TÜRKİYE'DEKİ BİLİŞİM SUÇLARININ SOSYOLOJİK BİR ANALİZİ: TEHDİTLER VE ÇÖZÜM STRATEJİLERİ

Furkan YILMAZ

(Yüksek Lisans Tezi)

Eskişehir, 2015

TÜRKİYE'DEKİ BİLİŞİM SUÇLARININ SOSYOLOJİK BİR ANALİZİ: TEHDİTLER VE ÇÖZÜM STRATEJİLERİ

Furkan YILMAZ

YÜKSEK LİSANS TEZİ

Sosyoloji Anabilim Dalı

Danışman: Doç. Dr. Fuat GÜLLÜPINAR

Eskişehir

Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

Aralık, 2015

Bu Tez Çalışması BAP Komisyonunca kabul edilen BAP-1507E560 nolu proje kapsamında desteklenmiştir.

JÜRİ VE ENSTİTÜ ONAYI

Furkan YILMAZ'ın "Türkiye'deki Bilişim Suçlarının Sosyolojik Analizi: Tehditler ve Çözüm Stratejileri" başlıklı tezi **15 Aralık 2015** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca toplanan **Sosyoloji** Anabilim Dalında, **yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

		İmza
Üye (Tez Danışmanı)	**: Doç.Dr.Fuat GÜLLÜPINAR**	.....
Üye	**: Doç.Dr.Zafer ÇELİK**	.....
Üye	**: Doç.Dr.Emre GÖKALP**	.....

Prof.Dr.Kemal YILDIRIM
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

Yüksek Lisans Tez Özü

TÜRKİYE'DEKİ BİLİŞİM SUÇLARININ SOSYOLOJİK BİR ANALİZİ: TEHDİTLER VE ÇÖZÜM STRATEJİLERİ

Furkan YILMAZ
Sosyoloji Anabilim Dalı
Anadolu Üniversitesi Sosyal Bilimleri Enstitüsü, Aralık 2015
Danışman: Doç. Dr. Fuat GÜLLÜPINAR

Bu çalışmanın amacı, teknolojik gelişmeler sayesinde hayatımızın her alanının dijitalleştiği günümüzde, bilişim suçlarının nedenlerini ve yarattığı riskleri, faillerin özellikleri ve motivasyonlarını sosyolojik açıdan analiz ederek, bilişim suçlarının izlediği seyir hakkında genel bir bilanço çıkarmaktır. Bu kapsamda bilişim suçlarının teorik açıklamaları, mevzuattaki yeri, bilişim suçlarıyla mücadele yöntemleri, sosyal medyanın bilişim suçu içindeki rolü ve suç öncesi koşullar ayrıntılı olarak soruşturulacaktır. Çalışmanın bulgularına göre, sosyal medya ve bilişim teknolojileri sayesinde işlenen suçların arttığı ve bu kapsamda bilişim suçlarından çocuk istismarı ve kişisel bilgilerin farklı amaçlarla suiistimali suçlarında ciddi düzeyde artış olduğu anlaşılmaktadır.

Son olarak, bu çalışmada bilişim suçlarındaki genel bilançosu değerlendirilerek eğitim, denetim, uluslararası işbirliği ve mevzuat ölçeğinde çözüm önerileri getirilerek, Türkiye'deki bilişim suçlarıyla mücadele edebilmek için bireysel ve kamusal ölçekte uygulanabilecek tedbirlere yer verilmiştir. Ayrıca, bilişim suçlarına yönelik devlet eliyle yapılacak denetimlerin yeterliliği ve yerindeliği konusu tartışılarak, denetimlerle kişi hak ve özgürlükleri ihlal edilmeden verilecek bir mücadele için nasıl bir yol izlenebileceği hakkında öneriler sunulmuştur.

Anahtar Kelimeler: Bilişim, Bilişim suçu, Sosyal medya, Suç, Fail, Türkiye.

Abstract

A SOCIOLOGICAL ANALYSIS OF CYBER CRIMES IN TURKEY: THREATS AND STRATEGIES FOR SOLUTION

Furkan YILMAZ

Anadolu University, Graduate School of Social Sciences, December 2015

Adviser: Assoc. Prof. Dr. Fuat GÜLLÜPINAR

The aim of this study, by analyzing in sociological view the reasons and risks of cybercrimes, the features and motivations of perpetrators, is to express general perspective about the pattern of cybercrimes, when every scope of life became digitalized owing to technology in nowadays. In this matter, detailed analysis of conceptual perception of cybercrimes, related legislation, methods of combatting with cybercrimes, the role of social media in cybercrimes and pre-crime conditions will be evaluate. According to findings of this study, it is came out the crimes via IT technology and social media increased and also the figure of child exploitation and privacy data abuse for various reasons as cybercrimes increased seriously.

Finally, in this study the precautions which can be apply in the private and public to combat cybercrimes in Turkey scale are stated by the solutions offering on the scale of education, control, legislation and international cooperation. Also, the propriety and the adequacy of the governmental controls against cybercrimes discussed and the solutions offered about how the controls combat cybercrimes without any violation of private rights and liberties.

Key words: Cyber, Cybercrime, Social Media, Crime, Perpetrator, Turkey.

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tez/proje çalışmasının bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumunda bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilmeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan bilimsel intihal tespit programıyla tarandığını ve hiçbir şekilde intihal içermediğini beyan ederim.

Her hangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

Furkan YILMAZ

Önsöz

Tez çalışmalarım süresince değerli yardımlarını eksik etmeyerek, çalışmalarımın her safhasında engin bilgileriyle beni yönlendiren, her konuda ilgi ve destek sağlayan, bu tezin tamamlanmasında benim kadar emeği olan, beni cesaretlendiren, benim elimden tutan, eksiklerimi kendi gayretleriyle kapatmaya çalışan, hocalıktan daha fazlasını yapan çok değerli danışman hocam Sayın Doç. Dr. Fuat GÜLLÜPINAR' a teşekkürlerimi sunarım. Böyle bir çalışma yapmak benim için ne kadar değerliyse, Sayın Fuat Hocam'ı tanımak ve onunla beraber çalışmış olmak da en az aynı derecede değerlidir.

Tez hazırlama sürecinde bana yol gösteren, değerli tavsiyeleriyle ışık tutan saygıdeğer hocalarım Doç. Dr. Emre GÖKALP'e ve Doç. Dr. Zafer ÇELİK'e teşekkür ederim, akademik hayatımda her zaman bu kadar şanslı olabilmem dileğiyle…

Hayatım boyunca maddi ve manevi desteklerini, dualarını eksik etmeyen yaşamımda başardığım her şeyi borçlu olduğum saygıdeğer anneme, babama ve kıymetli kardeşime sonsuz şükranlarımı sunarım.

Bu zorlu süreç içerisinde bana destek veren ve sabır gösteren sıralı amirlerime ve mesai arkadaşlarıma teşekkürlerimi sunarım.

Ayrıca BİDEB 2210 Yurt İçi Yüksel Lisans Burs Programı kapsamında yüksek lisans çalışmalarımı maddi olarak destekleyen TÜBİTAK'a da teşekkürlerimi sunarım.

Özgeçmiş

Furkan YILMAZ

Sosyoloji Anabilim Dalı
Yüksek Lisans

Eğitim

Lisans	2011	Polis Akademisi, Güvenlik Bilimleri Fakültesi
Lise	2007	Polis Koleji, Sayısal

Kişisel Bilgiler

Doğum yeri / yılı: 02.01.1989/Eskişehir Cinsiyet: Erkek Yabancı dil: İngilizce

İçindekiler

Şekiller Listesi

Kısaltmalar Listesi

ABD	Amerika Birleşik Devleti
AOL	American Online
ARPA-NET	Advanced Research Project Agency-Network
ATM	Automated Teller Machine
C.	Cilt
CIA	Central Intelligence Agency
CSA	Central Stupidity Agency
GB	Gigabyte
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protokol
ICQ	I Seek You
IP	Internet Protocol
IRC	Internet Relay Chat
İTÜ	İstanbul Teknik Üniversitesi
KGB	Devlet Güvenlik Komitesi (SSCB)
MPEG	Moving Picture Experts Group
MS	Microsoft
NASA	National Aeronautics and Space Administration
NSA	Naitonal Security Agency (ABD)
ODTÜ	Orta Doğu Teknik Üniversitesi

PHP	Personel Home Pages
RDS	Radio Digital Service
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
TC	Türkiye Cumhuriyeti
TD1	Adli Kopyalama Cihazı
TTNET	Türkiye Telekominikasyon A.Ş. İnternet Hizmeti
TÜBİTAK	Türkiye Bilim ve Teknik Araştırma Kurumu
TV	Televizyon
UNESCO	United Nations Educational, Scientific and Cultural Organization
Vb.	Ve benzeri/ Ve bu(gibi)
Wi-Fi	Wireless Fidelity
www	Word Wide Web

1. Giriş

Bu çalışma ile Türkiye'nin ve dünyanın yeni bir sorunu olan bilişim suçları bazı önemli boyutları açısından ele alınmaya çalışılmıştır. Bilişim teknolojilerinin hayatımıza nasıl girdiği ve insanların bilişim teknolojileri üzerinden nasıl suça bulaştıkları olduğu açıklanmaya çalışılmıştır. Bu noktada internet alışkanlıkları ve sosyal medya kullanımı konularına değinilerek, insanların bilişim teknolojileri sayesinde hangi mekanizmalar üzerinden illegal bir takım eylemlere yöneldikleri ortaya konulmuştur. Suç kavramı bilişim kavramıyla birlikte ele alınmış ve bilişim suçuna yol açan faktörler ve bilişim suçlarının sonuçları literatürdeki mevcut çalışmalar üzerinden tartışılmıştır.

Türk Ceza Kanunu ve diğer iç mevzuattaki bilişim suçlarına ilişkin hükümler incelenerek, başta internet kanunu olarak bilinen 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ele alınarak toplum üzerindeki etkileri sosyolojik açıdan analiz edilmeye çalışılmıştır.

Bilişim suçunun failleri bu suçu neden işledikleri ve hangi özelliklerdeki (yaş, cinsiyet, sınıfsal köken vb. değişkenler üzerinden) insanların bu suça meyilli oldukları sosyolojik ve kriminolojik teoriler ışığında analiz edilmiştir. Bilişim suçu faillerinin bu suçu işlemedeki motivasyonları; suç öncesi ve suç sonrası nedenler olarak iki farklı kategoride ele alınmıştır.

Türkiye'deki 2013-2014 yılları arasındaki istatistikleri ele alındığında bilişim suçlarının %28,9 arasında arttığı görülmüştür. Alaca'nın (2008) çalışmasında 2006 yılındaki Türkiye'nin bilişim suçlarındaki istatistiki durumu ortaya konmuştur. 2014 yılıyla kıyaslandığında 8 yıllık artışın yaklaşık 40 kat olduğu görülmüştür. 2013 ve 2014 yılları arasındaki en dikkat çekici yükselişin %133 artış ile çocuğun cinsel istismarı ve %129,5 ile çocuk pornografisi suçunda olması da düşündürücü ve önemli bir husustur. İlbaş (2009) çalışmasında toplum tarafından en ağır bilişim suçu olarak algılanan suç fiili olduğunu belirtmiştir.

Tüm bu bilişim suçlarının genel bilançosu üzerine sonuçlar kısmında Türkiye'deki bilişim suçlarıyla mücadele edebilmek için bireysel ve kamusal ölçekte uygulanabilecek tedbirlere yer verilmiştir. Kişisel ve kurumsal ölçekte alınabilecek bazı sistemsel ve

yapısal tedbirlere kısaca değinilmiştir. Durmaz (2005), çalışmasında bu tedbirlere detaylı olarak yer vermiştir; ancak bu çalışmada eğitim kısmında bilişim suçlarıyla mücadele eden görevlilerin eğitiminde bahsetmemiştir. Etkin mücadele için öncelikle aile ve çocukların eğitilerek bilinçli birer kullanıcı olması, daha sonrasında da bilişim suçlarıyla mücadele eden gerek kolluk kuvvetleri olsun gerekse yargı mensupları olsun görevlilerin eğitilerek etkin mücadelenin sağlanmasına değinilmiştir. Ayrıca, devlet eliyle yapılacak denetimlerin yeterliliği ve yerindeliği konusunda tartışmaya gidilerek; denetimlerle kişi hak ve özgürlükleri ihlal edilmeden azami verimlilikte bir mücadele için nasıl bir yol izlenebileceği hakkında öneriler sunulmuştur. Ayrıca sınır aşan niteliği olmasından dolayı bilişim suçlarıyla etkin mücadele için uluslararası işbirliğinin önemine ve mevzuata ilişkin bazı önerilere yer verilmiştir. Bilişim suçları ile mücadelenin, bilişim suçlarının temelindeki sosyolojik sorunlardan bağımsız olmadığı vurgulanarak bilişim suçlarının analizine sosyolojik bir bakış açısı kazandırılmaya çalışılmıştır.

1.1. Amaç ve Problem

Bu çalışmanın temel amacı hayatımızda oldukça önemli yer etmiş olan bilişim teknolojisinin, suç sosyolojisi açısından ne tür fırsatlar ve tehditler ortaya çıkardığını analiz etmektir. Bilişim suçları olarak adlandırılan fiillerin ülkemizdeki mevcut yasalarla nasıl yaptırımlara bağlandığı ve bu mevzuatların hangi değerleri korumaya çalıştığı ele alınacaktır. Ancak uygulamadaki yetersizlikler, failleri bilişim suçlarına iten nedenler, bilişim suçlarının tarihsel gelişimi ve Türkiye'deki işlenen suçlar birlikte ele alınıp, suçla etkin mücadeleye ilişkin çözüm önerileri getirilmeye çalışılacaktır.

Türkiye'de gittikçe artan bilişim suçlarının sayısı ele alındığında, özellikle bilişim yoluyla işlenen çocuğun cinsel istismarı ve çocuk pornografisi gibi uluslararası mücadelenin etkin yürütülmeye çalışıldığı ve toplumdaki etkileri bakımından oldukça hassas olan konulardaki artış yüzde yüzden daha fazla şekilde gerçekleşmiştir.

Bu çalışmanın temel problemleri şunlardır:

- Türkiye'de bilişim suçları kapsamına hangi eylemler girmektedir?

- Bilişim suçları failleri neden bu suçu işlemektedir?
- Türkiye'deki bilişim suçlarıyla mücadele nasıl yürütülmektedir?
- Bilişim suçlarıyla mücadele konusunda ne tür önlemler alınabilir?

1.2. Önem

Bu çalışmanın yanıtlayacağı sorularla, kısaca Türkiye'nin bilişim suçlarındaki mevcut durumu ortaya konulacaktır. Suçların nasıl gerçekleştiği, mevzuatta hangi suçların bilişim suçu olarak değerlendirilmesi gerektiği, faillerin hangi kastla bu suçun faili oldukları ortaya çıkarılmaya çalışılacaktır. Çalışmadan elde edilecek sonuçlar, kamu politikalarına yön verebilecek nitelikteki bürokraside yer alan uzmanlarla paylaşılarak güvenli internet kullanımı ve sosyal medya okuryazarlığı konusunda programlar oluşturulmasıyla, hem toplumun bilinçlenmesi, hem de bilişim suçu mağduriyetlerinin azaltılmasına katkı sağlayacaktır. Çalışmanın özellikle öneriler bölümünde, mağduriyetlerin ve etkin mücadelenin nasıl olacağına ilişkin öneriler getirilerek bilişim suçları konusunda adliyenin ve kolluk birimlerinin iş yükü azaltılarak devletin kaynaklarının daha verimli kullanılmasına yönelik değerlendirmeler yer alacaktır.

1.3. Sınırlılıklar

Bu çalışma Türkiye'de meydana gelmiş olan olaylarla sınırlıdır ve sonuçları yalnızca Türkiye kapsamında genellenebilir ve geçerlidir. Ayrıca, çalışmanın temel sınırlılıklarından birisi de çalışmada ele alınan bilişim suçları, Türkiye'de meydana gelip de, adliyelere ve dolaylı olarak da Siber Suçlarla Mücadele Daire Başkanlığı'na yansıyan olaylarla sınırlıdır.

1.4. Yöntem

Bu çalışmada araştırma modeli olarak, tarama yöntemi kullanılmıştır. Bu yöntemle Türkiye'deki mevcut olan bilişim suçları sorunu ortaya konulmaya çalışılmış ve geçmiş

yıllara ait elde edilen istatistiki veriler değerlendirilmiştir. Araştırma modeli, çalışma amaçlarına uygun olarak, verilerin toplanması ve çözümleme yapılabilmesi için koşulların düzenlenmesi (Karasar, 2005: 76) olarak tanımlanmaktadır. Durum tespiti niteliğinde olan bu çalışmada araştırma modeli 'genel tarama modeli'dir. Karasar (2005: 77) genel tarama modeli, "geçmişte ya da halen var olan bir durumu, var olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımı" olarak açıklamıştır. Bu şekilde Türkiye'deki bilişim suçlarının kavramsal ve hukuki algısı ortaya çıkarılmaya çalışılmış ve bu suçla ilişkin çözüm önerileri ortaya konulmuştur.

Bu tarama yöntemi ile bu alanda oluşturulmuş çalışmalar, hem ulusal çapta hem de uluslararası çapta ele alınmış ve konuya ilişkin sonuçlar birlikte değerlendirilmiştir. Bunun yanı sıra, bilişim suçlarının sosyolojik yönden ele alınmasına ilişkin çalışmalar değerlendirilerek, Türkiye'deki istatistiki verilerle değerlendirilmesi yapılmıştır. Bu sayede özellikle bilişim suçlarının faillerine ilişkin varsayımlarda bulunulmuş, bilişim suçunun ne olduğu, neden ve nasıl işlendiği sorularının yanıtlarıyla mantıksal çıkarımlar yapılarak Türkiye için bilişim suçlarına ilişkin çözüm önerileri sunulmuştur.

Literatür taraması sayesinde özellikle sınır aşan suç niteliğindeki bilişim suçlarına ilişkin uluslararası alanda yapılmış çalışmalarla birlikte yerli kaynaklardan azami düzeyde veri elde edilerek, bu verilerin değerlendirilmesi, problemin tanımlanmasında ve çözümlenmesinde göz ardı edilen hususların asgari düzeye indirilmesi hedeflenmektedir.

Değerlendirilen veriler, literatür taramasıyla elde edilenlerin yanında Türkiye'de işlenen bilişim suçlarına ilişkin Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'nın 2013 ve 2014 yılına ait suç türlerine göre işleniş sayıları kullanılmaktadır. Bu açıdan veriler açısından örneklem söz konusu değildir. Her ne kadar bilimsel araştırmalarda örneklem kullanmak çoğu açıdan birçok avantaj sağlasa da bu çalışmada örneklem kullanılmamıştır. Ancak, araştırmada yer verilen bazı sınırlı düzeydeki veriler Türkiye'deki işlenen bilişim suçlarıyla ilgili istatistikler olduğundan Türkiye evrenini belli ölçülerde temsil etmektedir.

Türkiye'deki işlenen bilişim suçlarının türlerine ve sayılarına ilişkin veriler, suç türlerine göre tek tek ele alınmış, literatür taramasından elde edilen verilerle birlikte sosyolojik ve kriminolojik açıdan analiz edilmiştir. Bu sayede her bir suç türü için

faillerin işleme sebeplerine ilişkin ve profillerine ilişkin açıklamalar yapılarak bu verilerin sınırlı düzeyde analizi yapılmıştır.

2. Hayatımızın Dijitalleşmesi

Castells'in de dediği gibi (2013: 1), bilgiyi temel alan teknoloji devrimi toplumun temel dinamiklerini yeniden şekillendirmiştir. Artık hiçbir şey eskisi gibi değildir. Yüz yıllarca gerek tekstil, gerek tarım, gerek matbaa alanlarında olsun teknolojik olarak dünyanın bir adım önünde olan Çin, sanayi devriminde ve takip eden yüzyıldaki bilgi devriminde ikinci planda kalmıştır.

Gün geçmiyor ki, yeni bir teknolojik gelişme yaşanmasın, yeni bir tanesi hayatımıza girmesin. Cep telefonları, bilgisayarlar, akıllı telefonlar, tabletler, akıllı saatler, wi-fi harddiskler, toplu taşıma için manyetik kartlar ve daha niceleri, eğer bunlardan herhangi birini kullanmıyorsak gerçekten türümüzün nadir örneklerinden biriyiz.

Artık çok boyutlu iletişimler gerçekleşmekte, yazılı, görsel, işitsel hatta tensel iletişimler günümüzde olmaktadır. Bunun çıkış noktasının internetten önce video kayıt cihazlarının yaygınlaşması da diyebiliriz. Bu cihazlarla birlikte insanlar görsel, işitsel içeriği kendileri oluşturabilmişler ve içeriğe yeni anlamlar katarak, bu anlamda güç kazanmışlardır.

Bir bebek dünyaya geldiği an, soyadıyla beraber kayıtlarda yer almaya başlamaktadır. İsmi kayıtlara geçirilip, Türkiye Cumhuriyeti vatandaşı olmasıyla on bir haneli bir numara ile sayısallaşmış olmakta ve bu sayede dijital veri haline gelmiş bir kimlik kazanmaktadır.

