bilgi Güvenliği" ve ISO/IEC 27037, 27041, 27042 ve 27043 standartları haricinde özellikle Adli Bilişim alanında adli kolluk tarafından uygulanacak ve hukuki alt yapısı bulunan belli bir standart ve bilimsel kuralların düzenlenmesi gerekmektedir. Örneğin; olay mahallinde adli bilişim uzmanları tarafından gidildiğinde, hangi donanımlar ve hangi programlar ile incelemenin yapılması gerektiği konusunda hukuki olarak bir düzenleme yoktur. Bir başka ifade ile savcılıklar tarafından yürütülen soruşturmalarda adli kolluk fezlekeyi hazırlarken, teknik açıdan uyması gereken bir kriter veya bilimsel bir dayanak düzenlemesi hali hazırda bulunmamaktadır. Bu halde; adli bilişim incelemelerinde adli kolluk tarafından farklılık teşkil edecek ekipman ve donanımlar kullanılmaktadır. Bu ekipman ve donanımların ne şekilde akreditasyonun sağlandığı, hangi ülkeler tarafından kabul edildiğine ilişkin bir fikir birliği yoktur.

Bir başka husus ise mevcut yasal düzenlemenin gelişen teknolojik yeniliklere cevap vermemesidir. Olay mahallinde canlı sistemler ile karşılaşılması durumunda, adli kolluk birimlerinin hukuki olarak nasıl davranması gerektiği konusunda bir düzenleme yoktur. Zira olay mahallinde çalışır durumda olan bir sistem ile karşılaşılması durumunda, tüm analizin sıhhatli bir şekilde yapılabilmesi için sistemin kapatılmadan analizinin gerçekleştirilmesi gerekmektedir. Olay mahallinde çok sayıda canlı sistemin bulunması durumunda ise incelemenin günlerce sürmesi kuvvetli muhtemeldir. Her ne kadar karşılaşılan böyle bir durumda, bilişim sistemlerine el koyma kararı uygulanarak donanımların bilişim şubelerine götürülmesi hukuken mümkün olsa bile bilişim sistemlerinde geçici hafıza limitlerinin artması sebebi ile soruşturma konusu aranan tüm bilgilerin bu belleklerde yer alma ihtimali vardır. Bu aşamada yapılacak bir hata delillerin yok olmasına sebep olarak ve soruşturmanın sıhhatini tehlikeye düşürecektir. Bunun yanında, soruşturmanın özelliğine göre bilişim sisteminde yer alan delillerde farklı bölümlerde olabilir. Örneğin; failin tarayıcı internet aktivitesi veya sosyal ağlarda gerçekleştirdiği aktiviteler noktasında toplanabilir. Söz konusu analizlerinde bazı durumlarda, çalışır halde bulunan sistemler üzerinde yapılması gerekmektedir.

Bilişim sistemlerine arama ve el koyma işleminde CMK 134'te yer alan şartların koruma tedbiri olarak ele alındığı görülmektedir. Öncelikle kanun maddesinin başlığının *"bilgisayarlarda, bilgisayar programlarında kütüklerinde arama ve el koyma"* yeni teknolojik gelişmeler ve ileride çıkması muhtemel teknolojik gelişmeler ışığında güncellenerek daha genel bir isimle düzeltilmesi gerekmektedir. Söz konusu madde soruşturma aşamasında, şüphelinin bilgisayarlarında ve bilgisayar programlarında arama ve el koyma işleminin uygulanmasına cevaz vermektedir. Halbuki bu tür suç tiplerinde, gerçek

faillere ulaşılabilmesi için şikayetçi, mağdurunda bilişim sistemlerinde inceleme yapılması gerekmektedir. Her ne kadar uygulama aşamasında, bu inceleme şikâyetçinin rızası dahilinde gerçekleştiriliyor olsa da bu durumun hukuksal alt yapıya kovuşturulması gerekmektedir.

CMK 134 gereğince kopya çıkartılması ana kural iken, uygulama aşamasında, dijital delillere el koyma işleminin ana kural halinde dönüştürülmesi sorunu çözülmelidir. Yeni teknolojik gelişmeler ışığında özellikle canlı sistemler ile karşılaşılması durumunda uygulanacak yöntem ve analizler madde metninde yerini almalıdır.