İnternetle birlikte insanların iletişim biçimleri radikal bir biçimde değişmiştir. Artık hiçbir şey eskisi gibi değildir. İnsanlar arası iletişimin mesafe tanımaksızın, çok boyutlu hale gelmesi sosyolojik bir varlık olan insan için hayatta büyük değişimlerin habercisidir. Denizaşırı ülkelerden görüntülü konuşmak mümkün hale gelmiştir. On binlerce kilometre uzaklıkta bulunan bir veri saniyeler içinde başka mekânlara aktarılabilmektedir. İnternetin sahip olduğu bu imkânların yanında günlük hayatımıza ilişkin birçok ihtiyacımızı da gidermekteyiz. İnternet üzerinden ödeme yapan, bilet alan, alışveriş yapan, sınava başvuran, araştırma yapanların sayısı günden güne artmaktadır.

2008'den beri Türkiye'de faaliyet gösteren E-devlet uygulaması da bu dijitalleşen hayatımızın bizlere sunduğu kolaylıklardan. Vatandaşlar E-devlet uygulaması sayesinde

devletle ilgili işlerini internet üzerinden takip edebilmektedir. Vatandaşlar kişisel bilgilerine ilişkin sorgular yapabilmektedir E-devlet olanakları sayesinde 197 kurumdan toplam 1300 hizmet sunulmaktadır.[1]

Kısacası hayatımıza bilişim her gün daha fazla girmekte ve hayatımız bir bakıma dijitalleşmektedir ancak bilişim alanındaki bu devasa gelişmeler bir yandan hayatımızı kolaylaştırmakta bir yandan da beraberinde bazı riskleri de getirmektedir.

2.1. Bilgisayar

Bilgisayar kelimesi İngilizcede yer alan *"computer"* kelimesinin Türkçe karşılığıdır. İngilizce *"to compute*= hesaplamak" kelimesinden türetilerek oluşturulan *"computer"* kelimesinin Türkçe karşılığı "kompüter (Kurt, 2005: 29)", elektronik beyin", "bilgileri otomatik işleme tabi tutan sistem" (Dülger, 2004: 220), *"ordinatör"* (Yenidünya ve Değirmenci, 2003; Kurt, 2005: 157, Dülger, 2004: 220) olarak çevrilmektedir. Bilgisayarları, "uzun ve karmaşık hesapları dahi büyük bir hızla yapabilen, lojik (mantıksal) bağlantılara dayalı karar verip işlem yürüten" makineler olarak tanımlayabiliriz (Topaloğlu, 1997: 19). Yazıcıoğlu'na (1997: 28) göre ise bilgisayar "veri saklayabilen, depolayabilen ve bunları işleyebilen, depolanmış bir programı işletebilen ve işlem akışı ile sırasını otomatik olarak değiştirebilen bir aygıt" olarak tanımlamaktadır. Kardaş ise bilgisayarı, "aritmetik ve mantık işlem dizileriyle oluşturulmuş programlara göre verileri otomatik olarak işleyen makinedir." (Kardaş, 2003: 8) Değirmenci de bilgisayarı, "dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan işleyen, yeni sonuçlar üreten, veri iletişimini sağlayan makine" şeklinde tanımlamaktadır (Değirmenci, 2002: 10).

Topaloğlu ise, "Bilgisayar; belli kurallar dahilinde verileri işleyerek sonuçlar elde eden ya da problem çözen bir makinedir. Bilgisayar, bir veya birden fazla görevi yerine getirmek üzere meydana getirmiş parçalar bütündür." şeklinde tanımlamıştır (Topaloğlu, 2014: 25).

[1] https://www.turkiye.gov.tr/ (Erişim tarihi: 20.09.2015)

Dülger'e (2004: 43) göre bilgisayar; "bir giriş – çıkış aygıtı ve bir belleği bulunan, her türlü simgeleştirilmiş işlemi yapabilen ve bu işlemleri belleğine kaydedilmiş yazılımlarla gerçekleştirilen bir ana işlemciye sahip, veriler üzerinde dönüştürme işlemi yapan işletim sistemi bulunan, bilgileri belirli bir düzende saklayan, üzerine farklı yazılımlar yüklenebilip aynı yöntemle çıkartılabilen, veri iletişimini sağlayan, salt bir konuya özgülenmemiş, her türlü işlemi yapabilmek için genel amaçlı olarak üretilmiş makinelerdir."

Bilgisayar, teknolojinin kendini en iyi göstergesidir. Vücut bulmuş halidir. Tüm teknolojik işlemler, bilgisayar veya bilgisayarların temeli niteliğindeki mikro işlemciler üzerinden gerçekleşmektedir. Diğer taraftan bu çalışmanın esas konusu olan bilişim suçları için de aynı derecede önem arz etmektedir. Tüm bilişim suçları bir şekilde bilgisayarlar kullanılarak veya bilgisayarlar hedef alınarak işlenmektedir. Bu sebeple bilgisayar, hem kavram olarak hem de teknik yapısı itibariyle bilişim suçları için hayati bir önemdedir.

2.2. İnternet

İnternet, yeni bir iletişim ağı olarak yüzyılımıza damgasını vurmuştur. Tüm fırsatlarının yanında, barındırdığı tehditlerle de gün geçtikçe adından söz ettirmeye devam etmektedir. Bilişim suçlarının büyük bir çoğunluğu internet vasıtasıyla işlenmektedir. İnternet, bilişim suçunun ilk faktörü olan bilgisayarları birbirine bağlamaktadır. Bu sayede de fail dünyaya açılabilmekte ve işleyeceği suçlar için uygun hedefler belirleyebilmektedir. İnternet, fail ile mağdur arasında, onları birbirine bağlayan bir köprü vazifesi görmektedir. Bu çalışmada, bilişim suçlarının işlenişi ve doğasının daha iyi anlaşılması için internetin yapısına ilişkin açıklamalara ihtiyaç duyulmuştur.

Ağların ağı olarak da adlandırılan internet, *"international*" ve *"network"* kelimesinin bir araya gelmesinden oluşmaktadır (Yenidünya ve Değirmenci, 2003: 36). İnternet, birden fazla haberleşme ağının birlikte meydana getirdikleri, tüm bilgilerin paylaşıldığı ve bilgisayarlar arasında karşılıklı olarak iletildiği bir ağdır (Özdilek, 2002: 13). "İnternet dünya üzerindeki irili ufaklı bilgisayar ağlarının aralarında tekrar bağlantı kurmaları ile gelişen ağlar arası bir ağdır (Sınar, 2002: 23). Böyle ağların toplamından

oluşan internet, bilgiye ve bilgisayar kaynaklarına global erişimi sağlamaktadır (Yaycı, 2007: 14). Ketizmen (2008: 36) ise interneti, "genel olarak veri işleme faaliyeti merkezinde çalışan bilgisayar sistemlerinin, veri iletim esaslı, elektronik iletişim olanaklarını kazanması" olarak açıklamaktadır.

Nihayet internet sayesinde, insan iletişiminin yazılı, sözlü, görsel-işitsel biçimlerini aynı sistem içinde bütünleştiren bir hiper metin dili gelişmiştir (Castells, 2013: 440). Bu yazının icadı gibi, alfabenin bulunması gibi insanlık için büyük bir adımdır. Yeni bir iletişim kanalıdır, çok boyutludur. Kültür de iletişimle aktarıldığı için ve kendini oluşturan din ve geleneklerin işlenişi, aktarımı temelden değişmiştir. Bunun anlamı da internetin aslında sadece bir iletişim, bilgi aktarım yolu olmadığı, çok daha makro değişimlere yol açtığı ve daha büyüklerine de gebe olduğudur.

ABD (Amerika Birleşik Devleti) Savunma Bakanlığı'nın, olası bir savaşta iletişim kesintisi tehlikesi yaşamayacağı bir iletişim ağı kurma isteği, internetin düşünsel temelini oluşturmaktadır (Yenidünya ve Değirmenci, 2003: 37). ARPA tarafından geliştirilen internet, aslında Soğuk Savaş sürecinde ABD'nin Sovyetler Birliği'nin önüne geçme kaygısının ürünü olduğu söylenebilir. İlk olarak 1969 yılında, Kaliforniya'da yer alan üç ayrı bilgisayar ve Utah'da yer alan bir bilgisayar arasında veri transferi gerçekleştirilmiştir (Sınar, 2000: 22). Sonraki aşamada ise, bu dört bilgisayar arasındaki ağ sistemi geliştirilerek ARPANET adında askeri bir ağ kurulmuştur (Cerf vd., 2009). Aslında bu düşmanın gücüne hareket kabiliyeti ve arazi handikaplarından bağımsızlığı ile karşı koymak için gerilla güçlerinin Maocu taktiklerinin elektronik bir dengiydi ve bunun sonucunda da hedeflendiği gibi merkezden kontrol edilemeyen, birbirleriyle sayısız biçimde bağ kurabilen özerk bilgisayarların ağ mimarisi oldu (Castells, 2013: 8). 1980'li yılların sonunda ise, internet ABD'nin yanı sıra İngiltere ve Japonya gibi ülkelerde de yaygınlaşmıştır (Sınar, 2000: 23).

1986 yılında, Amerikan Ulusal Araştırma Kurumu'nun internetin iletişiminin temel yapıtaşını oluşturan NFSNET'i kurması (Cerf vd., 2009) dönüm noktası olmuştur. 1989 yılında world wide web (www) teknolojisinin, 1990 yılında ise en temel dosya transfer protokolünün - http - geliştirilmesi ile ARPANET iptal edilmiş, bütün ağ omurgalarının tek bir yapıda birleştirilmesi ve internetin bireysel kullanıma açılmasıyla milyonlarca

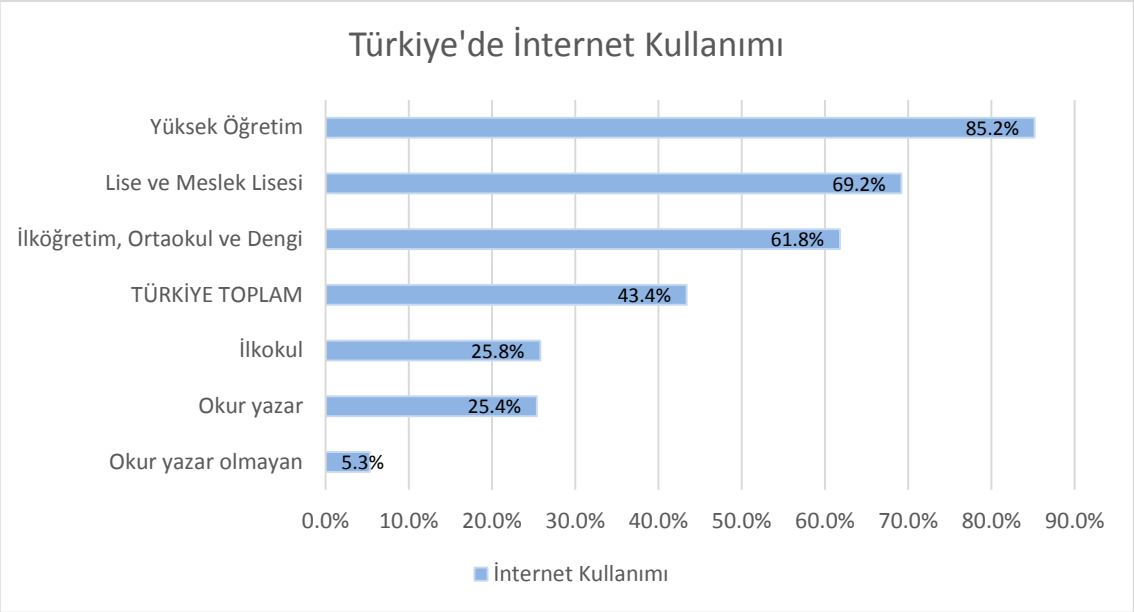
bilgisayar kullanıcısının tek ağa bağlanması gerçekleşmiş ve internet yaygınlaşmıştır (Sınar, 2000: 22 Özdilek 2001: 78). Yalçın (2003: 78) ise, internetin yaygınlaşmasının, "başıboş bırakılmasına" bağlı olduğunu belirterek bu başıboşluğun interneti çekici kıldığını belirtmektedir.

Şöyle ki, bu başıboşluğun ilk çıkış noktasını askeri bir amaçla kurulmuş olan ARPANET'e dayandırmak çok mümkün değildir. ARPANET yaklaşık 20 yıl bilgisayarlar arası ağı olma görevini üstlenmiştir. Daha sonrasında modası geçtiği için 1990 yılında kapatılmıştır. Bundan sonra internetin iskeleti olma görevi Ulusal Bilim Vakfı'nın işlettiği NFSNET tarafından yerine getirilmiştir (Castells, 2013: 59). Ancak ticari baskılar, özel şirketlerin bu özel ağlar arasında işbirliği için ortak hareket etmesiyle hükümetin kontrolündeki internet hizmeti tamamıyla özelleştirilmiş ve 1995 yılından itibaren özerk, başıboş bir internet meydan gelmiştir.

Ülkemizde ise internet deyince akla ilk gelen kurum ODTÜ (Orta Doğu Teknik Üniversitesi)'dür. İlk defa 12 Nisan 1993 yılında, TÜBİTAK (Türkiye Bilim ve Teknik Araştırma Kurumu) tarafından desteklenen bir projeye bağlı olarak ODTÜ'de gerçekleştirilen bağlantının temel amacı, akademik çevrede bilimsel veri iletişimi için kullanmaktır (Dülger, 2004: 61).

Subaşı'nın (2005: 106) da dediği gibi internet ile birlikte girişimci eğilimler, kendilerini devletin baskısı veya sermayenin tahakkümü olmaksızın ifade edebilmektedir. Bu araç diğer ifade araçlarına göre o kadar farklıdır ki: herhangi bir denetim, ambargo olmaksızın yeni düşünce ve kültürler üretilebilmektedir.

İnternetin en büyük getirdiği yenilik, bireyler için mevcut kimliklerinden bağımsız, herhangi bir gözetime tabi olmaksızın kendilerini ifade edebildiklerine olan inançtır. Çünkü yasalar genelde koyuldukları devletlerin egemenlik sınırları içinde geçerlidir; ancak internetin tabi olduğu bu tip bir egemenlik alanı mevcut değildir. Bu sebeple de insanlar kendilerini daha özgürce ifade edebilmektedirler.



Şekil 2.1. Türkiye'de Eğitim Durumuna Göre İnternet Kullanımı (Temmuz 2013)[2]

Şekil 2.1'de Türkiye'de eğitim durumuna göre internet kullanımı gösterilmektedir. Türkiye'de %43,8 oranda aktif internet kullanıcı bulunduğu ve internet kullanımının eğitim seviyesi artıkça artma eğilimi görülmektedir.

2.3. Sanal Cemaatler

Bilişim suçları ileriki bölümlerde de detaylı ele alınacağı şekilde, bir suç fırsatı olarak, muhtemel suçlu, suça karşı yetenekli koruyucunun yokluğu ve bunların yanında uygun hedefin varlığı sayesinde meydana gelmektedir. Bu bölümde insanın neden bilişim suçu mağduru olacağı ortamlardan biri olan sosyal medyaya ve diğer dijital sosyalleşme ihtiyacını duyduğu açıklanmaya çalışılmıştır.

Tonnies'in 1887'de yazdığı Gemeinshaft und Gesellshaft (Cemaat ve Cemiyet) isimli eserinde, modern kapitalizmin sonucunda giderek salt-ekonomik egemenliğin boyunduruğuna giren bir toplumdan bahsetmektedir. Modern toplumların, sanayi öncesi

[2] IAS Türkiye İnternet Ölçülmesi Araştırması, Yapısal Çalışma (2013) http://pro.webrazzi.com

toplumlarının toplumsal ilişkilerin var olan sahiciliği ve doğallığını kaybettiklerini savunmuştur (Swingewood, 1998: 129).

Cemaat diye adlandırılabilecek olan sanayi öncesi toplumlarda, toplumsal ilişkiler samimidir. Dayanışma ruhu ve ortak irade ön plandadır. Aile hayatı ve birincil yüz yüze ilişkiler toplumun temel motorudur. Öte yandan cemiyetlerde ise durum çok farklıdır. Kentlerdeki yaşam bu kapsamda değerlendirilebilir. Kentlerde cemiyet tarzı sosyal ilişkilerin oluşumunda hukuk, sözleşmeler, rasyonellik, tek başınalık ve kişisel çıkar ön plandadır (Bozkurt, 1999: 66). Artık bakkalların yerini büyük alışveriş merkezlerinin alması, birbirini tanımayan komşuların varlığı cemaat toplumunda ziyade, cemiyet toplumunda yaşandığını göstermektedir.

Bazı sosyologlara göre, modern insanın en önemli özelliği tek başına olması, yalnız olmasıdır (Bozkurt, 1999: 65). Kent yaşamında, insanlar için ilişkiler daha yüzeysel, daha rasyonel hale gelmektedir. İlişkiler çıkar odaklı şekillenmektedir. Bu sebeple de insanlar tek başınalığı toplumsal bir kültür olarak, istemsizce yaşamaktadırlar. Bu noktada insanlar ne kadar tek başınalık içinde olsalar da, yalnız kalmış olmak istemezler ve kendi ilgilerine, kendi seçimlerine göre dâhil oldukları sanal cemaatler önem kazanmaktadır.

Kendisini internet bağımlısı olarak tanımlayan ve birçok sanal cemaatin kurucusu olan Rheingold, sanal cemaati "kişisel ilişkiler ağının yaratılması için yeterli sayıda insan bir araya geldiğinde, networkler (internet) vasıtasıyla yaratılan sosyal gruplardır." şeklinde tanımlamaktadır (Bozkurt, 1999: 67). Sanal cemaatler için cemaatlerdeki gibi ortak paylaşılan şeylerin varlığı kaçınılmazıdır; ancak ortak bir mekânsal birliktelikten söz etmek imkânsızdır.

Öte yandan, her ne kadar sanal cemaatlerdeki iletişimin ve ilişkilerin yüz yüze ilişkiler kadar sahici ve samimi olmadığı düşünülse de, güvensiz dışarı yerine, güvenli evde kurulan ve sürdürülen ilişkiler günümüz toplumunda tercih sebebi olabilmektedir. Hatta şöyle ki, sanal cemaatler dışarıda bir ilişki kurmak için yeterli fiziksel gücü olmayan yaşlılar ve sakatlar için de yeni fırsatlar sunabilmektedir (Bozkurt, 1999: 68).

Cemiyet toplumunun özelliği olarak ortaya konulan tek başınalıkla birlikte ortaya çıkan bireyselleşme ve toplumsal çözülmeye karşı toplumsa bağların güçlenmesinde

internetin önemli bir yeri vardır. Her ne kadar samimiyetsiz olarak atfedilse de internet ortamındaki ilişkiler, bireyin toplumsal baskılardan ve değer yargılarından uzaklaşıp anonim olarak fikrini ortaya koyabilmesi bir açıdan daha samimi bir ortam sunduğunu ortaya koymaktadır (Castells, 2013: 479). Ama samimiyet ne kadar yüksek olursa olsun ilişkiler yüz yüze olmadığı için kalıcılığı da sorguya açıktır.

Sanal cemaatler sayesinde bireyler, toplumsal etiketlerinden ve yargılardan sıyrılarak yeni oluşturulan personalar ile olmak zorunda oldukları kişi değil de, olmak istedikleri kişi gibi davranabilmektedir. Bunun sonucunda gerçek hayatta olamadıkları şekilde mutlu olabilmekte ve kişisel tatmine ulaşabilmektedirler. Sanal cemaatlerin tamamen gerçek dışı olduğunu varsaymanın diğer yanılgısı da, birey sanal platformlarda kurduğu ilişkileri, memnuniyet derecesine göre gerçek hayatına taşımayı istemektedir.

Sanal cemaatler bireylerin kendini özgürce ifade edebilmelerini sağladığı için özellikle Twitter gibi platformlarda demokrasinin en üst düzey örneklerini görebilmekteyiz. Her bir birey kitlelere sesini duyurabilme yeteneğine sahip olmakta bu sayede demokrasiye katılım sağlayabilmektedir.

Welmann, (2013'ten aktaran Castells, 2013, s. 477) sanal cemaatin fiziksel cemaate karşı olmadığına dikkat çekmektedir. Asıl olanın kişisel cemaat olduğu ve ilişkilerin yakın ve dar çevredekilerden, uzak ve zayıf bağlar kurduğu bir yelpazede varlığını sürdürdüğüdür. Cemaatler, sosyal ağların kurulduğu bir platformdur, aynı şekilde internette bu alternatiflerden biridir. Bu sebeple fiziksel cemaatle sanal cemaat birlikte aynı amaca hizmet edebilmektedir.

Sanal cemaatin oluştuğu en geniş platform olan internetin ve dolaylı olarak sosyal medyanın bu fonksiyonu kazanabilmesi için önemli olan bilgi ve metin topluluğundan ziyade topluluğu oluşturacak şekilde ustaca düzenlenmiş ilişkileri çerçevesinde sosyal açıdan anlamlı hale gelmesidir (Baym, 2010: 404).

Sonuç olarak, bireyler sosyal bir ihtiyaç olarak sanal cemaatlerin içinde yer almaktadır. Yukarıda da detaylı belirtildiği üzere dijital ortamda kurulan bu ilişkilerin birçok olumlu fonksiyonu vardır. Ancak sanal ilişkilerin kurulduğu bu platformlarda tüm bu olumlu yönlerinin yanında kişilerin güvenilmez ortamlarda bulunması, aldatılması,

dolandırılması veya çocukların uygunsuz içeriklere maruz bırakılması gibi bir tür bilişim suçunun mağduru olma ihtimalini de barındırmaktadır.

2.4. Sosyal Medya

2.4.1. Sosyal medya nedir?

Sosyal medya deyince akla Facebook başta olmak üzere Twitter, Instagram, Mynet Oyun gibi kişilerin internet üzerinde vakit geçirdikleri platformlar gelmektedir. Sosyal medya, sanal topluluklar ve ağlar üzerinde insanların kendi aralarında bilgi ve fikirlerini ürettiği, paylaştığı veya değiştiği sosyal etkileşimdir (Ahlqvist vd., 2008: 13). Kaplan ve Haenlein (2010:61) ise sosyal medyayı "Web 2.0 üzerinde ideolojik ve teknolojik içeriklerin, kullanıcı merkezli üretilmesine ve paylaşılmasına müsaade eden internet tabanlı uygulamaların bütünüdür" şeklinde tanımlamaktadır.

Bir diğer tanıma göre ise "sosyal medya, özünde, insanların karanlığa haykırıp, birilerini duymasını beklediği yerdir. En temel özelliği etkileşimli bir kurgu oluşturmasıdır. Zaten sosyal kelimesinin geldiği yer de işte bu interaktivitedir: Siyasetçi için seçmene ulaşma yolu; meşhur olmak isteyenler için fırsat kapısı; sanatçılar için eserleri tanıtabilecekleri bir yer; sivil toplum örgütleri için haberleşme ve bilgilendirme aracı… Tabi bireysel açıdan da çok değerli bir platformdur: birebir iletişim, kendine açık alanda ifade edebilme imkânı, iş arayabilme ve iş imkânlarını yönetebilme, yeni kişilerle tanışma ve sosyalleşme, anlık haber ve bilgiye ulaşabilme, eğlence vb. Hatta bu tarz platformları profesyonel olarak kendine sevgili bulabilmek için kullananlar ve hatta bunun için her gün mesai harcayanlar bile mevcut." (Tuncer, 2014: 15 - 17).

Yapılan tanımlardan anlaşılacağı üzere sosyal medya için sadece vakit geçirme, eğlenme işlevinin olduğunu söylemek kullanıcı sayısı milyarlarla ifade edilen bu platforma haksızlık etmek olur. Hoş vakit geçirmek, evet sosyal medyanın fonksiyonlarından biridir ancak; adından da anlaşılacağı üzere en önemli özelliği *sosyal* olmasıdır, içinde etkileşimi barındırmasıdır. Yani hoş vakit geçirmek için film izlenen bir internet sitesi sosyal medya sitesi değildir, ne zaman izlenen film ile ilgili altına

yorumlar yapılıp, içerikler oluşturularak etkileşim başlarsa, o zaman bu hoş vakit geçirilen ortam, sosyal olma özelliğini kazanmaya başlar.

Sosyal medya sitelerinin başında Facebook gibi içinde her şeyi barındıran komple yapıda bir örneğin olması, insanlar için genelde oyun oynamak, arkadaşlarından haber almak, onları izlemek, görüşüne uygun içerik barındıran gündemi takip etmek, eğlenceli video izlemek, karikatür okumak gibi zaman geçirmek ekseninde kullanıldığı için en önemli işlevinin bunlar olduğu düşünülebilir. Aslında tüm bu barındırdığı hizmetlerin temelinde etkileşim bulunmaktadır.

Sanal ortam, coğrafi sınırları kaldırmanın da ötesinde, işitsel, görsel ve oral tüm evreleri bünyesinde barındırarak toplumların birbirleriyle eş zamanlı iletişim kurmalarını sağlamaktadır. Bu durum firmalar için de çok önemli faydalar sağlamıştır. Dijital ortamları kendileri için bir fırsat gören firmalar; önce elektronik postalar, intranetler ve ekstranetler yoluyla eş zamanlı olarak personeliyle, aracı kuruluşlarıyla, tedarikçileriyle, müşterileriyle ve sosyal paydaşlarıyla iletişim kurup etkileşimde bulunurlar, reklam ve halkla ilişkiler uygulamalarını bu ortamlarda hayata geçirirken, daha sonra web sitesi kurarak tanıtımlarını yapmaya başlamışlardır (Onat vd., 2008: 1111).

Sosyal medya siteleri üzerinden Türkiye'de bulunan hemen hemen bütün alanlardaki firma hesaplarına ulaşmak mümkündür. İnternet arama motorları üzerinden "ara" sekmesinden üzerinden istenilen ürüne hangi firmalarda bulunduğunu, ürün hakkında görüş, şikâyetlerin ve önerilere ulaşabilmektedirler. Eğer firma ya da ürün hakkında bir şikâyet veya önerileriniz varsa firma yetkilileri kullanıcılarla DM (direct message) yoluyla hızlı bir şekilde iletişime geçebilmektedir. Bu durum müşteriler için çok kullanışlıdır. Diğer yöntem olan telefon ile müşteri temsilcisine ulaşmak zor ve sıkıcı bir durumdur.

Bu sebeple etkileşim temelinde yapılan sosyal medyaya dair tanımlarda sosyal medyaya duyulan ihtiyacın ne olduğu da ele alınarak yeniden bir tanım üretilmeye çalışılacaktır. Bunun için başlıca sosyal medya araçlarına kısaca bakmak gerekir.

2.4.2. Sosyal medya araçları

Facebook

2004 yılında Mark Zuckerberg tarafından Harvard Üniversitesi öğrencileri için kurulan bir sosyal paylaşım sitesidir. Daha sonrasında büyüyerek önce ulusal çapta hizmet verirken daha sonrasında ise uluslararası bir nitelik kazanmıştır. Günümüzde ise dünyada en çok ziyaret edilen Google'dan sonra 2. internet sitesidir. Bunun anlamı sadece arama motoru olan Google'a geçilen site en çok ziyaret edilen sosyal medya sitesidir.[3]

Tüm dünyadaki kullanıcı sayısı Ocak 2014 araştırmalarına göre 1 milyar 300 bin üzerindedir. Bu kullanıcıların %48 i günlük olarak Facebook'a girmektedir. Bunun 680 milyonu mobil olarak da kullanmaktadır.[4] Bu istatistiklere bakıldığında ne kadar muazzam bir platform olduğu gözler önüne serilmektedir.

Facebook'un fonksiyonlarına baktığımızda;

-Kişisel fotoğraflar ve diğer bilgilerin paylaşılması,

-Gruplar üzerinden alıcı ve satıcının bir araya geldiği bir pazar yeri,

-Arkadaşlarla veya tanımadığı kişilerle mesajlaşma, iletişime geçme,

-Etkinlikler düzenleme, davet etme

-Trajik, komik veya farklı gerekçelerle ilginç gelen haber, video vs.nin paylaşılması,

-Oyunlar gibi uygulamalar ile eğlence imkânı olarak görmekteyiz.

Özellikle kullanıcılarına sunduğu uygulama geliştirme özelliği ile kendi komple olan yapısını uçsuz bucaksız hale getirerek, insanların oyun oynamaktan, video izlemeye, arkadaşlar edinmekten, haberleri takip etmeye kadar her türlü ihtiyacını karşılamaya yönelik bir yapı edinmiştir.

[3] http://www.alexa.com/topsites (Erişim tarihi: 15.08.2015)

[4] http://www.statisticbrain.com/facebook-statistics/ (Erişim tarihi: 15.08.2015)

Bu fonksiyonları sayesinde gerçek hayatta da olan arkadaşlarıyla yaptığı paylaşımların sınırları zorlanmakta, yeni arkadaşlar edinerek farklı heyecanları ve duyguları tatmaktadır.

Twitter

2006 yılında sosyal ağ ve mikroblog sitesi olarak kurulmuştur. 140 karakterlik metin kısıtlaması ile kısa ve öz içeriklerin oluşturulmasına mecbur bırakmaktadır. Bu mecburiyet bir sınırlama gibi gözükse de aslında Twitter'ın en önemli artı değeridir. Irak ve Yazıcıoğlu'nun (2012: 18) eserinde belirttiği gibi "Twitter'ı farklı kılan, Facebook'un güçlü olduğu yerden değil, onun var olmadığı yerden girişmesi oldu. Facebook güçlüydü, çünkü dört başı mamurdu, ayrıntılıydı, zengindi. Facebook'un olmadığı bir şey vardı, basit değildi. 3G ve büyük ekranlı akıllı telefonlar öncesinde Facebook'u bir mobil cihazda açmanız gerekse dakikalar boyu beklemeniz gerekirdi ve o küçücük ekranda çıkandan pek bir şey anlayamazdınız. Facebook o haliyle mobil dünyaya yani internet teknolojisinin bir sonraki adımına tam da hazır sayılmazdı. Twitter ise tamamen o dünya için yaratılmıştı. Site basitti ve sırtını tamamen buna yaslıyordu."

Twitter dünyada en çok ziyaret edilen siteler sıralamasında 7. sırada yer almaktadır.[5] Sahip olduğu kullanıcı sayısı yaklaşık 650 milyondur.[6]

Twitter'ın en önemli özelliği anında oluşudur. Anında olarak milyonlarca kişiye ulaşılabilmektedir. Bu da Facebook'ta ön planda olan arkadaş olma engeline takılmaksızın, tüm ülkeye kimi zaman tüm dünyaya ulaşabilme imkânını sunmaktadır. Özellikle atılan tweetlere hashtag (#) ekleyerek belli bir etiketle yayılmasını sağlayarak gündem oluşmasında etkisi olabilmektedir. Bu şekilde Trending Topic (TT) listesine giren bir hashtag aynı gün üçünde geleneksel medyada kendine yer edinebilmektedir.

Ayrıca takip ederek ilgilenilen ünlü bir kişinin, bir siyasetçinin, bir haber ajansının paylaşımları anlık olarak takip edilebilmekte, istenilen içeriklere ulaşılabilirken, Facebook'un aksine kişi sesini herkese duyurabilmektedir. Türkiye için bunun en

[5] http://www.alexa.com/topsites (Erişim tarihi:15.08.2015)

[6] http://www.statisticbrain.com/twitter-statistics/ (Erişim tarihi:15.08.2015)

önemli örneği 2013 yılı Mayıs ayı sonunda yaşanan Gezi Parkı olaylarının, yüzbinleri bulan #geziparkı hashtagi ile dünya TT listesine girmeyi başarmasıdır.

Youtube

2005 yılında *Broadcast yourself; Kendini yayınla* sloganıyla kurulan kullanıcıların video yüklemesine imkân sunan bir internet sitesidir. Videolar aracılığı ile etkileşim imkânı sunmaktadır. Bu platformda insanlar yayınladıkları videolar ile ön plana çıkabilmekte, sosyal mesaj verebilmekte ve hatta ünlü olabilmektedirler. Justine Bieber ve PSY (Gangnam Style) en tanınmış Youtube ünlüleridir.

2.5. Türkiye'nin Bilişim Teknolojileriyle Tanışması ve Kullanımı

2.5.1. Türkiye'nin internetle tanışması

Ülkemizde internet 12 Nisan 1993′de 64 Kbps kapasiteli kiralık hat ile ODTÜ Bilgi İşlem Daire Başkanlığı sistem salonundaki yönlendiriciler kullanılarak, ABD'de NSFNet (National Science Foundation Network)'e TCP/IP protokolü üzerinden Türkiye'nin ilk internet bağlantısı gerçekleştirilmiştir.

1997 yılında tüm halka sunulduğunda ise yılsonu tahmin edilen kullanıcı sayısı 250.000[7] civarında iken, günümüzde internet kullananların sayısı Türkiye nüfusunun %55,9'una ulaşmıştır.[8] Bunun büyük çoğunluğu mobilden de bağlanabilmektedir.

Ülkemizde internetin ilk dönemlerinde doksanlı yılların ikinci yarısına tekabül eden dönemde, internete çevirmeli hatlar üzerinden bağlanılmaktaydı ve hızı 14,4 Kb/s idi. Bu hız şu an evlerde kullanılan internetin yaklaşık binde birini tekabül etmektedir. O dönemki teknoloji web 1.0dı. Bunun anlamı internet sitelerindeki içerikler sabit, değişimi zor, geri dönüş mekanizmasından yoksun ve tek taraflıydı.

Aynı dönemde Türkiye'de AVM (Alışveriş merkezi) ve gökdelenler dönemi henüz başlamış ve insan ilişkileri halen yer yer sıcak ve Tonnies'in cemaat toplumu, şehirlerin

---

[7]http://www.socialmediatr.com/blog/turkiyede-internetin-kisa-tarihi/ (Erişim tarihi: 26.10.2014)

[8]Türkiye İstatistik Kurumu - Hanehalkı Bilişim Teknolojileri Kullanım Araştırması (2015) http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660 (Erişim tarihi: 20.11.2015)

merkezine hâkim olmasa da ülke genelinde hâkim bulunmaktaydı. O dönemde çocuk olanlar için eğlence, sokakta top oynamak, saklambaç oynamaktı. Çünkü internetin evlerde bulunması çok nadir, hatta internetten öte bilgisayara sahip olmak bile bir prestij göstergesiydi.

Bu dönemde internetin halka ulaşamamış olması, ulaşanların da çok düşük bağlantı hızıyla ulaşması; öte yandan sokakta sosyalleşme imkânının bulunması yüzünden internet siteleri özellikle sosyal medya siteleri yaygınlaşamamışlardır. İlk sosyal medya siteleri için ülkemizde çok varlık gösterebildikleri söylenemez (bkz. Şekil 2.2).

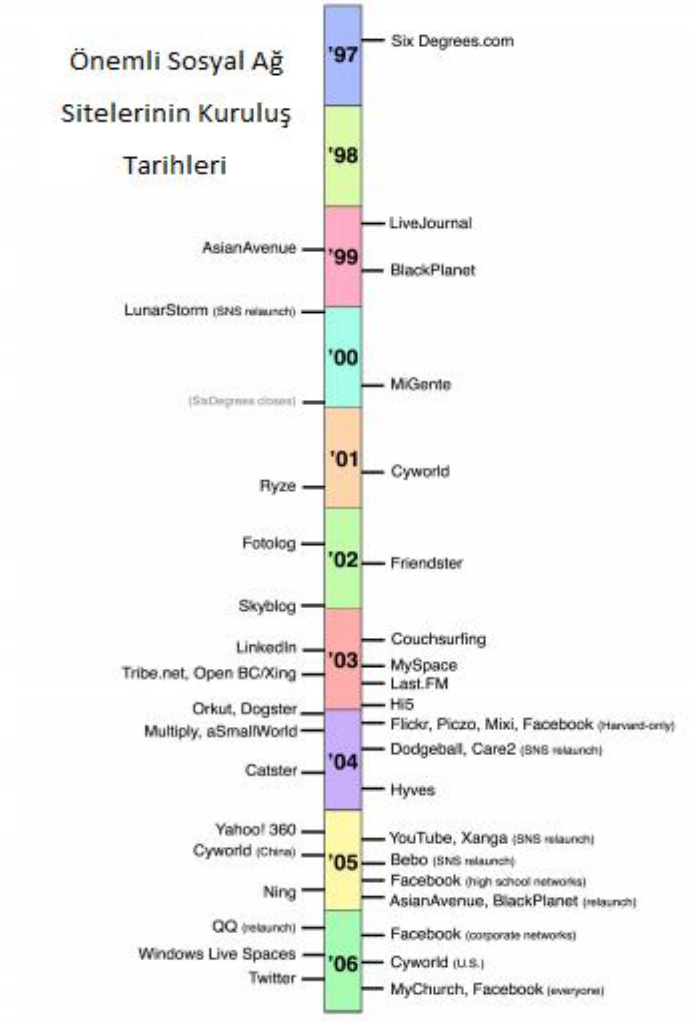
2.5.2. Teknolojinin Sosyalleşmesi

2000'li yılların başlarında artık teknoloji denince akla gelen internet de teknolojik gelişmelerden nasibini almaya başlayarak, iletişim için IRC (Internet Relay Chat)'den ötesine geçerek, daha fazla seçeneğin sunulduğu, insanlara anlık rastgele sohbetlerden belirli bir kimlik vererek ekledikleri insanlarla iletişim imkânı sunan MSN ortaya çıkmıştır. Burada fotoğraflar bile paylaşılabiliyorken, hatta web cam sahibi olanlar görüntülü sohbetler bile gerçekleştirebilmekteydi.

> "Sosyal medya iletişimin teknolojik araçlar üzerinden sosyalleşmesini de barındıran bir terim olarak ifade edilebilir. Bu açıdan bakıldığında karşınıza çıkan ilk uygulama IRC dir. İnternet üzerinden canlı sohbet olarak dilimize çevirebileceğimiz uygulamayla birden fazla kanal kurulabiliyor ve bu kanallara dâhil olanlar birbiriyle yazışabiliyordu. Sohbet amaçlı kurulan bu sunucularda yer almak için öncelikle bir odaya kaydolmanız gerekiyordu. Genellikle her şeyin bir odası bulunuyor ve aynı şehirde yaşamların bir araya gelmesini sağlıyordu akşamları başlıyor sohbetlerin bazen sabahlara kadar sürdüğü bu odalarda sohbet edenlerin birtakım sağlık problemleri çekmeye başladıklarını gazete haberlerinden öğrenir olduk. Hatta bu dönemin mizah anlayışı ise internetten yazışarak işleri hiç görmediği kişilerle buluşmak için Ankara Kızılay'daki Güvenpark, İstanbul Taksim deki Atatürk Heykeli veya İzmir Konak'taki Saat Kulesi önünde özellikle hafta sonları ellerinde çiçekle bekleyen ve daha sonra bir arkadaşı tarafından

işletildiğini onların gülüşmelerinden anlayan gençlerle sembolleşti." (Özutku vd. 2014: 52).

Bununla yakın döneme denk gelen ADSL (Asymmetric Digital Subscriber Line)'in kullanımına geçilmesi sayesinde telefon hattını ve iletişimini işgal etmeye ihtiyaç olmaksızın evlerden internete bağlanmak mümkün oluyordu. Hem bununla birlikte internetin fiyatı düşerken, diğer yandan bilgisayarların fiyatlarının düşmesi artık evlere internetin girmesine imkan sağlamış ve Web 2.0'ın önünü açmıştır.



Şekil 2.2. Önemli Sosyal Medya Araçlarının Kuruluş Tarihleri[9]

[9]http://www.danah.org/papers/JCMCIntro.pdf (Erişim tarihi: 06.09.2014)

Web 1.0'ın tek taraflı üretilen stabil içeriğine karşı, Web 2.0'da içerik kullanıcılara sunulmakta ve onlar tarafından da geliştirilebilmektedir. Bu yıllarda ortaya çıkan Vikipedi bunun en güzel örneğidir. Kullanıcıların (vikipedistler) oluşturduğu içeriklerle, herkesin ulaşabildiği, şu an 100'den fazla dilde içerik sunan bir 'özgür ansiklopedi'dir. Günümüzde herkes tarafından kullanılan bilgi kaynağı olup, güvenilirliği ise oldukça yüksek düzeydedir.

2003 yılında ortaya çıkan Vikipedi, her ne kadar web 2.0'ın en güzel örneklerinden dense de, asıl kırılma 2006 yılında Facebook'un tüm dünyaya açılmasıyla gerçekleşmiştir (bkz. Şekil 2.2). Facebook, eski arkadaşlarını bulmak ve onlar tarafından bulunmak için kullanılmaya başlanıldığından, oluşturulan profiller genellikle kendini en iyi şekilde anlatarak kolay bulunabilmek için dürüstçe oluşturulmaktaydı. Bu sebeple bundan önceki sanal sohbet deneyimlerinden farklı olarak insanlar burada kendi kişiliklerini katmaya başladılar. Bu platformda insanlar çoğunlukla mutlu günlerine ait fotoğraflarını paylaşırlar, doğun günlerini kutlar hatta Facebook'ta bulunan farklı konulu sayfalarda kendi kimlikleriyle dünyaya açılırlar. İşte tam bu noktada Facebook bir dönüm noktası oldu ve bu alanda en büyük başarıyı yakaladı.

Kronolojik olarak bundan sonraki en büyük gelişme 3G teknolojisiyle birlikte mobil internetin kullanımıdır. Akıllı telefonlar, mantık olarak cep telefonlarına işletim sistemleri yüklenerek; bilgisayarların işlevsel özelliklerini taşınabilir bu cihazlara aktarılmasıyla oluşturulmaktadır. Daha önce deneyimler olsa da 2007 yılında Apple şirketinin piyasa sürdüğü iPhone ile yaygınlaşan bu cihazlar, şu an hemen herkesin cebinde yer almakta, internete ve özellikle sosyal medya platformlarına bağlanmasına araç olmaktadır. Bu sebeple günümüzde herkesin ulaşabildiği sosyal medyanın fırsatlarını ve risklerini en iyi şekilde analiz etmek gerekir.