CMK 134 gereğince uygulanan koruma tedbirinde, şüphelinin bilişim sisteminde haberleşme metinlerinin bulunması durumunda, ne şekilde bir ayrıma gidilmesi gerektiği kanun maddesinde açıkça belirtilmelidir. Hangi hallerde CMK 135'in aranması gerekeceği, hangi hallerde CMK 134 gereğince verilen kararlarda elde edilen haberleşme metinlerinin hukuka uygun elde edileceğinin kabul edilmesi gerektiği ayrıntılı bir şekilde yer almalıdır.

CMK 134 maddelerinde açıkça belirtilen şartlar oluşmadan, mahkemeler tarafından arama ve el koyma kararları verilmemelidir. Hukuka aykırı olarak verilen bir karar bulunması durumunda, el edilen delillerin mahkeme aşamasında delil vasfını yitirdiği kabul edilerek, yargılama dosyasından çıkartılması sağlanmalıdır. Adli kolluk tarafından, dijital delillere el kopya alınması veya el konulması aşamasında, delil niteliğine zarar gelecek veya delilin orijinalliğini bozan birtakım şüpheli işlemlerden kaçınılmalıdır.

CMK 134 gereğince arama ve el koyma kararı verilebilmesi için *"somut delillere dayanan kuvvetli şüphe sebebinin"* varlığının aranması şartı yeniden düzenlenmesi gerekmektedir. Özellikle bu tür suç tiplerinde delillere ulaşılabilmesi için bu iki şartın oluşma ihtimali bir hali güçtür. Yine CMK'unda kuvvetli şüphenin arandığı diğer koruma tedbirlerine bakıldığında, getirdiği sonuçlar bakımından CMK 134'den daha ağır olduğu görülmektedir. Mevcut kanun maddesi, birçok savcının hukuka aykırı bir şekilde, hakimden arama ve el koyma kararı için talepte bulunmasına yol açacaktır. Bu sebeple; ilgili kanun fıkrasının düzeltilerek, makul şüphenin varlığı halinde bilişim sistemlerinde *arama ve kopya çıkartma*, kuvvetli şüphenin varlığı halinde ise *arama ve el koyma kararının* verilebileceği tekrardan düzenlenmelidir.

CMK 134 kapsamında arama ve el koyma kararı verilebilmesinin bir diğer şartı ise başka suretle delil elde etme imkanının bulunmaması durumudur. Bu tür suç tiplerinde, bilişim sistemlerinde yer alan deliller suçun kimin tarafından ne şekilde işlendiğini kati olarak

gösterebilecektir. Bu halde; soruşturma aşamasında savcılık makamı tarafından en son çare olarak arama ve el koyma tedbirine başvurulması dijital delillerin yok olmasına sebep olabilecektir. Bu sebeple; söz konusu fıkranın yeniden düzenlemesinin yapılması gerekmektedir.

Adli ve Önleme Aramaları Yönetmeliği md 17 ile Suç Eşyası Yönetmeliği md 9'un sistematiği değiştirilerek, Kanun'un tekrarından ziyade, üst normlara aykırı olmayacak şekilde adli kolluğa yol gösterecek ve delilin manipülasyona uğramasına engel olacak nitelikte birtakım ayrıntılı düzenlemeler yapılmalıdır. Türkiye genelinde, yeknesak uygulamalar olması açısından tüm kolluk birimlerince uyulması zorunlu olacak standartların bulunduğu bir kitapçık düzenlenmeli ve bu alanda bilimsel araştırma ve inceleme yapan dernek, sivil toplum kuruluşu, üniversite, baroların bilişim komisyonları, adalet akademisi tarafından adli kolluk personeli, hakim ve savcıların sürekli eğitim alması sağlanmalıdır.