2.5.3. Dijitalleşen Türkiye

Türkiye'deki bilişim teknolojileri alışkanlıklarına ilişkin TÜİK tarafından yapılan hane halkı araştırması yapılmıştır. 16 - 74 yaş aralığındaki bireylere yapılan 2015 yılındaki bu araştırmanın sonuçları ise şu şekildedir.[10]

Bilgisayar kullanımı %54,8'dir. Erkeklerin %64'ü bilgisayar kullanırken, kadınlar için bu sayı %45,6'dır. İnternet kullanımı ise ortalama %55,9 iken, erkeklerin %65,8'i internet kullanmaktadır. Kadınların oranı ise %46,1'dir. 2014 yılındaki bilgisayar kullanımı oranı %53,5 iken, internet kullanım oranı ise %53,8 olarak ölçülmüştür.

Türkiye genelindeki internet erişimi olan hanelerin oranı %69,5'dır. Evinde internet erişimi olmayan %30,5'lik kısmın gerekçeleri ise şu şekildedir: %59,5'lik kısmı evde internete ihtiyaç duymadıklarını belirtmiştir. İnternet kullanımını yeterince bilmediklerini belirtenler ise %44,7'lik bir oran oluşturmaktadırlar. İnternet erişimini fiyatı yüzünden tercih etmeyenlerin oranı ise %38,5'tir.

Cep telefonu veya akıllı telefona sahip olan hanelerin oranı ise %96,8 iken sabit telefonlu hanelerin oranı %29,6 oldu. Hanelerin %25,2'sinde masaüstü bilgisayar bulunurken, %43,2'sinde taşınabilir bilgisayar ve %20,9'unda ise internete bağlanabilen televizyon bulunmaktadır.

İnternet kullanım amaçları dikkate alındığında ilk sırayı %80,9 ile sosyal medya yer aldı. %70,2'si haber, gazete ya da dergi okumak için kullanırken, %66,3'ü sağlıkla ilgili bilgi araştırmak için kullanmaktadır. Bunları da sırasıyla %62,1 ile kendi oluşturduğu metin, görüntü, fotoğraf, video, müzik vb. içerikleri herhangi bir web sitesine paylaşmak üzere yükleme, %59,4 ile mal ve hizmetler hakkında bilgi arama takip etmektedir.

İnternetin kullanıldığı yerler ise, en çok %87,1 ile evde kullanılırken, sırasıyla %42,5 ile işyeri, %37,7 ile akraba ve arkadaş evleri, %29,2 ile alışveriş merkezi, havaalanı, vb. kablosuz bağlantı sunulan yerler ve %10,6 ile internet kafe takip etti.

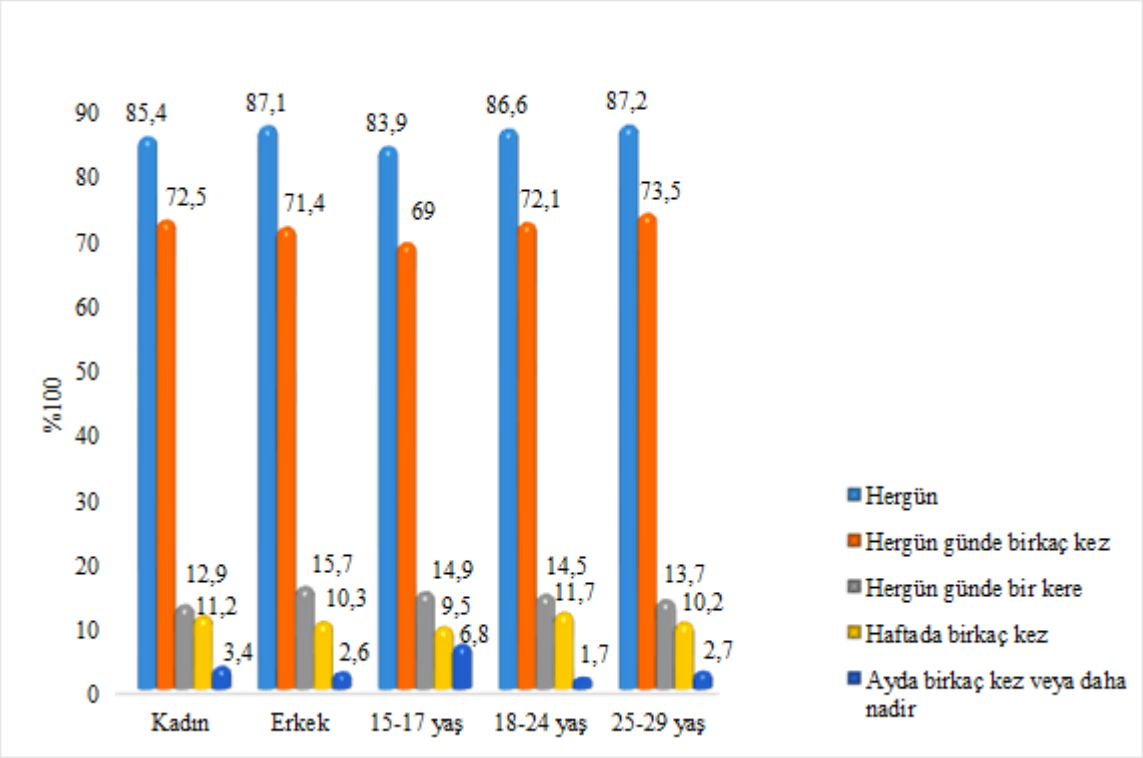
---

[10]Türkiye İstatistik Kurumu - Hanehalkı Bilişim Teknolojileri Kullanım Araştırması (2015) http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660 (Erişim tarihi: 20.11.2015)

Ev ve işyeri dışında internete bağlanmak için cep telefonu veya akıllı telefon kullanım oranı %74,4 iken, %28,9'u taşınabilir bilgisayar kullanılmaktadır.

İnternet üzerinden alışveriş yapanların oranı %33,1 oldu. Bu bireylerin %57,4'ü giyim ve spor malzemesi, %27'si ulaşım, %25,5'i ev eşyası için, %22,4'ü elektronik araçlar için, %18,4'ü ise kitap, dergi, gazete için kullandı.

İnterneti en az haftada bir gün kullanan düzenli kullanıcıların oranı ise %94,2'dir.



Şekil 2.3. Türkiye'de Cinsiyet ve Yaşa Göre Sosyal Medya Kullanım Yüzde Sıklığı (2013)[11]

Bireylerin özgürce kendilerini tanımlamalarına ve ifade edebilmelerine olanak tanıyan sosyal paylaşım ağları kullanıcılar tarafından birçok amaçla kullanılmaktadır. Kullanım

[11]Türkiye Cumhuriyeti Gençlik ve Spor Bakanlığı - Gençlik ve Sosyal Medya Araştırması (2013) http://pro.webrazzi.com (Erişim tarihi: 14.04.2015)

amaçları kişiden kişiye değişim gösterebilirken, toplumsal düzeyde de farklı amaçlarla kullanılabilmektedir. İnternet üzerindeki sosyal medya, tüm dünyada olduğu gibi Türkiye'de de son yıllarda giderek popüler hale gelmiştir.

Sosyal medya siteleri, çeşitli uygulamalarıyla hızlı bir şekilde gelişmekte; diğer pek çok site arasında popülerliği gün geçtikçe artmaktadır. Ülkemizde de sosyal medya, sunduğu olanaklardan dolayı bireysel ve sosyal hayatın ayrılmaz bir parçası haline gelmiş, insanların yaşam tercihlerini değiştirmiştir.

Toplumumuzda özellikle çocuklar ve gençler, sosyal medya uygulamalarına oldukça ilgi göstermekte; oyun oynama, iletişim kurma ve bilgi edinme gibi amaçlarla bu sitelere yönelmektedir.

Şekil 2.3'te Türkiye'de cinsiyet ve yaşa göre sosyal medya kullanım yüzde sıklığı görülmektedir. Sosyal medya kullanımında cinsiyete göre oranlar benzer olmakla beraber erkekler daha fazla sosyal medya kullandığı görülmektedir. 25 - 29 yaşları arasında sosyal medya kullanımı en yüksek seviyede olduğu görülmüştür.

Genel olarak bakıldığında kullanıcıların cinsiyet ve yaş fark etmeksizin her gün en az %80'nin sosyal medya hesaplarını ziyaret etmektedir. Bu durum kullanım amaçlarına göre değişiklik göstermektedir. Son dönemde ülkemizde alışkanlık haline gelmiş bu davranışın, sadece davranış boyutunda kalmayıp bağımlılığa dönüştüğü ortaya koymaktadır.

Toplumumuzda işini, gücünü ailesini ve hatta yemek yemesini bile ihmal edecek düzeyde sosyal medya kullanan insanlar sayısı bir hayli yüksektir. Ancak bu bağımlılık halen dünya genelinde tıbbi açıdan bir hastalık olarak değerlendirilmemektedir. İnsanların yanlarından ayıramadıkları cep telefonu, tablet cihazları bu bağımlılığa en güzel örnektir.

Sosyal medyanın getirdiği yeniliklerin yanında kötü niyetli kişilerinde ilgisini çekmektedir. Sosyal medya, kullanıcılar hakkında en mahrem olan bilgiler pazarlanmakta, elde edilen bilgiler sayesinde art niyetli kişilerin toplumun her kesiminden insanlara zarar verme olasılığını artırmaktadır. Bu durum özellikle toplumun en önemli ve en hassas yapı taşları olan çocuklar için büyük risk teşkil

etmektedir. Sosyal medya hesapları üzerinden oluşturulan sahte profillerle çocuklarla iletişime geçilerek cinsel istismar fiilini gerçekleştirmeye hazırlık olarak çocukla internet ortamında cinsel içerikli sohbet edilmesi fiillerinin gerçekleştiği bilinmektedir. Birçok ülkede bu suçla etkin mücadele kapsamında yasal düzenlemeler mevcuttur (Kara, 2014: 2). Ülkemizde de bu konu hakkında yasal düzenleme çalışmaları devam etmekle birlikte toplumsal farkındalık yaratılması büyük önem arz etmektedir.

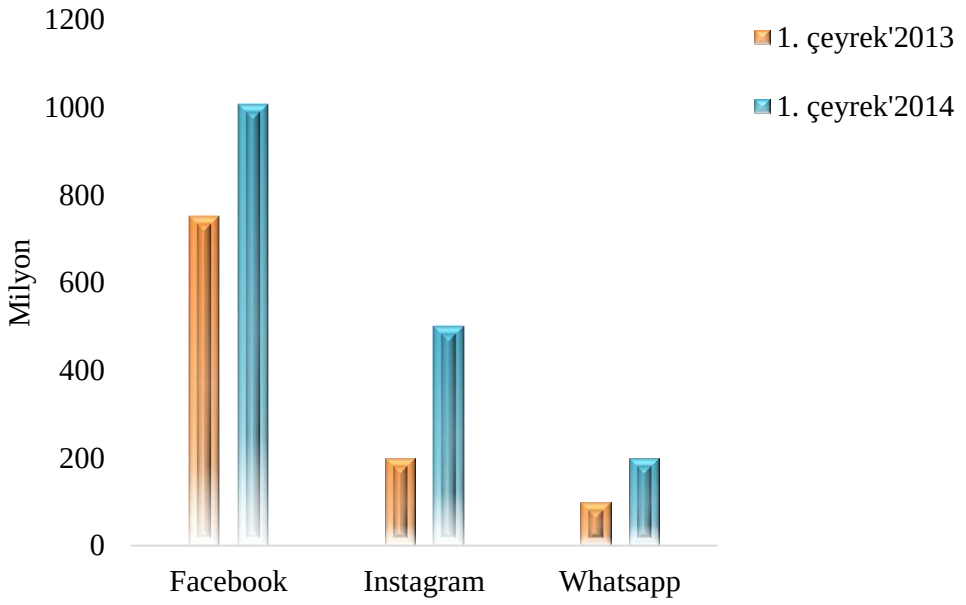
Günümüzde, birçok sosyal ağ sitesi ortaya çıkmış ve insanların iletişimini, etkileşimini, işbirliğini, çalışmasını yeniden şekillendirmiştir (Murray, 2008: 1). Milyonlarca kullanıcı gerçek kimlikleri ile sosyal ağlar üzerinde çevrimiçi olarak yer almaktadır. Dünya çapında bu denli yaygınlaşan sosyal ağlar, ülkemizde de yoğun bir şekilde kullanılmaya devam etmektedir. Bu yüksek ilgi, sosyal ağların birçok özelliği ve imkânları barındırmasından kaynaklanmaktadır.

Ülkemizde Facebook kullanıcılarının %37,5 kadın iken %62,5 erkektir.[12] Ülkemizde sosyal paylaşım ağları ile daha hızlı ve daha az maliyetle birbirleriyle iletişim kurabilen birey ya da topluluklar, ihtiyaç durumunda söz konusu ağları son derece etkin kullanmaktadır.

Türkiye'de kullanılan sosyal paylaşım ağlarının en yaygını Facebook, Instagram ve Whatsapp'tır. Şekil 2.4 ve 2.5'te Türkiye'de 1. çeyrek 2013 ve 1. çeyrek 2014 Facebook, Instagram ve Whatsapp'ın 2013-2014'te sahip olduğu aylık aktif mobil kullanıcı sayısı kullanıcılarının yaş dağılımı verilmiştir.

İncelenen üç sosyal paylaşım sitesi içinde aktif kullanıcı sayısı hızlı bir şekilde artış göstermektedir. Kullanıcı profilleri incelendiğine bu üç sosyal medya paylaşım sitesini en çok kullanan %33,7 oranıyla 18 - 24 yaş aralığındaki kişilerdir. 13 - 15 yaş kullanıcıların %15,3 ile ikinci en yüksek orana sahip olması dikkat çekicidir. Bu durum; ülkemizde özellikle çocuk cinsel istismar suçunun oluşmasına zemin sağlayabilmektedir.

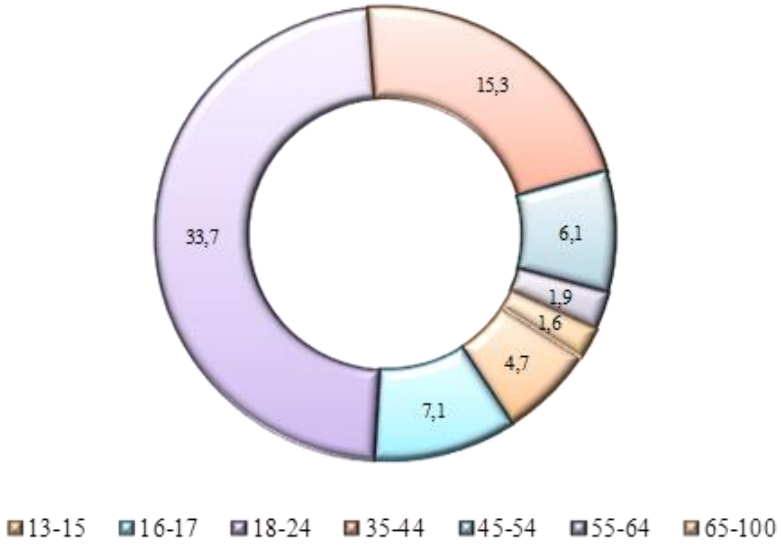
[12]Socialbakers (2015) http://pro.webrazzi.com (Erişim tarihi: 04.03.2015)



Şekil 2.4. Facebook, Instagram ve Whatsapp'ın 2013-2014'te Sahip Olduğu Aylık Aktif Mobil Kullanıcı Sayısı Kullanıcı Sayısı[13]

Sosyal paylaşım siteleri günden güne artan bir yoğunlukta kullanıcı sayısını artırmaktadır. Facebook; dünya çapında en çok tanınan sosyal paylaşım sitesi olması ülkemizde de yüksek bir ilgi görmekte Türkiye, Facebook'u kullanan ülkelerin başında gelmektedir. Facebook üzerinden sosyal medya kullanıcılar toplumsal kimliklerini kurmaktadır. Kullanıcılar bu ilgisinin basit bir ara yüzünün olması özellikle fotoğraf ve video paylaşımın sınırsız olmasından kaynaklanmaktadır. Facebook ülkemizde özellikle gençler (18 - 24 yaş arası) yoğun bir şekilde kullanmaktadır.

[13]Türkiye Cumhuriyeti Gençlik ve Spor Bakanlığı - Gençlik ve Sosyal Medya Araştırması (2013) http://pro.webrazzi.com (Erişim tarihi: 04.03.2015)



Şekil 2.5. Türkiye'de Bulunan Facebook Kullanıcılarının Yaş Dağılımı (2015)[14]

Dünya çapında 1,5 milyarın[15] üzerinde aylık aktif kullanıcı sayısına ulaşan Facebook'un bazı istatistiksel verileri şunlardır:[16]

-Facebook kullanıcıların %50'si her gün siteye giriş yapmaktadır.

-Kullanıcıların ortalama arkadaş sayısı 130'dur.

-Facebook kullanıcılarının tamamı sitede ayda 500 milyar dakika zaman harcamaktadır.

-Facebook'ta insanların etkileşime geçtiği 160 milyon konu (sayfa, grup ve olgu) vardır.

-Ortalama her bir kullanıcı 60 sayfa, grup ve olgu ile bağlantılıdır.

---

[14]Facebook, Instagram, Whatsapp, http://pro.webrazzi.com (Erişim tarihi: 04.03.2015)

[15]http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Erişim tarihi: 22.11.2015)

[16]http://www.facebook.com/press/info.php?statistics (Erişim tarihi: 12.06.2013)

-Ayda 25 milyar paylaşım yapılmaktadır.

-Kullanıcıların yüzde 70'i ABD dışındandır.

-250 binden fazla internet sitesi Facebook ile entegre durumdadır.

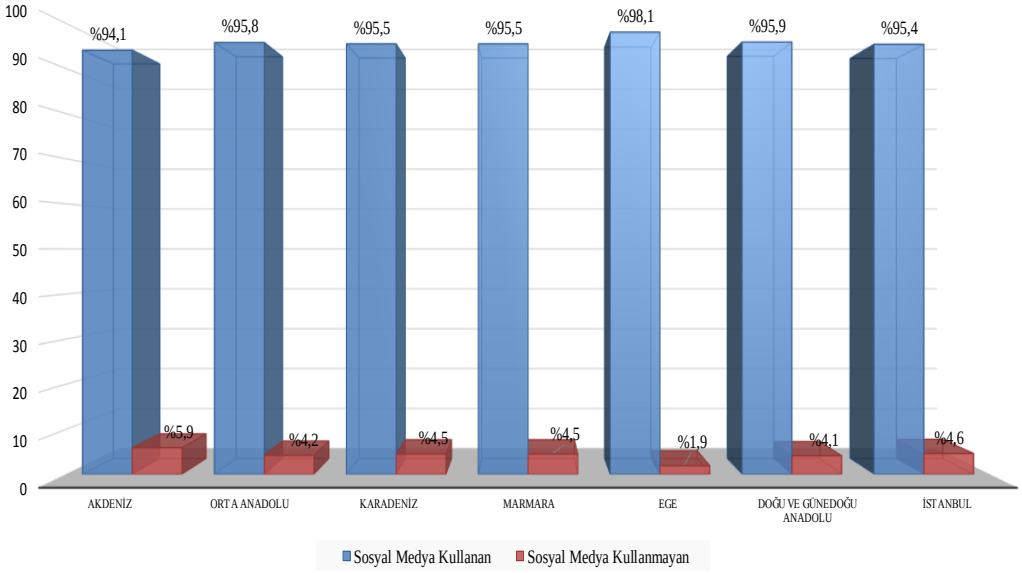
-100 milyondan fazla kişi mobil bağlantı kurmaktadır. Mobil bağlantı kuranlar

-Facebook'u kurmayanlara oranla 2 kat daha aktif kullanmaktadır.

-Facebook'un bin 400'ün üzerinde çalışanı vardır.

Facebook'a yoğun ilginin sebebi basit ara yüzü olması ve bu basitliğine rağmen hem de çok komple bir yapıda olarak birçok servisi barındırmasıdır. Başlıca amaçları: arkadaş bulma, paylaşımda bulunma, oyun oynama, siyasal ve ideolojik içeriklere erişme, ticaret, örgütlenme vb.dir. Hatta ilk yıldızının parladığı alan, kullanıcıların bağlarını kopardığı arkadaşlarıyla tekrar bağ kurabilmesini sağlamasıdır. Onlarla iletişimlerini ve ilişkilerini tazeleyebilmekte ve sürekli olarak iki yönlü veya tek yönlü olarak sürdürebilmektedirler.

Kullanıcılar öncelikle arkadaşlarını "gözetlemektedir". Facebook'un en sık kullanılan işlevleri arasında birinci sırada "arkadaşlarının fotoğraflarına bakmak" gelmektedir (Şener, 2009). Facebook gibi sosyal paylaşım sitelerinin boş zaman etkinliği olarak ön plana çıktığını göstermektedir (Toprak, 2009: 28).



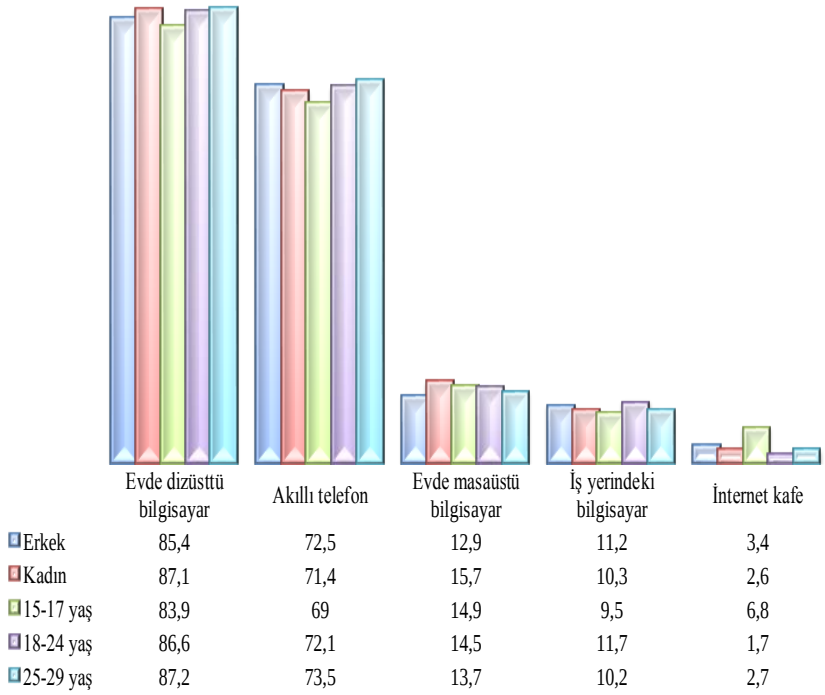
Şekil 2.6. Türkiye'de Bölgelere Göre Sosyal Medya Kullanımı (2013)[17]

Şekil 2.6'da Türkiye'de bölgelere göre sosyal medya kullanımı görülmektedir. Genel olarak bölgeler arasında benzerlik gösterirken en çok sosyal medya kullanımı %98,1 oranla Ege bölgesinde görülmektedir. En az sosyal medya kullanım oranı ise %94,1'lik bir değerle Akdeniz Bölgesi'nde görülmüştür.

Ülkemizde görülen cemaatten cemiyete geçiş süreci ve sonrasındaki toplumun her kesiminde sosyal medya bağımlılığı görülmektedir. Bu durum sosyal medya günümüzde birçok etkinliğe ev sahipliği yapması, yaşanan toplumsal olayların birçoğunda etkin rol üstlenmesinden kaynaklanabilir. Sosyal medyanın birey ve toplum hayatına olan katma değerinin yanı sıra, toplumsal hayattan neleri eksilttiğini sorunsallaştırmak sosyal bilimcilerin son zamanlarda en çok tartıştığı konulardandır.

Söz gelimi "kullanıcıların büyük çoğunluğunu gençlerin oluşturduğu adları sosyal ağ olsa da bu tarz siteler zaman içerisinde yoğun ve bilinçsiz bir kullanım ile bireyleri gerçek sosyal yaşamdan uzaklaştırabilir" (Aydoğan, 2010: 4).

[17]Türkiye İstatistik Kurumu http://pro.webrazzi.com (Erişim tarihi: 03.03.2015)



	Evde dizüsttü bilgisayar	Akıllı telefon	Evde masaüstü bilgisayar	İş yerindeki bilgisayar	İnternet kafe
Erkek	85,4	72,5	12,9	11,2	3,4
Kadın	87,1	71,4	15,7	10,3	2,6
15-17 yaş	83,9	69	14,9	9,5	6,8
18-24 yaş	86,6	72,1	14,5	11,7	1,7
25-29 yaş	87,2	73,5	13,7	10,2	2,7

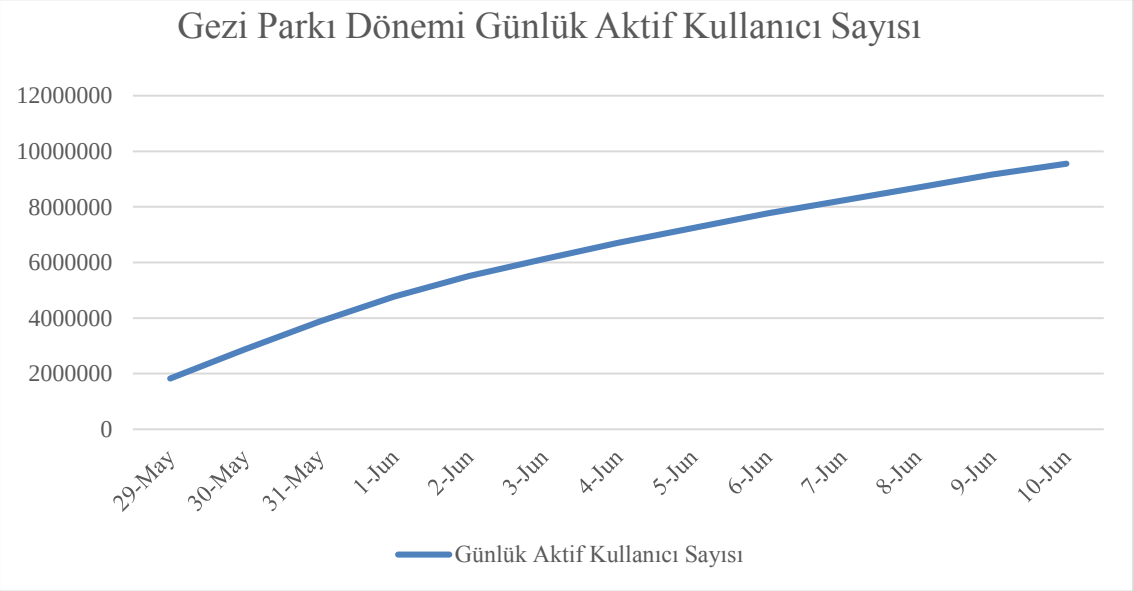
Şekil 2.7. Türkiye'deki Genç Nüfusun Cinsiyet ve Yaşa Göre Sosyal Medya Bağımlılık Biçimi[18]

> "Kullanıcılar toplumsal paylaşım ağlarında sanal bir yaşam kurabilmektedirler. Bu kapsamda kullanıcıların toplumsal paylaşım ağlarında yer alan profil özelliklerinin çoğu istedikleri ama ulaşamadıkları yaşam biçimlerini karakterize edebilir. O kişi ile arkadaşlık kurmak isteyen kimseler, bu durumda kişinin gerçeği yansıtmayan özellikleri doğrultusunda ilişkiye geçerler ve kendilerinden izledikleri karakterin sahip olduğu özelliklere gerçekten de sahip olduğuna, kurulan ilişkinin yol açacağı ya da ima edilen sonuçlara gerçekten yol açacağına ve genelde her şeyin göründüğü gibi olduğuna inanmaları istenir." (Binark, 2009: 25).

[18]Türkiye İstatistik Kurumu http://pro.webrazzi.com (Erişim tarihi: 03.03.2015)

2.5.4. Gezi parkı deneyimi üzerine kısa bir değerlendirme

Sosyal medyanın ülkemizde ön plana çıkması açısından zirve yaptığı olaylar Mayıs 2013 yılındaki Gezi Parkı olaylarıdır. Gezi Parkı olaylarında sosyal medyanın yoğun bir şekilde kullanılması ülkemiz için sosyal medya kullanımı açısından ciddi bir dönüm noktası olarak tezahür etmiştir. Gezi Parkı olayları öncesinde 2009 İran Yeşil Devrimi, 2011 Arap Baharı, 2011 Occupy Wall Street gibi dünyanın diğer bölgelerinde sosyal medyanın yoğun kullanımına sahne olan örnekler olmuştur. Sosyal medya devriminin, diğer medya devrimlerinden en önemli farkı diğerlerinin teknolojik ve bilimsel gelişmeler doğrultusunda kapitalist tahakküm altında gerçekleşmesiyken, sosyal medya için ise durum mantık açısından tam tersi niteliktedir. Çoban'ın da dediği gibi (2014: 9) sosyal medya devrimi, kendisini sokaklarda üzerinden gösteren bir devrimdir, her ne kadar gelişmesi sistem içi olsa da, kullanımındaki devrimci dönüşüm sistem karşıtı olarak gerçekleşmiştir.



Şekil 2.8. Twitter'da Günlük Aktif Kullanıcı Sayısı (2013)

Türkiye'de gezi parkı olaylarında en fazla ön plana çıkan platform kuşkusuz Twitter olmuştur. Türk halkı büyük ölçüde Twitter'la resmen 2013 Haziran'ından itibaren tanışmıştır diyebiliriz. Türkiye'deki gezi parkı olayları sırasındaki Twitter kullanıcı

sayısı Şekil 2.8'de gösterilmiştir (Özutku vd. 2014: 159). 29 Mayıs günü 1.819.403 olan günlük kullanıcı sayısı 10 Haziran günü 5 kattan daha fazla artış göstererek 9.548.503'e yükselmiştir.

Her ne kadar Gezi Parkı olaylarında çok farklı bir yer edinmiş olsa da sosyal medyaya ilişkin bir diğer husus ise, sosyal medyanın geleneksel medya gündemini belirleyip belirlemediğidir. Çetin ve Bel'in (2014: 60) yaptığı çalışmada, Türkiye'deki en fazla izlenen üç televizyon kanalı ve en yüksek tirajlı üç gazete incelenerek sosyal medya araçları üzerinden içerik kıyaslaması yapılmıştır.

2013 yılında gerçekleştirilen bu çalışmanın sonucunda, sosyal medyanın gündemi belirleyen platformdan ziyade gündemin konuşulduğu bir platform olduğu görülmüştür. Burada oluşan içeriklerin gazetelerin ilk sayfalarında veya ana haber bültenlerinde nadiren yer aldığı, genellikle yer alınma sebebinin de ciddi mesele oluşlarından ziyade habere eğlence veya görsel unsur katmak için kullanıldığı görülmüştür (Çetin ve Bel, 2014: 70).

Gündem oluşturma konusunda, sanıldığı kadar etkili olmadığı bu çalışma sonucunda ortaya konmuş olsa da, sosyal medyanın günümüzde örgütlenme ve kitlelere ulaşma aşamasında çok önemli bir araç olduğu yadırganamaz bir gerçektir. Kaldı ki, Gezi Parkı sürecindeki sosyal medyanın etkisinin ve gücünün istisnai oranda yüksek olduğu açıktır.

Gezi Parkı olaylarının en uzun süre yaşandığı illerden biri olan Eskişehir'de birçok örgütlenme çağrısı yapılmış, bu toplanmaların sonucunda polisle grup çokça kez karşı karşıya gelmiş çatışmanın olduğu veya olmadığı durumlarda kimi zaman yerel basında kimi zaman da ulusal basında yer bulmuştur.

Bu kadar hayatımıza girmiş olan teknoloji ve sosyal medyanın aslında nasıl bir evrim geçirdiğini kısaca anlamış bulunmaktayız. Castells'in (2013: 484) "insanlar, teknolojiyi kendi gereksinimlerini karşılayacak biçimde şekillendirmiştir." sözü hem hayatımızda neden bu kadar büyük role sahip olduğunu en net biçimde ifade etmektedir.

3. Bilişim Suçlarının Kriminolojik ve Sosyolojik Yönü

3.1. Kriminoloji ve Bilişim Suçu

Kriminoloji için kısaca suç bilimi diyebiliriz. Daha geniş olarak ele alırsak suça etki eden biyolojik, psikolojik, sosyolojik, ekolojik ve diğer faktörleri ve sebepleri araştırarak suçun oluşumuna ilişkin tahminlerde bulunan ve önlenmesine ilişkin çözüm önerileri sunan bir bilim dalıdır (Dolu, 2010: 31). Bu özelliklerine ilaveten kriminoloji, suçun sebeplerini bilimsel bir perspektiften araştırırken aynı zamanda suçun önlenmesine yönelik stratejiler ve politika önerileri ortaya koyan bir bilim dalıdır (Adler vd. 2004: 2'den aktaran Dolu, 2010: 31).

Uzun yıllar boyunca suçun düşük sosyoekonomik sınıftaki kişiler tarafından işlendiğine inanılırdı. Bunun anlamı suçlu genellikle eğitimsiz, sosyal ve ekonomik düzeyi düşük kişilerden oluşmasıydı; ancak bu düşünce 1950'li yıllarda Edwin Sutherland tarafından literatüre kazandırılan 'beyaz yakalılar' olarak ekonomide sınıflandırılan idarecilerin de suç kategorisine dâhil edilmesi ile radikal bir şekilde etkilenmiştir (Polat, 2004: 31).

Bilişim suçları için yukarıda sayılan suça etki eden faktörler olan biyolojik, psikolojik, sosyolojik, ekolojik faktörlere teknolojik faktörleri de eklemek gerekir. Çünkü bilişim suçlarının işlenmesi, çeşitlenmesi, yayılması hep teknolojik gelişmelerin neticesinde meydana gelmektedir.

İnsanların bu teknolojik gelişmelerin kilit noktalarından biri sayabileceğimiz bilgisayar ile tanışması yaklaşık 60 yıl önce başlamıştır. İlk bilişim suçları ise bu cihazların, bu sistemlerin manipüle edilebilmesinin kolaylığının fark edildiği 1960'lı yıllarda ortaya çıkmıştır (Karagülmez, 2005: 43). Ancak kırılma noktası kişisel bilgisayarların piyasaya sürülmesiyle olmuştur. Artık sıradan bir birey de, bu bilişim ağına internet veya diğer yollarla katılmış ve bu sonu gelmeyecek potansiyel suç denizinde yer almaya başlamıştır.

Ancak bilişim suçları, kriminolojinin ilgilendiği meseleler arasında çok daha gerilerde kalmaktadır. Bunun bir nedeni günümüzde bile bilişim suçunun tanımı konusunda mutabık olunamamasıdır. Bir diğer neden ise kriminolojinin ilk ortaya çıktığından beri geleneksel veya klasik suç dediğimiz, somut, toplumda sıkça görülen ve her bireyin

potansiyel mağduru olabileceği suçlarla ilgilenmesidir. Bunlar hırsızlık, yağma, cinsel saldırı, kasten adam öldürme ve yaralama gibi toplum tarafından daha ciddiye alınan suçlar olup, yasal düzenlemeler de bunlarla mücadele üzerine kurulmuştur (Karagülmez, 2005: 43 - 44).

Bilişim suçlarının kriminolojik yönden ele alınması ilk olarak bilişimin ve teknolojinin anavatanı pozisyonundaki ABD'de olmuştur. Bunun sebebi ise açıklanamayan bazı olaylar neticesinde büyük zararların meydana gelmesidir. 1971 yılındaki New York-Pennsylvania arasındaki seferlerin, demiryolu şirketi bilgisayarlarına dışarıdan yapılan yetkisiz erişimlerle rotasından sapması ve her seferinde büyük maddi zararlara yol açması olayından sonra ilk önce adli makamların daha sonra da kriminologların ilgisini çekmeyi başarmıştır (Karagülmez, 2005: 43).

3.2. Bilişim Suçlarının Sosyolojik Teorilerle Analizi

Bu bölümde suça sebep olan sosyolojik teoriler ele alınmış ve bunların bilişim suçlarıyla ilişkilendirilmesi hedeflenmiştir.

3.2.1. Ayırıcı birliktelikler teorisi

Ayırıcı birliktelikler kuramı kriminoloji ve sosyoloji alanlarındaki en bilinen kuramlardan biridir. Bu teorinin yaratıcısı olan Edwin Sutherland bu alana önemli katkılarından dolayı birçok çevrelerce 'Amerikan kriminolojisinin babası' olarak görülmektedir. Ayırıcı birliktelikler Kuramının arkasındaki temel fikir kriminal davranışın öğrenilebilir olduğu ve diğer sapkın kişilerle etkileşim içinde öğrenildiğidir (Imhof vd., 2010: 65, Sokullu-Akıncı, 2011: 196).

Sutherland insanların suçlu olmayı öğrenebildiğini savunmaktadır (aktaran Dolu, 2010: 232). Bu durum, yakın olduğu insanlarla birlikteyken suça yöneltici, teşvik edici, rasyonelleştirici etkilere daha çok maruz kalması sonucu meydana gelmektedir. Buna göre suç yasadışı aktivitelere katılan diğer insanlar ile etkileşim aracılığıyla gerçekleşir. Bu teori önemlidir çünkü bu teori, birçok biyolojik faktörün bireyi suç işlemeye daha

açık yapmaya katkısının olduğunu ileri süren o günkü kriminolojik teorilerden ayrılmaktadır.

Bu şu anlama gelmektedir: kriminal etkilere yasal etkilerden daha fazla maruz kaldıkları için bir bireyin suçlu olması muhtemeldir. Bu, yasaya ve otoriteye yönelik negatif görüşleri güçlendirebilecek düşük sosyoekonomik şartların bulunduğu çevrelerde görülebilmektedir.

Edwin Sutherland'a göre onun ayırıcı birliktelikler teorisini oluşturan 9 faktör bulunmaktadır (aktaran Imhof, 2010: 67, Dolu, 2010: 233, Sokullu-Akıncı, 2011: 196). İlki, daha önce de bahsedildiği gibi, bu teorinin temeli niteliğindeki kriminal davranışın öğrenildiğidir.

İkinci faktörün birinci ile sıkı bir bağı vardır ve kriminal davranışın iletişim süreci sırasında diğer birey aracılığıyla öğrenildiğini ortaya koymaktadır.

Ayırıcı Birliktelikler Teorisinin üçüncü faktörü bireylerin kriminal davranışı yakın bulunulan grupların parçası olunduğunda öğrenildiğidir. Bu grup, aile ya da yakın arkadaşlar gibi, bireyler üzerinde önemli etkisi olan herhangi bir grup olabilir.

Dördüncü faktörü birkaç parçalıdır. İlk parçası; kriminal davranışın öğrenildiğinde, bireyin ayrıca suçu nasıl işleyeceğine yönelik teknikleri de öğrenmesidir. İkinci parçası ise, suça ilişkin motivasyon, dürtü, rasyonalizasyon ve tutumun öğrenilmesidir. Yani kişinin suçu nasıl meşrulaştıracağını öğrenmesidir.

Beşinci faktör bir bireyin sapkın davranışa, yasal kodları olumlu ya da olumsuz görmesine bağlı olarak sürüklendiğini belirtmektedir. Bu bireyin yasaları sert ve adaletsiz görmesi durumunda onun sapkın davranışa sürükleneceğini belirtmektedir.

Altınca faktör de bu teorinin temel parçalarından biridir. Bir kişi yasayı çiğnemek için yasayı korumaktan daha fazla sebep görürse kriminal olmaktadır. Birey yasaya bakar ve yasaya uymayla yasayı bozmanın ödüllerini karşılaştırır ve hangisinin daha fazla yarar sağlayacağına göre karar verir.

Yedinci faktör, Ayırıcı Birlikteliklerin, sıklık, süre, öncelik ve yoğunluk bakımından değişkenlik gösterebileceğini belirtmektedir. Bu faktör; bireylerin, kriminal davranış

içindeki bireyler ile ne kadar sıkı bir bağa sahip olduğuna bağlanabilir. Eğer günlük olarak etkileşim içerisindeyseler ve güçlü duygusal bağlara sahiplerse normal zamanda olduğundan daha fazla sapkın davranış gösterme ihtimalleri vardır.

Sekizinci faktör ise kısaca kriminal davranışlar diğer öğrenme mekanizmaları gibidir yani birey yasal davranışları nasıl öğreniyorlarsa bunları da aynı şekilde öğrenir.

Son faktöre göre; kriminal davranış genel ihtiyaç ve değerlerin bir yansımasıyken bu sapkın davranışa neden olan ihtiyaç ve değerlerin zorunlu olarak tatmin edilmesi gerekmemektedir. Çünkü kriminal olmayan davranışlar da aynı ihtiyaç ve değerlerin bir ifadesidir. Bunun bir örneği kabul edilmeye ve sevilmeye duyulan ihtiyaçtır.

Özetle bu dokuz faktör, suç modelini bireyin iki unsur üzerinden öğrenmesini ortaya koymaktadır. Suç işleme teknikleri ve suç işlenmesini meşrulaştıracak sebepleri yakın ilişkide bulunduğu kişiler tarafından öğrenilmesidir.

Ayırıcı birliktelikler teorisi bilişim suçlarına uygulanabilir. Bu teorinin temel dayanağı, kriminal davranışın diğerleriyle sosyal etkileşim aracılığıyla öğrenilmesidir. Geleneksel bir hackerın profili, daha yalnız ve çok zeki bir kişilik göstermektedir. Onların sosyal etkileşimi, benzer teknolojik ilgileri paylaşan diğer bireylerle elektronik iletişim aracılığıyla gerçekleşir. Hali hazırda bir çok hacker grubu bulunmaktadır.

Teorinin yedinci faktörüne göre; bireyler, yasal olmayan davranışlarda bulunan grup üyeleriyle daha çok zaman harcadıkça bu onların ayrıca sapkın davranışlarda bulunma sıklığını da arttırmaktadır. Şu an dünyada birlikte hareket eden irili ufaklı bir çok hacker grubunun olduğu bilinmektedir.