Özellik bilişim sistemleri üzerindeki delile ulaşma yöntemi haricinde, o delilin ne şekilde dosyaya sunulacağı, ne şekilde analiz edileceği ve analizi gerçekleştirecek programların sahip olması gereken sertifikasyonlar sorgulanmalı ve kısa zamanda buna ilişkin bir standart getirilmesi gerekmektedir. Soruşturma ve Kovuşturma aşamasında adli bilişim uzmanı tarafından dosyaya sunulacak rapor bir hayli önemlidir. Teknik bir konu olması sebebi ile Savcı veya Hakim birçok hususta rapora bağlı kalmaktadır. Bu sebeple; özellikle mahkeme aşamasında verilen adli bilişim raporlarına dikkat edilmesi ve mahkeme tarafından istenen hususlarda sade bir açıklama yapılarak konunun işlenmesi gerekmektedir. Açıklamalar bu alanda hiçbir bilgisi olmayan bir kişinin raporu anlayabileceği kıvamda olmalıdır. Raporda, teknik bilirkişi kesinlikle olaya ilişkin kanaatini veya hukuki yorum açıklamasında bulunmamalıdır. Bu sebeple; Adli bilişim standartlarının geliştirilmesinin yanı sıra, mahkemelerde bu alanda bilirkişiliğe başvuran uzmanların eğitimden geçirilerek, uzmanlaşmaları sağlanmalıdır. Bir başka ifade ile sürekli gelişen teknolojik yenilikler ışığında adli bilişim alanında bilirkişilik yapanlar için meslek içi eğitim son derece önem arz etmektedir.

Bilişim suçları ve internet üzerinden yapılan yayınlara ilişkin yapılması gereken en önemli unsur, uluslararası alanda gerçekleştirilen çalışmalara katılmak ve tüm dünya ülkelerinin kabul ettiği ve uyulması gereken ana kuralların tahlilini sağlamaktır. Gerçekleştirilen bu düzenlemeler ise her geçen gün, bilişim teknolojilerinin gelişmesi ile yenilenmelidir. Bunun sonunda, kanunlarımızı buna göre uyarlamak ve sürekli güncellemek

gerekmektedir. Aynı zamanda kanun maddesi düzenlenirken, teknik açıdan doğurduğu sonuçlar ve uygulanabilirliği de araştırılması gerekmektedir. Şüphesiz sadece hukuki alt yapının düzenlemesi yeterli olmayacak, ayrıca teknik altyapının da sağlanması ve her şeyden önemlisi bilişim sistemlerinin mantığının ülke insanı tarafından kavranması gerekecektir.

Bir diğer tartışma konusu ise, uzunca bir süreden tartışılan bu alana özgü Bilişim İhtisas Mahkemelerinin kurulmasıdır. Gerçekten bu tüp davalar uzmanlık gerektiren bir yapıya sahiptir. Fakat sadece mahkemelerin isimlerinin değiştirilmesi ile başarılı bir sonuca ulaşılması mümkün değildir. Özellikle Hakim ve Savcıların meslek içi eğitimine önem verilmesi gerekmektedir. Artık her davada bilişim sistemlerinin yer aldığı deliller sunulmaktadır. Her geçen gün insanların bu alana yönelmesi ile ortaya çıkacak hukuki ihtilaflarda bu alan genelinde gerçekleşecektir. Bu halde; bu yöndeki teknik eğitimlerinde arttırılmasında fayda vardır. Aynı zamanda bilişim şube'de görev yapan Adli Kolluk personelinin sürekli eğitilerek mesleğinde gelişmesi, yapılacak atamalarında yine bu alandaki şube veya bölümlerde yapılması sağlanarak böylece ihtisaslaşmış kalifiye personele sahip olunması gerekmektedir.

Görüldüğü üzere, bilgi teknolojileri her geçen gün kendisini yenilemektedir. Yükselen teknik imkanlar sayesinde, sürekli farklı suç tipleri meydana gelmektedir. Sadece meydana gelen suçlar açısından değil elde edilen imkanlar bakımından da bilgi ve iletişim teknolojilerinin önemi derhal kavranması gerekmektedir. Amerika Birleşik Devletleri bu konuda sürekli kendisini yenilemekte hatta ulusal stratejik varlıklarını korumak için siber güvenlik ordusu kurmaktadır. Zira ülkeler tüm sistemlerini ve tüm gizli bilgilerini artık dijital dünyaya aktarmaktadır. Ülkemizde de bu konuda ivedilikle çalışmalar yapılara ve dijital dünyada gerekli önlemleri almamız gerekmektedir.