Genel olarak: birçok hacker ve hackerlık faaliyetleri grup içerisinde oluşmaktadır. Birçok kişi benzer ilgilere sahip kişilerle zaman harcamaktadır. Üçüncü faktör bu gruplarda geçerlidir. Çünkü bu faktöre göre sapkın davranış yakın grupların bir parçasıdır. Bu gruplar iyi niyetli çalışmalar yapabilirler: beyaz şapkalı hackerlık gibi; ancak bir grup içinde olmak iyi niyetli bireylerin diğer kişiler tarafından etkilenmesi sonucunda suç işlemesine neden olabilir. Aynı zamanda bu sayede bireyler yaptıklarını bu araçlarla rasyonel bir düzleme oturtabilirler. Mesela Microsoft ya da Apple'ı hedef almalarındaki sebep, bunların muadilleri olan Linux veya Android gibi açık kaynak kod

olması gerektiğine olan inançlarıdır. (Imhof, 2013: 71) Sapkın davranışın rasyonelleştirmesi de sosyal etkileşimlerle olur. Mesela bazı hacker gruplarının siyasi ve ideolojik gerekçelerle bu fiili gerçekleştirdikleri bilinmekte ve bu sayede de benzer görüşte olan bireyler tarafından sempati ile bakılmaktadırlar.

Sonuç olarak, Ayırıcı Bileşenler bilişim suçlarının neden bu kadar hızlı artış gösterdiğini anlamamıza yardımcı olan birçok faktörü içeren kapsamlı bir teoridir.

3.2.2. Caydırıcılık teorisi

Klasik kriminolojide kökleşen, Klasik Caydırıcılık teorisi, suç işleme kararı veya ondan kaçınmanın maksimum faydalara ve minimum maliyete, yani cezanın ödüle karşı kıyaslanmasına dayandığını varsayar. Bu çok eski bir teoridir ve Cesare Beccaria ve Jeremy Bentham'ın 18. yüzyıldaki suç ilkeleri üzerine yayınlarına dayanır. Maliyet yani bedel ödeme, resmi cezalar veya kanuni yaptırımlar olarak tanımlanır.

Maliyet faktörü, cezanın seviyesi veya şiddeti yanında, cezanın kesinliği ve çabukluğunu içerir. Bu teoriye ve genellikle kamu algısına göre, belirli bir suç olabilirliği ve yakınlığı kaldırılarak ve sonucundaki cezanın şiddeti yükseltilerek önlenebilir (Seymour, 2013: 23).

Şekil 3.1'de suçun özelliğine göre caydırıcı etkinin yüksek ya da düşük olması gösterilmektedir. Eğer suç için karar verme rasyonel bir tercih sonucu veriliyorsa, caydırılma oranı yüksektir. Rasyonel değil de duygusal veya sapkın saiklerle işleniyorsa caydırılma oranı daha düşüktür. Bu, bilişim suçları için ele alındığında mala karşı işlenen suçlar olan bilişim sistemleri kullanılarak dolandırıcılık veya hırsızlık suçlarında cezai yaptırımların artırılmasının bu suç tipleri için caydırıcılık arz etmesi beklenir. Ancak diğer bir bilişim suçu tipi olan bilişim sistemleri kullanılarak çocuğun cinsel istismarı suçunda ise suça konu davranışın rasyonel bir süreçten geçmemesinden dolayı yaptırımların ağırlığının caydırıcı etkisi daha düşüktür.

Suçun Özelliği	Caydırılabilirlik Düzeyi
Karar Verme Şekline Göre	
Rasyonel	Yüksek
Rasyonel Değil	Düşük
Suçun Araç ya da Amaç Oluşuna Göre	
Araç	Düşük
Amaç	Yüksek
Suçun Hedefine Göre	
Mala Karşı	Yüksek
Şahsa Karşı	Düşük
Suçun Tanımlanışına Göre	
Mala Prohibita (topluma göre suç değil; ancak kanuna göre suç)	Yüksek
Mala in Se (Topluma göre de suç)	Düşük
Suçun İşlendiği Yere Göre	
Kamusal Alan	Yüksek
Özel Alan	Düşük

Şekil 3.1. Suçun Özelliğine Göre Caydırıcı Etkideki Değişim

Kaynak: Dolu, 2010: 104.

Suçu farklı bir amaca ulaşmak için araç olarak görenler için, suçun salt amaç olduğu fillerin faillerine göre caydırılma oranı daha yüksektir. Bilişim sistemine girme suçu her iki durumda da olabilir. Eğer bilişim sistemine hırsızlık gibi maddi menfaat elde etmek için giriliyorsa caydırılma oranı daha yüksektir; ancak bu suç kişisel tatmin veya popülarite gibi bir motivasyonla işleniyorsa caydırılma oranı daha düşük olmaktadır.

Suçun hedefinin kişi veya mal olmasına göre de caydırıcı faktörlerden etkilenme oranları değişmektedir. Suçun hedefi doğrudan bir kişi olması durumunda yani düşmanlık, kin veya nefret gibi motivasyonların caydırıcılıktan daha az etkilenmeleri beklenmektedir. Mala karşı suçlar ise caydırıcılıktan en çok etkilenen suçlardır. Yukarıdaki örneklerde olduğu gibi mala karşı işlenen suçlar, genellikle rasyonel ve araç suçlardır.

Kanuna göre suç olarak kabul edilen fiillerin toplum nazarında suç olup olmaması suçun caydırıcılıktan etkilenmesinde belirleyicidir. Eğer suç toplum tarafından suç

olarak görülmüyorsa, engellenmesi için caydırıcı etkilere daha çok ihtiyaç duyulmaktadır. Zaten toplumsal olarak meşru görülmeyen fiillere göre caydırılma oranları daha yüksektir. Bilişim suçlarında ise bu caydırıcılık türünün daha farklı bir boyutu ortaya çıkmaktadır. Çünkü toplumda kimi hackleme fiillerine sempatiyle bakılmaktadır. Özellikle milliyetçi veya duygusal saiklerle işlenen bu tip fiiller, kanunlara göre ne kadar suç sayılsa da toplum tarafından hoş karşılanmakta hatta desteklenmektedir. Bu tip durumlarda caydırıcılık etkisinin azalması beklenmektedir.

Kişinin özelliklerine göre caydırılma oranı Şekil 3.2'de gösterilmiştir. Kişi suçtan hayatını idame ettiriyorsa, bu durumlarda caydırıcılık oranı düşmektedir. Bilişim suçları nadiren hayatın sürdürülmesi için araç durumunda olmaktadır. Ancak bilişim suçu işleyerek de çok büyük miktarlarda para kazanmak mümkündür. Bilişim suçu konusunda hayatını sürdürecek kadar maddi menfaat elde edilmesi çok daha fazla uzmanlık gerektirmektedir. Failin uzman olması da aynı şekilde caydırıcılığı olumsuz yönde etkilemektedir.

Kişi için riske atılacak şeylerin miktarı arttıkça suça karşı caydırıcılık faktörlerinin oranı artmaktadır. Riske atılacak şeyler ile kast edilen kişinin topluma adanmışlığıdır. Kişi toplumda daha önemli yer elde ettiyse, sosyoekonomik durumunun ve yaşının artması durumlarında suçun yaptırımlarından daha çekinir hale gelmektedir. Klasik 'kaybedecek bir şeyi olmayandan daha tehlikelisi yoktur' sözü gibi, kişi ne kadar çok kaybedecek şeye sahipse, suçtan cayma oranı da o denli artmaktadır.

Cinsiyet olarak bir ayrıma gidildiğinde erkeklerin, kadınlara göre toplumsal baskılardan ve diğer yaptırımlardan daha az çekindiği görülmektedir. Bu ataerkil bir topluma sahip olan ülkemiz için de oldukça geçerli bir durumdur. Erkekler, doğumundan itibaren kız çocuklarına göre daha güçlü olması, daha hoyrat olması yönünde yetiştirilmektedir.

Suçlunun Özelliği	Caydırılabilirlik Düzeyi
Suçu Hayat Tarzı Olarak Görme	
Düşük	Yüksek
Yüksek	Düşük
Suçtaki Uzmanlık Seviyesi	
Amatör	Yüksek
Profesyonel	Düşük
Riske Attığı Şeylerin Miktarı	
Çok	Yüksek
Az	Düşük
Yaş	
Yaşlı	Yüksek
Genç	Düşük
Cinsiyet	
Kadın	Yüksek
Erkek	Düşük
Sosyoekonomik Durum	
Yüksek Seviye	Yüksek
Düşük Seviye	Düşük
Genel Kişinin Özellikleri	
Gelecek Eksenli	Yüksek
Şimdiye Odaklı	Düşük
Tutarlı	Yüksek
Tutarsız	Düşük
Kötümser	Yüksek
İyimser	Düşük
Risk Alamayan	Yüksek
Risk Alabilen	Düşük
Otoriter	Yüksek
Otoriter Olmayan	Düşük

Şekil 3.2. Şahsın Özelliğine Göre Caydırıcı Etkideki Değişim

Kaynak: Dolu, 2010: 106.

Failin kişisel özelliklerine göre caydırılma oranı değişmektedir. Eğer kişi geleceğinden çok şimdiye düşünen bir yapısı varsa caydırılma oranı düşüktür. Benzer şekilde tutarlı bir yapısı değil de, ne yapacağı belli olmayan bir yapısı varsa da caydırılma oranı düşmektedir. Daha iyimser yapısı olanların, hayatların genelinde kötümser olanlara göre caydırılma oranı düşüktür. Bu durum suçun planlandığı şekilde başarıyla tamamlanıp tamamlanmayacağı konusundaki iyimser veya kötümser bakış açısına göre değişmektedir. Risk almaktan korkan insanların caydırılması daha muhtemeldir. Aynı şekilde baskın karakterli kişilerin, daha otoriter oldukları ve bu sebeple de caydırıcı faktörlerden daha az etkilenmeleri beklenmektedir.

Bilişim suçları için Türk Ceza Kanunu'ndaki maddelerin yaptırımlarının birçok suça göre düşük oluşu bu suç tipi için caydırıcılık faktörünü azaltmaktadır. Ayrıca suçun tespiti, delillendirilmesindeki zorluklar, soruşturma birimlerinin bu konudaki bilgi yetersizliklerine olan inanç da failin suç işleme kararını güçlendirmektedir.

3.2.3. Rutin aktivite teorisi

Rutin Aktivite teorisi, suçludan ziyade suç olgusuna yoğunlaşır. Bu sayede de suçun bileşenleri ortaya konarak suçun nasıl işlendiğini ve nasıl önlenebileceğini ortaya koyar. Suç işlemek için bir suçlunun fırsatlarını vurgular; bu teori, bir suç fırsatı "muhtemel suçlu, uygun hedef ve suça karşı yetenekli bir koruyucunun yokluğu" ile oluştuğunu belirtir. Yani klasik okulun 'suç rasyonel bir tercihtir'in ötesine geçerek, kişinin suç işleme iradesinin ötesinde bazı etkenlerin de suç işlemede etkili olduğunu göstermektedir (Dolu, 2010: 119).

Bunlar model geliştirmede üstün faktörlerdir. Felson, özel bir motivasyonun önemini azaltarak muhtemel suçlu için "herhangi bir kimse, herhangi bir nedenle suç işleyebilir" önermesinin geçerli olabileceğini vurgulamıştır. (aktaran Seymour, 2013: 24).

"Mağdur" yerine "Uygun hedef" kelimelerinin kullanılması, nefret gibi özel motivasyonun önemini daha da azaltır. Felson, suçların caydırıcılığının geleneksel sonuçlarının geleneksel sonuçlarının önemini azaltmak için, üçüncü unsurla ilgili olarak polis "ya da" ceza adaleti " yerine "suça karşı yetenekli bir koruyucu yokluğu" ifadesini

kullanır (aktaran Seymour, 2013: 24). Ancak, kişi bir suç için caydırıcı olarak sonuçları düşünmekten kaçınamaz.

Bilişim suçları için de bu teorinin geçerli olduğunu söyleyebiliriz. Örnek olarak maddi menfaat teminine yönelik gerçekleştirilen banka kartlarının kopyalanması suretiyle yeniden üretilerek banka ve kredi kartlarının kötüye kullanılması suçu genellikle şu şekilde gerçekleştirilmektedir. Suç işleme kastına sahip kişiler tarafından ATM (Automated Teller Machine)'lere yerleştirilen kartların manyetik şeritlerini okuyabilen aparatlar sayesinde, aparatların bulunduğu süreçte, o ATM'yi kullanan kişilerden kartları kopyalanmaya müsait uygun hedeflerin kartları kopyalanır. Son olarak da herhangi bir kolluk görevlisinin olmadığı, hiçbir denetleyenin olmadığı anda da aparatta depolanan veriler, aparat ATM'den sökülmek suretiyle elde edilir.

Eğer kimse o süre zarfında ATM'yi kullanmazsa, ya da kullananlar da kopyalanmaya karşı tedbirli davranırsa uygun hedef olmadığı için suç işlenemez. Ya da kolluk görevlilerin bu aparatı fark etmesi durumunda da suç işlenemez hale gelecektir.

Aynı şekilde hacktivizm maksatlı internet sitelerinin hacklenmesinde de süreç aynıdır. Genellikle siyasi veya ideolojik tepki devletin en üst tabakasına yöneliktir. Ancak hacktivizm maksatlı saldırılar her zaman bu düzeydeki internet sitelerine gerçekleşmemektedir. Çünkü korunma düzeyi yüksek sitelere bu tip bir saldırı yapmak ve başarılı olmak çok güçtür. Bunun yerine daha yerel devlet kurumlarına ait sitesinde açıklar bulunan siteler hacklenmektedir. Çünkü bunlar uygun hedef niteliğindedir.

3.2.4. Rasyonel tercih teorisi

Bu teori, "bir suçlunun her biri kendi maliyetleri ve faydalarıyla sonu belli bir dizi alternatiften birini seçerek memnuniyeti maksimize etmek amacıyla suç işlemede seçim yaptığı" görüşünü sunar. Belli bir suç aktivitesini üstlenme seçimi, 'yasal seçenekler, birey için daha az tatminkâr olduğunda veya suç daha az ceza gerektirdiğinde' meydana gelir (Seymour, 2013: 24).

Clark ve Cornish'e göre suçlar, suç sonrasında elde edilecek getirilere ve suç öncesi ve sonrasındaki götürülerin hesaplanmasının sonucudur. Ancak sadece motivasyonel bir

süreç değil aynı zamanda bir fırsat sorunudur. Birey suça ilişkin önüne gelen fırsatları süzer ve bir tercih yapar (Dolu, 2010: 93).

Ancak, bu teorinin kullanımı karar vermenin kusurlu doğasını tanımak zorundadır. Bu kusurların bazıları şunlardır:

-Suçun oluşmasının önündeki eksik koşullar,

-İnsanlar kendi karar yeteneklerinde ve herhangi bir meseleyle ilgili öngörülebilirlikte eksik ve kusurludurlar.

-Yetersiz bilgilerle de kararlar alınır ve eylemlerde bulunulur.

Profesörler Ray Paternoster ve Sally Simpson 1996 yılındaki bir çalışmasında, 96 işletme yüksek lisans öğrencisi ve yöneticilerle ilgili bir çalışmasında kurumsal suça Rasyonel Seçim Teorisini uyguladı. Yapılan çalışmanın hedefi, kurum suçlusunun, kurumu ilgilendiren bir suçu işlemeye karar vermesinde, cezaların ne kadar rolü olduğunu tespit etmektir (Seymor, 2013: 26).

Bu 96 katılımcı, ne kadar olasılıkla bu 4 kurum suçundan birini işleyeceklerine karar vermek için örnek senaryolar verildi.

(1) Fiyat belirleme, (2) Rüşvet, (3) Satış istatistikleri manipülasyonu ve (4) Çevre Koruma Ajansı (EPA) emisyonlarının ihlali.

Yanıtlara dayanarak çıkartılan sonuç aşağıdaki gibi oldu:

1. Kurumsal suç işleyip işlememek kararları önemli bir şekilde algılanan teşvikler, hareketin caydırıcı önlemleri, örgütsel bağlamdan ve kurumun ahlaki ikliminden etkilendi.

2. Örgütün ahlaki iklimi de ifade edilen niyetler üzerinde etkiye sahipti.

3. Resmi ve gayri resmi öz saygı kaybı sonuçları suç işleme olasılığı üzerinde istatistiksel olarak önemli ölçüde etkisi vardı.

4. Kurumsal suç işlemeye olan eğilim, hareketin kişisel kariyer ilerlemesi ile sonuçlanacağı düşünüldüğünde ve kendisi için heyecanlı olacağı algılandığında daha yüksektir.

Paternoster ve Simpson, geçmişte bu tür çalışmaların, kurum suçlarında çok güçlü bir caydırıcı olabilecek ayıp ve utanç gibi belli gayri resmi yaptırımların gözden kaçırdığını kaydetti. Şirketler genelde iyi bir isim ve üne birincil varlık olarak değer vermektedirler. Gayri resmi yaptırımların, ahlaki değerlendirmelerin ve örgütsel faktörlerin dikkate alınması, beyaz yakalı suçun rasyonel bir fayda-maliyet analiz sonucunda suç işleme niyetini azalttığı görülmektedir.

Beyaz yakalı suç ve bilişim suçu için ortak olarak belirtilebilecek hususlar şu şekildedir: Her iki suç için de fail, kurbanlarından fiziksel olarak uzaktadır. Aynı zamanda işlenen fiilin suç olup olmadığı geleneksel suçlarda olduğu gibi siyah ve beyaz ayrımından ziyade gri alan içerisinde kalmaktadır (Seymour, 2013: 27). Failler bu eylemi gerçekleştirirken kasıtlı hareket etmektedirler ve belirli bir amaca yönelme içerisindedirler. Bu suç faillerinin genellikle geleneksel suçlarla ilgili bir sabıkaları yoktur.

3.2.5. Kontrol teorileri

Kontrol teorilerinin temelinde kriminolojinin genel olarak insan neden suç işler sorusunun yerine, insan neden suç işlemez sorusu yatmaktadır. İnsanın doğasından suç işlemeye meyilli olduğu varsayılmakta ve buna mani olan iç ve dış kontrol mekanizmalarının kurulması gerektiği kabul edilmektedir (Dolu, 2010: 262).

Bu kurama göre, insanlar, geleneksel düzene bağları kopması nedeniyle suç işlerler. Sosyal kontrol teorileri, insanların doğru ve yanlış arasındaki farkı öğrendiğini varsayarlar. Bu öğrenme, ya dini ve / ya da laik felsefeden ortaya çıkabilir. Bu sosyal kontrol bağı bozulduğunda, suçlu davranışı meydana gelebilir. Bu açıkça, ahlaklı bireylerin büyük bir getirisi olmadığında bile neden bilişim suçlarına yöneleceğini açıklamaktadır. Bu suçlu davranışının meydana gelmesine izin veren sosyal kontrol bağlarında zayıflığı oluşturan yasaların belirsizliği ve kurbandan uzaklık olabilir

(Seymour, 2013: 31). Öte yandan suç için özel bir açıklamaya gerek olmadığı, suçun beraberinde getirdiği para, mal, heyecan veya diğerleri üzerinde güce sahip olma gibi ödülleri zaten yeterli bir açıklama olduğu varsayılmaktadır (Polat, 2004: 48).

3.2.6. Düşük öz kontrol teorisi

Düşük Öz Kontrol teorisi, suçun belirli yönlerinin anlaşılmasına uygulanmıştır. Gottfredson'un ve Hirschi suç davranışına yönelik cazibeye karşı koyamayan bireylerin altı farklı özelliklerini aşağıdaki gibi sunmaktadır (Seymour, 2013: 29).

1. Dürtüsellik

2. Kısa dönem sonuçlarına yönelik basit görevler için tercih

3. Risk peşinde olma

4. Fiziksel olarak, zihinsel faaliyetler yerine fiziksel aktivitelerle ilgilenme eğiliminde olma

5. Öz-merkezcilik, başkalarına karşı duyarsızlık

6. Sinirlilik/huysuzluk

Bu teori ve Kontrol teorisi için istek, hemen altında, diğer suç teorilerinin aksine suçlunun sapkın özellikleri üzerine odaklanır. Piquero, Exum ve Simpson'a göre "bireysel kişilik" ile ilgilenmek daha önemlidir. Ancak, onlar Düşük Öz Denetim teorisi beyaz yakalı veya kurumsal suçlara başarıyla uygulanamadığını ortaya koymuştur: Bu sonuç, aşağıdaki faktörlerle açıklanmıştır (aktaran Seymour, 2013: 29).

1. Onların suça katılımlarına bakmaksızın, hayatlarını yasalara saygılı şekilde sürdüren vatandaşların çok daha farklı görünmemesi, böylece alışılmışlık ile karakterize olan bir sapmadır.

2. Beyaz yakalı meslekler genellikle, başkalarının ilgilerini ertelemeye istekli ve hazzı erteleme yeteneği gibi özelliklere sahip bireyleri tasvip eder.

Bilişim suçunun beyaz yakalı suçlarla ilgili ortak olan yönlerini bu teori ile açıklamak çok mümkün değildir. Ancak daha düşük düzeyde bilgi isteyen ve dürtüselliğin temel olduğu bilişim yoluyla işlenen 'Çocuğun cinsel istismarı' ve 'Çocuk müstehcenliği' suçlarının failleri için düşük öz-kontrol teorisinin geçerli olduğunu söyleyebiliriz.

3.2.7. Kontrol arzusu teorisi

Kontrol arzusu teorisi, gündelik yaşam olayları üzerinde kontrolün olması genel isteği ile ilgilenir. Burgher ve Cooper, bu istek ile karakterize olan insanları şöyle tarif eder (aktaran Seymour, 2013: 29):

"...iddialı, kararlı ve aktif. Onlar genellikle bu tür etkiler avantajlı olduğunda başkalarını etkilemeye çabalarlar. Onlar, istenilen sonuçları elde etmek için olayları manipüle ederek tatsız durumlardan veya başarısızlıklardan kaçınmayı tercih ederler. Bu kişiler, genellikle grup ortamlarında liderlik rolleri ararlar."

Bu tür insanlar başarılarını beceri, bilgi ve çaba gibi "istikrarlı" iç faktörlere ve kendi başarısızlıklarını kötü şans gibi "istikrarsız" dış etkenlere bağlama eğilimindedirler. Onlar, kendileri için elde edemeyecekleri hedefleri seçerler. Son olarak, kendi yetenek ve etkilerini abartma ve dolaysıyla zihinlerinde "kontrol illüzyonu" yaratma eğilimindedirler. Çünkü bu, böyle insanların hedeflerine ulaşmak için riskli davranış eğilimi gösterdikleri "kontrol illüzyonudur."

Piquero, kurumsal suçluların kontrolünün, yüksek arzu ve düşük öz-kontrole göre kıyasla, hareketlerinin gelecekteki etkileriyle birlikte şimdiki etkileriyle de daha çok meşgul olur (aktaran Seymour, 2013: 30).

Bu yazarlar kontrol özelliği için istekle ilgili aşağıdaki sonuçlara varmışlardır:

Suçlunun veya potansiyel suçlunun, kontrole olan arzusu nasıl bir rasyonel seçim yapılacağını etkiler. Suçlu davranışı ile ilişkili kontrol arzusu ve düşük öz-denetim gibi özelliklerin olmaması, gelecekteki sonuçlar için kaygıya sebep olabildiğinden, yaptırımlar birey ya da şirkete yönelik olduğunda, ağır ve belli gayri resmi yaptırımlar suçun caydırılmasında etkili olur. Öte yandan, sonuçları resmi yaptırımlar olduğunda ve

sadece bireye karşı uygulandığında, suçun şaşırtıcı bir şekilde caydırılması düşmektedir; ancak şirkete karşı uygulandığında suç caydırıcı nitelik kazanır. Suçlu davranışı ile ilişkilendirilen düşük öz-denetim ve kontrol arzusu gibi özelliklerin anormal olmadığı konusu da unutulmamalıdır. Bu özellikler, normal insanlar arasında istenilen özellikler olmamasının yanında, belli suçlara katılan suçlular arasında yaygın özelliklerdendir.

Bu motivasyonu hackerlık için kabul edebiliriz. Çünkü hackerlık fiili maddi menfaatten ziyade belirli bir fiili gerçekleştirme, yani güç gösterisi olarak kabul edilebilir. Hatta kendisine ait olmayan sistemleri kontrol ediyor olmak da, bir nevi bu duyulan arzuyu tatmin etmek olarak açıklanabilir.

3.2.8. Kontrol denge teorisi

Charles Tittle bireylerin yaşamları üzerindeki kontrollerinde dengesizlik olması durumunda sapkın davranışlarda bulunduğunu ileri sürmektedir. Bireyin, yaşamı üzerinde çok fazla kontrolü olması ya da yeterince kontrolü olmaması durumunda farklı şekillerde tepki verdiğini iddia edilmektedir. Kontrol Denge Teorisine göre, yaşamları üzerinde yeteri kadar kontrolü olmayan bireyler 3 farklı şekilde tepki vermektedirler ve buna 'baskıcı sapkınlık' denilmektedir (Imhof vd., 2010: 94).

Bireyin vermiş olduğu ilk tepki şekli saldırgan (yağmacı) davranışlarda bulunmaktır. Bu bir bireyin verebileceği en tehlikeli tepki yöntemidir çünkü bu en fazla zararı topluma vermektedir. Bu kategori altında değerlendirilen suçlar fiziksel zararlar ve mal hırsızlıklarıdır.

Bireyin kontrol eksikliğine gösterebileceği ikinci tavır 'başkaldırıdır'. Bu tür bir davranış gençlerde kolayca görünmektedir çünkü gençler genel olarak çevrelerinin çok az kontrolü altındadırlar.

Tittle tarafından önerilen, bireyin kontrol eksikliğine gösterebileceği son tepki çeşidi ise 'boyun eğmedir'. Bu teori dâhilinde, boyun eğenler kendilerinin kontrol edilmesine, kötü davranılmasına, istismar edilmesine ve aşağılanmasına izin veren bireylerdir. İstismarcı bir ortamda büyüyen bir birey, kendi çevresini ve koşullarını kontrol

edebilecek olmasına rağmen, diğer yaşam tiplerini bilemeyebilir ve sonuç olarak kendilerinin kontrol edilmesine ve kötü davranılmasına izin vermektedirler.

Bunun tam tersi durum ise çok fazla kontrole sahip bireyler, farklı olarak üç değişik şekilde davranabilmektedirler. Gösterebilecekleri ilk tepki suiistimal etmektir. Bu kategori altında hareket eden bireyler çevreleri üzerinde oldukça fazla kontrole sahiptirler ve bu kontrolü kaybetmediklerinden emin olmak için her şeyi yapacaklardır. Bu neden güçlü insanlar arasında dolandırıcılık ve yolsuzluğun bu kadar yaygın olduğunu açıklayabilmektedir.

Bireylerin çok fazla kontrole sahip olduklarında gösterebileceği ikinci tepki çeşidi yağmalamaktır. Bu tip bir davranışın, şiddet içeren davranışa sebep olabileceği için, üç tür içindeki en tehlikelisi olabileceği düşünülmektedir. Tarihte çok fazla gücün ve kontrolün insanları nasıl bozduğunu ve nasıl onların daha önceden oldukları kişilerden başka birisine döndürdüğüne ilişkin birçok örnek bulunmaktadır. 'Güç yozlaştırır, mutlak güç mutlak yozlaştırır.' sözü bu durumu gayet iyi ifade etmektedir.

Bireylerin çok fazla kontrole sahip olduklarında içinde bulunabilecekleri son davranış şekli ahlaki anlamda çöküştür. Bu temel olarak şu anlama gelmektedir; bir birey kendi fiziksel ve/veya zihinsel düşüşüne neden olacak davranışlarda bulunmuştur. Bunun klasik örneği bireyin bağımlı olmasına neden olan ilaç ve benzeri madde kullanımı olabilir.

Daha önce bahsedilen 6 davranış türünün, bir bireyin kontrol dengesizliğinden ne anladığının bir sonucu olduğu göz ardı edilmemelidir.

Ayrıca bu teori kontrol dengesizliği olan bir kişinin sapkın davranışlarla ilişkilendirmenin doğrudan gerekmediğini, bu dengesizliklerin bir eşikten sonra sapkın davranışları oluşturabileceğini belirtmektedir. Bireyin maruz kaldığı kontrol miktarı, onun sahip olabileceği/gösterebileceği miktara göreceli olarak, ne tür bir sapkınlığın oluşabileceğinin yanı sıra sapkınlık ihtimalini de belirlemektedir.

Imhof'un (2010: 97) da belirttiği gibi bu teori siber suçların dünyanın bazı bölgelerinde neden çok hızlı olarak yükseldiğini iyi bir şekilde açıklamaktadır. İnternetin rolü, onlara güç eksikliklerini kapatabilecekleri fırsatları sunmaktır. Örneğin, baskıcı bir ülkede bir

hacker internet erişimine sahip olabilmektedir ve bunu, uygulayabilecekleri kontrol miktarını arttırarak kontrol oranını arttırabileceği bir araç olarak görmektedir.

Genel olarak, bir birey, zararlı yazımları diğer makineleri kontrol etmek amacıyla geliştirerek, mesela botnet yaratarak, saldırgan davranışlarda bulunabilir. Eğer bu birey çok büyük bir botnet yaratırsa çok fazla güce sahip olabilir. Eğer yeterince güçlü olursa büyük organizasyonlarda iletişim altyapılarını kapatmamak için bu şirketlerden dilediklerini isteyebilir. Bunu isteyebilecek güçte olmak veya bu gücün farkında olmak onların kendilerinin kontrol duygularını önemli ölçüde arttırabilir.

3.3. Beyaz Yaka Suçluluğu ve Bilişim Suçları

Kriminolojinin bilişim suçlarına ilgi duymasındaki gecikme benzer şekilde beyaz yaka suçluluğu içinde yaşanmıştır. Çünkü her ikisi de ilk kriminolojik teorilerin temelinde yer alan faillerin belirli bir sosyoekonomik açıdan dezavantajlı konumunda bulunması gerekliliği ile çelişmektedir. Cohen, suçun sosyolojik açıdan ele alınmasında beyaz yaka suçluluğunu da katan bir açıklama ile kriminolojinin bu başarısızlığını ortaya koymaya çalışmıştır:

> "Toplum suçu nasıl yaratır? İlk olarak, toplumlar öyle bir yapılandırılmış olabilirler ki, toplumun belli kesimleri diğerlerine kıyasla suç oranlarına daha fazla katkı sağlayabilirler. 'Fakirlik suça neden oluyor' gibi çok genel determinist iddialarda bulunmaya gerek yok—ki öyle olsa bu çok saçma bir basitleştirme olurdu—fakat hiçbir sofistike araştırma ya da teori de sanayileşmiş Batı toplumlarındaki şu gerçeği saklayamaz: resmi olarak kaydedilen suçların çoğunluğu, sosyoekonomik merdivenin en altındaki kişiler tarafından işlenmektedir. Bu durum fırsat eşitsizliği, maruz kalınan baskı, hayal kırıklığı ve ümitsizlik deneyimleri ve (mutlak yoksunluktan ziyade) göreli yoksunlukla ilişkili olmasının yanında, aynı zamanda bu grubun (ve etnik azınlıkların) göreceli olarak tutuklama, mahkûmiyet ve cezalandırma gibi resmi kontrol mekanizmalarına karşı daha savunmasız durumda olmalarıyla da ilişkilidir. Toplumumuz, işçi sınıfındaki gençler gibi bazı kesimler için sorunlar yaratmaya devam edecektir ve sonrasında da

> bu gruplar yaşadıkları sorunlara karşı geliştirdikleri çözümler nedeniyle de kınanıp suçlanacaktır. Şunun farkına varmalıyız: bireycilik, maskülinite ve rekabetçilik gibi bizim için en üstün öneme sahip toplumsal değerlerimiz aynı zamanda suça neden olan değerler ile aynıdır. … Kriminologların çok uzun zamandır teorik olarak yaklaştıkları fakat gerçekte ciddi bir şekilde ele almadıkları diğer bir alan da beyaz yaka ya da "saygıdeğer" suçlar: vergi kaçırma, hileli reklam, yerel yetkili memurların yozlaşması, dev şirketlerin şaibeli işleri, ilaç şirketlerinin kanunu ihlal etmeleri gibi. Güvenilir şekilde yapılan her değerlendirme şunu göstermiştir: bu suçların neden olduğu finansal kayıp ve kamuya verdiği zararlar 'sıradan' suçlarınkinden çok daha fazladır…" (Cohen'den çeviren Topçuoğlu, 2004: 270, 271, 278)

Suçların bu şekilde ele alınması gerektiğinden, Philadelphia'da 1939 yılında ilk kez Edwin Sutherland tarafından 'Beyaz Yaka Suçları' kavramı kullanılmıştır.[19] Sutherland toplumun üst kesimindekiler tarafından işlenen suçların göz ardı edildiğini; aslında bu suçların çok daha ciddi ve toplum için daha zararlı olduğunu belirtmiştir. Beyaz yaka suçluluğu için üst seviyedeki, saygın pozisyondaki kişilerin herhangi bir fiziki bir uygulama olmaksızın, hukuka aykırı dolandırıcılık ve aldatma fiilleridir diyebiliriz (Karagülmez, 2005: 45).

Bilişim suçlarının da işlenebilmesi için hem teknik alt yapı, hem üst düzey teknolojik bilgi gerektirmesi, çoğu bilişim suçunun da beyaz yaka suçları arasında değerlendirilmesine sebep olabilir. Çünkü sahip olunması gereken bilgi ve teknik araçlar, düşük sosyoekonomik düzeydeki insanlarda bulunması gereken vasıflar ve imkânlar değildir. ABD'de bilgisayarı suçta en fazla kullananların da, beyaz yaka suçluları olduğu kabul edilmektedir (Karagülmez, 2005: 46).

Beyaz yakalı suç gibi bilişim suçu, genellikle bireysel suçlunun ve onun yakınları yararına işlenir. Bundan dolayı, fiziksel ceza, parasal ceza veya utanç gibi caydırıcılık sadece bireysel saldırganın bakış açısına göre değerlendirilebilir. Siyasal ya da ideolojik nedenlerle işlenen bilişim suçları, bu durumun istisnası sayılabilir.

[19]The American Sociological Association İnternet Sitesi http://www.asanet.org/about/presidents/Edwin_Sutherland.cfm (Erişim tarihi: 11.05.2015)

O zaman, bilişim suçunu birçok yönden beyaz yakalı suça benzediğini belirtmek zorunludur ve bu suç biçimi Rasyonel Tercih Teorisi ve diğer suç teorilerinden faydalanılarak anlaşılabilir. Her iki suçun kurbanları fiziksel olarak saldırganlarından uzaktadırlar. Her ikisi de yanlış ve doğruyu tanımlamak için belirsiz yasalara sahiptir ve kanunlarda bazı muğlak hususlar vardır. Beyaz yakalı suçlar, "yasadışı davranışa ilişkin ortak örgütsel uygulamalar ihlalin önemini itibarsızlaştırdığında veya yasanın belirsiz olduğu gri alanlarda sıklıkla görülür", Piquero, Exum and Simpson ve Kadish'e, göre beyaz yakalı suç, hesaplı, kasıtlı ve ekonomik kazanca yöneltilmiştir (Seymour, 2013: 27).

Bilgisayar suçu, ancak, sadece ekonomik kazanç için olmamasına rağmen, aynı zamanda hesaplı ve kasıtlıdır. Genellikle, beyaz yakalı ve bilişim suçu faillerinin başka bir suç alanlarında öyküsü yoktur.

Ahlak ve yaptırım gibi hususlar, bazı göze çarpan istisnalarla, büyük olasılıkla bu suçlarda caydırıcıdırlar. Bu tip beyaz yakalı suçlarda bireyin suçtaki menfaatleri ile birlikte alacağı cezayı ve/veya yaşayacağı itibar kaybını ölçmesi sonucu suç işleme kararı vermesi beklenir.

3.4. Bilişim Suçu Faillerini Suç İşlemeye İten Nedenler

Bilişim suçunun failleri çeşitli nedenlerle bu suçları işlemektedirler. Bu nedenleri suçun öncesindeki -kişisel nedenler ve suç sonrasındaki nedenler- ceza almama inancı olarak iki kategoride ele alabiliriz.

3.4.1. Suç öncesi nedenler

Suç öncesi nedenlere bakıldığında, bu suçu işlemedeki amaç her ne kadar maddi menfaat sağlamak gibi gözükse de; birçok diğer sebep de bu suçun işlenişinde etkili olabilmektedir. Maddi çıkarın ötesinde özellikle bilişim suçlarının kanunda tanımlanmış olan eylemlerine bakarsak, "yalnızca kişisel bir zevk almak ve tatmin olmak, yapabildim diyebilmek için hareket eden bilişim korsanlarının hukuka aykırı olarak

verileri ele geçirmek gibi çeşitli eylemlerin" (Dülger, 2013: 119) cezalandırılması amacı güdüldüğü görülmektedir.

Jordan ve Taylor (2010: 231), korsanların bilgisayar ve ağlarına duydukları ilgi ve meraktan dolayı bu suça meyil ettiklerini ileri sürmüştür. Hatta bu merak duygusunun normal yaşantılarındaki heyecanlarından çok daha baskın olduğunu daha fazla heyecan vermesi sebebiyle çevrimiçi fiiller gerçekleştirdiğini belirtmektedir.

Clough ise bilgisayar korsanı için verinin içeriğinin bilinmesinden ziyade veriye ulaşılabilmesi daha önemli olduğunu ileri sürmüştür (aktaran Dülger, 2013: 119). Bunun göstergesi olarak da Zone-h gibi internet sitelerinde korsanlar tarafından hacklenen sitelerin duyurularının yapılıyor olması sayılabilir. Bu şekilde fail kendini ispatlamış olmakta ve bu alanda popülarite kazanmaya çalışmaktadır. Aslında bu pek çok korsan için en önemli motivasyondur. Bu şekilde topluluk içinde kabul görülür ve hiyerarşide daha üst pozisyona gelebilir (Jordan ve Taylor, 2010: 231). Eğer ki, siber saldırıya maruz bırakılan hedef, CIA (Central Intelligence Agency) gibi ulusal veya uluslararası arenada önemli bir yerde ise güç sahibi olabilmenin çekiciliği daha da dikkate alınması gereken bir faktördür. Açılımı Merkezi İstihbarat Teşkilatı olan CIA'in korsan saldırılar sonucu açılımı Merkezi Budalalık Teşkilatı olan CSA (Central Stupidity Agency)'ye çevrilmesi bu güç hevesinin bir göstergesidir (Jordan ve Taylor, 2010: 221).

Hactivizm de ise; hackleme eylemleri siyasi veya ideolojik bir amaç doğrultusunda gerçekleştirilmekte, bu ses getiren eylemler vasıtasıyla propaganda yapılmaktadır. Bu eylemlerde hedefler genellikle kamu kurumlarına veya dünya çapında faaliyet gösteren büyük şirketlere ait internet siteleri olabilmektedir.

Siber terörizm kavramı ise, terör amaçlı eylemlerin bilişim yöntemleri kullanılarak gerçekleştirilmesine denilmektedir. Özcan ise siber terörizmi "bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması amacıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinlikler" olarak tanımlamıştır (aktaran Dülger, 2013: 158). Bu eylemlerdeki amaç silahlı terör

eylemlerinde olduğu gibi halk içinde korku ve panik yaratarak devlete ve kamu kurumlarına olan güvenin sarsılması amaçlanmaktadır.

Kimi zamanda bu suçun failleri yaptıkları eylemleri iyi niyetli olarak yaptıklarını düşünmekte, sadece sistemin açığını göstermek için yaptıklarını iddia etmektedirler. Bu şekilde iyi niyetli olup herhangi bir zarar vermek istemeyenlere 'beyaz şapkalı hacker' denilmektedir. Bunun tam tersi kastla hareket edenlere ise 'siyah şapkalı hacker denilmektedir. Her iki kast ile hareket edenlere ise 'gri şapkalı hacker' denilmektedir.

3.4.2. Suç sonrası nedenler

Suç sonrasındaki nedenler ele alındığında ilk öne çıkan yaptıkları işte uzman olduklarına inanmalarından dolayı asla yakalanmayacaklarını sanmaktadırlar ve "bilgisayarlar, daha önce hiçbir suçta görülmemiş bir biçimde suçu işleyenlere, kimliklerini gizleme imkânı sunmaktadır…" (Karagülmez, 2005: 51). Kanundaki cezai karşılıklarının diğer suç tiplerine göre daha hafif oluşu da yakalandıklarında alacakları cezalardan çekinmemelerine sebep olmaktadır.

Soruşturma ve kovuşturma aşamasında delil toplama eylemlerinin oldukça zor olması, yeterli delil elde edilmesinin çok güç olacağı kanaati uyandırmaktadır. Doğru faile ulaşılsa bile fail kendisinin de mağdur olduğu, kendisine ait kimlik, kullanıcı, IP (Internet Protocol) bilgilerinin kullanıldığını iddia edebilmektedir. Çünkü bu alanın ne kadar suiistimallere açık olduğunu gayet iyi bilmektedirler.

Öte yandan failin soruşturma yapan kolluk birimlerinin bilgi ve becerilerinin düşük olduğuna ve bu yüzden kendisine asla ulaşamayacaklarına inanması işledikleri suç sonunda herhangi bir yaptırımla karşılaşmayacaklarına olan güvenlerini daha da artırmaktadır.

3.5. Bilişim Suçu Faillerinin Özellikleri

Günümüzde hemen herkes teknolojik cihazları bir şekilde kullanabilmektedir. Hatta akıllı telefonlar sayesinde her zaman yanı başında ve hayatın en mahrem anlarına dahi

teknoloji girebilmektedir. İnsanların bunları kullanabilmek için belirli bir düzeyde teknolojik bilgi ve beceriye sahip olmaları gerekmektedir. Ama bu gereken bilgi temel düzeyde olmaktadır. Çünkü artık teknolojik şirketler kullanıcı dostu ara yüzler (user-friendly interface) kullanarak kullanıcıları teknik kısımdan olabildiğince uzak tutmak istemektedir. Hatta bu seviye olabildiğince aşağı çekilmeye çalışılmış, kullanılan ara yüzler için aptal dostu ara yüz (idiot-friendly interface) kavramı dahi ortaya çıkmıştır.

Bilgisayar veya diğer teknolojik cihazları kullanabilen herkes bu suç için fail olamaz, teknoloji konusunda günlük yaşantı ihtiyacının ötesinde bir bilgi ve beceriye sahip olmaları gerekmektedir. Bilişim suçlarına ilişkin yapılan araştırmalar bilişim suçu faillerinin genellikle; genç, eğitimli, teknik yeteneğe sahip ve agresif olduğunu ortaya koymuştur (Karagülmez, 2005: 51).

Öte yandan kişisel bilgisayarların yaygınlaşmasıyla, bilişim suçu için kullanılan araçlar da yaygınlaşmış ve internetteki açık kaynaklardan ulaşmak ve video içeriklerinden anlayarak kullanmak, konuyla ilgilenen kişilerin yatkınlık düzeyine göre giderek kolay hale gelmektedir. Ama verilere ulaşmak ne kadar kolay olursa olsun bu fiilleri gerçekleştirmek için günlük kullanıcı bilgisinden fazlası gerekmektedir.

Özellikle örneğin hedef alınan banka veya kamu kurumları gibi yüksek düzeyde güvenlikle korunan sistemlere erişmek için ise gereken bilgi düzeyi en üst seviyededir. Kişisel bilgisayarların kullanımıyla birlikte bu tip sistemlere yapılan müdahaleler içeriden gerçekleşmekten daha çok dışarıdan yapılan yetkisiz erişimlerle meydana gelmeye başlamıştır (Dülger, 2013: 122).

Bilgisayarlar ve teknolojik gelişmelerle ilgili ileri düzeyde bilgi ve beceri ya da ortalamanın üzerinde yatkınlıklarının bulunması faillerde görülen başlıca özelliklerin başında gelmektedir. Bunun yanı sıra Ksander bu özelliklerine meraklı olmayı, detaylarla ilgilenmeyi, kendi meslek veya tutkularıyla ilgili problem veya sıkıntılı konuları çözmeyi, sezgiye dayalı düşünmeye yönelmeyi ve zor konularda orijinal çözümler üretmeyi eklemiştir (aktaran Karagülmez, 2005: 51).

Ayrıca korsanlar için erkek baskınlığı durumu mevcuttur. Genellikle toplu olarak hareket ederler ve en önemli motivasyonlarından biri de bu topluluktur. Gizliliğe önem verirler; ancak bu iki yönlüdür. Hem yakalanmamak için gizli kalmak, hem de

popülarite ve bilginin yayılması için alenilik. Bir korsan grubu üyesi olan Zoetermeer "bilgisayar korsanlığı kendisi bir ödül sayılır, çünkü bazen size gerçekten heyecan verir. Ancak deneyimlerinizi başkalarıyla paylaşırsanız sizi çok daha fazla tatmin eder ve tanınmanızı sağlar… Bu grup olmasaydı işletim sistemlerine girmek için ekran başında bu kadar vakit geçirmem imkânsızdı." (Jordan ve Taylor, 2010: 227).

Fail özelliklerine ilişkin ülkemizde yapılmış en kapsamlı çalışma Eriş tarafından gerçekleştirilen Türkiye'de Hacker Kültürü isimli doktora tezinde 258 hacker ile yaptığı görüşmedir. Bu görüşmeler sonucunda failler için ön plana çıkan özellikler, genellikle erkek oldukları, 14 - 21 yaş aralığında ve genellikle öğrenci oldukları bilgisine ulaşmıştır. Gelir düzeyleri orta alt seviyede ve eğitimi düzeyi ise lise ve üniversite düzeyindedir (Eriş, 2011).

Eriş'in de belirttiği üzere (2011) özellikle ülkemiz hackerlarının diğer ülke hackerlarından ayıran motivasyonu ise ülkü, milliyetçilik, din gibi faktörlerdir. Dünya genelinde özgürlük ve anarşist motivasyonlar ön plandayken; Türkiye'de ise bilakis milliyetçilik ve muhafazakârlık temel saikler durumundadır.

Bilişim suçu faillerinin özellikleri, caydırıcılıktan etkilenmelerine göre ele alındığında şu şekilde bir sonuç ortaya çıkmaktadır. Bilişim suçu failleri kendilerini bu işin uzmanı olarak gördükleri için, caydırıcılıktan etkilenmeleri düşüktür. Çünkü genelde bilişim suçlarıyla mücadele eden görevlilere kıyasla kendilerinin bilgilerini oldukça iyi olduğuna inanmaktadırlar. Riske attıkları şeyler ne olursa olsun yakalanma risklerinin diğer suçlara kıyasla daha düşük olmasından dolayı caydırıcılıktan etkilenme oranları düşüktür. Hackerların yaş ortalamasının 14 - 21 yaş arasında olduğu ve genel itibariyle bilişim suçu faillerinin yaş ortalamalarının düşük olduğu bilindiğinden, yine yaşlılara göre caydırıcılıktan etkilenmeleri oranı düşüktür. Ayrıca, faillerin büyük çoğunluğunun erkek olmasından dolayı da kadınlara göre caydırmaya yönelik faktörlerden etkilenmeleri düşüktür. Sosyoekonomik durumları genelde geleneksel suçlardaki gibi düşük değildir. Bu özellikleriyle caydırılma oranları yüksektirler. Genel itibariyle bilişim suçu failleri özellikleri caydırıcı etkinin çok fazla etkili olmadığı bir profil çizmektedir.

4. Karmaşık ve Modern Bir Sorun: Bilişim Suçları

4.1. Suç Kavramı

Suç, topluma zarar verdiği ya da tehlikeli olduğu kanun koyucu tarafından kabul edilen ve belirtilen eylem, davranış, tavır ve harekettir (Dönmezer, 1981: 62). Suç devletin hukuk nizamı içinde kendisine netice ve müeyyide olarak ceza konulmuş olan fiildir (Gözübüyük, 1988: 4). Sonuç olarak suç haksız bir davranıştır ve suçun mağduru olan kişiye maddi ve manevi zararlar verir.

4.1.1. Suçun maddi ve manevi unsuru

Manevi unsur, işlenen fiil ile kişi arasındaki manevi bağı ifade etmektedir. Bu bağ tesis edilmeden, gerçekleştirilen davranış fiil niteliği taşımaz ve dolayısıyla, bir suçun varlığından söz edilemez (Özgenç, 2007: 223). Suçun manevi unsurunu kusurluluk oluşturur. Kusurluluktan kasıt ise fiilin kusurlu olmasıdır.

Bir suçun söz konusu olabilmesi için, kanuni tarifine uygun bir fiilin bulunması şartı, maddi unsuru ihtiva eder (Özgenç, 2007: 223). Suçun maddi unsuru fiilidir. Ceza hukukunda fiil denilince hareketle netice arasında bulunması gereken nedensellik bağı anlaşılır (Kurt, 2005: 157).

4.1.2. Hukuka aykırılık unsuru

Bir fiilin suç sayılması için kanunda gösterilmiş olması ve karşısında bir ceza bulunması lazımdır (Özgenç, 2007: 223). Bir suçun varlığı için, suçta kanunilik prensibinin zorunlu bir sonucu olarak, işlenen fiilin kanunda gösterilen tarife uygun olması gerekir (Özgenç, 2007: 278).

4.2. Bilişim

1960'lardan sonra teknoloji dünyasında yaşanan hızlı gelişmeler, toplum hayatında önemli ölçüde etki yapmıştır. Özellikle bilginin iletilmesinde geliştirilen yeni cihazlarla, yapılan işlem sürecin hızlanması ve mekânın önemini yitirmesi, "bilişim" kavramını ortaya çıkarmıştır. "Bilginin ekonomik bir değer olması, yonga temelli cihazların hayat içerisinde çok önemli bir paya sahip olması gerçeği ile birleşince", yeni dönemin bilişim teknolojileri çevresinde toplandığı söylenebilir (Tanşu, 2004: 140).

Bilişim sözcüğü; Fransızca *"informatique"* kelimesinden Türkçe'ye uyarlanan "enformatik" ya da "enformasyon" sözcüklerinin yerine türetilmesi ile oluşmuştur.

Aydın'ın ifadesi ile bilişim; "bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerden ve öte yandan da; bilgiyi kaynağından alan alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir" (Aydın, 1992: 3).

Türk Dil Kurumuna göre ise bilişim; "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir[20]."

Akıncı ve diğerleri tarafından bilişim aşağıdaki şekilde tanımlanmıştır; "verileri otomatik işleme tabi tutan, bilgi işlem ve iletişim kavramlarının her yönüyle bir araya geldiği elektronik teknolojisi olup, bilişim cihazlarının geliştirilmesi ve kullanılması faaliyetini tanımlayan en güzel ibaredir" (Akıncı, 2004: 157).

Değirmenci (2002: 7) ise bilişimi, "teknik, ekonomik, sosyal, hukuki alandaki verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi ve aktarılması" şeklinde ifade etmektedir. Dülger'in (2004: 220) kendi yapmış olduğu bilişim tanımlamasında "…bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı bir

[20]Türk Dil Kurumu Resmî İnternet Sitesi
http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.56775c57b3a548.07423531 (Erişim tarihi: 21.12.2015)

biçimde işlenmesi…" gerektiği vurgulanmaktadır. Kardaş (2003: 7) ise bilişim kavramını, "insan bilgisinin, teknik, ekonomik ve sosyal alanlardaki iletişimin otomatik makinelerde akılcı olarak işlenmesini konu alan bilim" olarak vermektedir. Görüldüğü üzere bilişim tanımlaması yapılırken, "bilginin işlenmesi aktarılması ve saklanması" üzerine vurgu yapılmıştır (Kurt, 2005: 157).

Bilişim kelimesi "bilgisayara göre daha geniş bir alanı kapsayıp, bu haliyle üst bir kavramdır". Özel (2004: 341) ise bilişimin, "bilgisayardan faydalanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini" ifade ettiğini belirtmektedir.

Bilişim kavramı için "bilginin elektronik olarak işlenip, yüksek hızla veri, ses ve görüntü kaydı taşıyan iletişim hatları aracılığıyla aktarma faaliyetlerinin gerçekleştiği alan" şeklinde bir tanımlama da yapılmaktadır (Yazıcıoğlu, 1997: 19). Bu noktada bilgisayarın, yapılanan faaliyetleri gerçekleştiren en önemli aygıt olduğunu görüyoruz.

Bilişim teknolojilerinin gelişimi, aslında bir anlamda da toplumsal yapılanmaların yeniden şekillenmesi şeklinde yorumlanabilir (Şehitoğlu, 2005). Özellikle tüm insanlık tarihi boyunca, gerçekleşmiş olan toplam teknolojik gelişmenin önemli bölümünün 20. yüzyıl içerisinde gerçekleştiği göz önüne alındığında, bilişim teknolojilerinin yarattığı etkiler; toplumsal yapıların kırılganlığı ve geçişkenliği çatışmalara neden olabilmektedir (Çubukçu, 2010).

Bilgi teknolojilerinin hızla gelişimi, bu gelişmelere aynı hızda ayak uydurabilecek bir toplum yapısı geliştirme ihtiyacını doğurmuştur. Özellikle bilişim kavramının gelişmesi sonucunda yaşanan sosyoekonomik alandaki değişmeler, toplumun her alanında da değişimini gerektirmektedir.

Bilişim teknolojisindeki gelişmelerle birlikte, sanayi ekonomisi yerini bilgi ekonomisine bırakırken, ekonominin üçlü sacayağı olarak nitelendirdiğimiz üretim, tüketim, dağıtım ilişkileri ve ekonomik yapının tümü, bilgi temeli üzerine yeniden yapılanmış ve bilgi rekabetin temel faktörü durumuna gelmiştir (Tekin ve Çiçek, 2006). "Bilgi toplumu" olma hedefindeki toplumlar, istikrarını sürdürebilme adına bilim ve teknolojiye daha fazla önem vermektedirler. Bu bağlamda; gelişen teknoloji değişen gereksinimler artan

nüfus bilgiye olan gereksinimi, bilgi kullanımını ve bilgi güvenliğini de ön plana çıkarmıştır.

Toplumsal ve kurumsal açıdan bilginin ve otomasyonun değerinden ötürü çağı yakalamak adına bilişim alanına yatırımlar kaçınılmaz hale geldiği aşikârdır. Diğer yanda bireysel olarak da insanlar özellikle akıllı telefonlar sayesinde bilişimin sürekli içinde olmakta ve mikro ölçekte de olsa yatırımlar yapmaktadır.

4.3. Bilişim Suçu

Günümüzde bilişim teknolojilerinde yaşanan hızlı gelişmeler, yaşamımızın her alanında getirdiği kolaylıkların yanında, yeni suçların işlenmesine zemin hazırlamaktadır. Teknolojiye bağlı olarak bilişim alanına kazandırılan her türlü araca bağlı olarak işlenen suç şekilleri de sürekli gelişmektedir. İnternetin özellikle hukuksal alanda pek çok davranış şekilleri ile birlikte yeni sorunları da beraberinde getirdiği söylenebilir (Özberk, 2002: 101).

Özcan'ın bilişim suçunun kapasitesini ve sonuçlarını aşağıdaki gibi açıklamaktadır (aktaran Dilek, 2007: 8)

> "21. yüzyılın en önemli güç kaynağı hiç şüphesiz bilgidir. Bilgiyi elinde tutan gücü de elinde tutmuş olmaktadır. Bilginin gücüyle teknolojik alandaki gelişmeler tüm yaşamımızı olumlu yönde etkiliyor. Internet, bilgisayar, uydular, cep telefonları gibi. Bunlar sadece günlük yaşamımıza giren teknolojinin ürünlerinden bazıları. Yine bilginin gücünü kullanarak aynı araçlar birer silaha dönüşebilmekte ve karşımıza siber savaş ve siber terör kavramları çıkmaktadır. Siber terör, yeni yüzyılda terörizmin yeni yüzü olarak yansıyacaktır ki teröristlerin elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis,

hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dâhilindedir."

Yukarıdaki bölümlerde geçen bilişim kavramının tanımındaki fikir birliği, bilişim suçu tanımında görülememektedir. Bilişim suçunun tanımı yapılırken, suçun en keskin ve en belirsizlik taşıyan "ceza kanunu tarafından yasaklanan davranıştır." (Polat, 2004: 31) tanımından yola çıkarsak dünya genelinde ülkelerin bilişim suçu olarak kastedilen suçları, mevzuatlarında farklı terimlerle belirttikleri görülmektedir. ABD'de "computer crime", "cyber crime" veya "computer related crime", İngiltere'de "high-tech crime", Almanya'da "computer-kriminalität", İtalya'da "la criminalitá informatica", Fransa'da "la fraude informatique" olarak adlandırılmaktadır (Yazıcıoğlu, 1997: 125 - 128).

Bilişim suçlarının ilk çıktığı ABD'de bugün en hakim olan kavram olarak 'computer crime' yani 'bilgisayar suçu' terimi kullanılmaktadır. Amerikan hukukundaki bu kavramın açıklaması ise; "bilgisayar verilerinin çalınması ya da sabote edilmesi veya herhangi bir suçun işlenmesi için bilgisayarın kullanılması gibi bilgisayar teknolojisini gerektiren suç çeşidi" şeklinde yapılmaktadır (Dülger, 2013: 64).

Türkiye'deki durum ise biraz daha karışıktır. Bu suç türü için kullanılan terimler: siber suç, sanal suç, internet suçu, bilgisayar suçu, bilgisayar ile ilgili suç, bilişim sistemi aracılığı ile işlenen suç bilişim alanında işlenen suç, bilgisayarlara karşı işlenen suç, bilgisayarlar aracılığıyla işlenen suç ve bilişim suçudur (Dülger, 2013: 66).

Ancak bunların içinde dünümüzde en ön plana çıkan 'bilişim suçu' ve 'siber suç' kavramlarıdır. Hatta bu suçla mücadele için İçişleri Bakanlığı Emniyet Genel Müdürlüğü tarafından 2011 yılında kurulan Bilişim Suçlarıyla Mücadele Daire Başkanlığı da bu suç biçiminin yaygınlığını ve buna karşı tedbir alınmasının önemini göstermektedir. Ancak suçun işlenişi, mağdurun ve suçlunun mekânsal özerkliği sebebiyle soruşturmasının uluslararası arenada sıklıkla yönetildiği göz önüne alınması ve bu sebeple bilişim suçu kavramı yerine daha evrensel kavram olan siber suç (cyber crimes) kavramının kullanılasına karar verilmiştir. 2013 yılında Bilişim Suçlarıyla Mücadele Daire Başkanlığı ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir.

Adı geçen suçları tanımlamak için en uygun kavramın ‘bilişim suçu’ veya ‘siber suç’ olduğunu kabul etmek gerekir; ancak bu kavramlarla kast edilenin ne olduğu için şimdiye kadar ortaya atılmış görüşlere bakmak gerekir.

Tanım yapılması için en büyük sıkıntı hangi fiillerin bilişim suçu sayılacağı, hangi fiillerin bilişim suçu sayılmayacağı konusundaki sınıflandırmada yaşanmaktadır. Bu fiil için kullanılan terimlere bakıldığında bilgisayar suçu, bilgisayar ile ilgili suç gibi kavramların kullanıldığı görülmektedir. Bilgisayar temelli tanımlamaların kısmen dar, kısmen de içeriği sarsacak kadar geniş olması sıkıntısı bulunmaktadır. Ancak Orlovskaya’nın dediği gibi (aktaran Karagülmez, 2005: 39) bilişim suçları, hem bilişim teknolojisine ilişkin bilgi birimi hem de bu alanda özel bazı yetenekler gerektirdiği için, farklı yapıda ve kriminolojik açıdan belli nitelikte failleri gerektiren, aslında herkesin işleyemeyeceği ‘üst seviyede’ suçlardır. Buna bağlı olarak bu suçların her gün yeni işleniş modelleri ortaya çıkmaktadır. Bilişim suçlarının bu özellikleri ve teknolojiyle birlikte sürekli yenilenmesi nedeniyle, kriminologlar, yasa koyucular, öğreti ve uygulayıcılar arasındaki tanım tartışması süreklilik göstermekte ve tek bir tanım üzerinde uzlaşma sağlanamamaktadır. Çünkü işlenebilecek suçların sınırı yoktur, hayatımıza giren teknolojinin boyutu genişledikçe, bu yollarla işlenen suçların hayatımızdaki etki gücü o kadar artmaktadır.

Bilgisayar temelli veya bilgisayar aracılığı ile işlenen her suçun ‘bilişim suçu’ olduğunu kabul edersek, Türk Ceza Kanunu’nda yer alan suçların nerdeyse tamamının bilişim suçu olabileceği anlamı çıkmaktadır. Örnek vermek gerekirse, alacağını tahsil etmek için muhatabına mail atarak borcunu ödemezse çocuklarını öldüreceğinden bahisle tehdit etmek bilişim suçu mudur? Sahibinden.com isimli internet sitesi üzerinden araba almak isteyen kişinin, tanımadığı kişiye önden kapora göndererek, daha sonrasında hiçbir şekilde ulaşamayarak dolandırılması, bilişim suçu mudur? Ya da Facebook isimli sosyal medya sitesinden eski eşinin müstehcen fotoğraflarını herkesin görebileceği şekilde yayınlayarak eski eşini etiketleyen adamın gerçekleştirdiği fiil bilişim suçu mudur? Bu soruları bilişim suçları hakkında tanımlamaları ve kriterleri değerlendirdikten sonra ele almak daha uygun olacaktır.

Bilişim suçlarına ilişkin öğretideki tanımlar incelendiğinde karşımıza çok sayıda tanım çıkmaktadır. Hatta bilgisayar suçu ile bilişim suçu birbiri yerine kullanılmış, ancak

ortak bir tanım yapılamamıştır (Karagülmez, 2005: 38). Bilişim suçuna yönelik tanımlar aşağıdaki gibi çeşitlilik göstermektedir.

Bilişim suçlarının tanımı için Akbulut, "verilere veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar" tanımını kullanırken; İçel ise bilişim suçları, bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik eylemler olduğu şeklinde tanımlamıştır. Aydın ise bilgisayar kullanılarak, başkalarının malvarlığına yönelik yapılan her türlü kasıtlı saldırı, tecavüzler olarak bilişim suçunu tanımlamıştır (Dülger, 2013: 68).

Tiedemann ise aracı veya gayesi bilgisayar olan suçluluk görünümleri bilişim suçu olacağını belirtmiştir (Karagülmez, 2005: 39). Uzunay ise bilişim suçu için ceza kanununu ihlal etmesi gerektiğini, işlenmesinde veya araştırılmasında bilgisayar teknolojisi bilgilerini içermesi gerektiğini belirtmiştir. (Atalıç Taş, 2010: 3) "Ceza kuraları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller" tanımı da bilişim suçu için bilgisayar ve benzeri donanımların bu suç için temel şart olduğunu ortaya koymaktadır (Yazıcıoğlu, 1997: 142).

Durmaz (2005: 69) ise; "elektronik malzeme ve bilgisayar kullanarak, bilişim sistemleriyle veya bilişim sistemine karşı işlenen, kişisel hak ve hürriyetin ihlal edilmesine, illegal yollardan menfaat ve maddi kazanç elde edilmesine, kuruluş ve kişiler lehinde menfaat sağlanmasına yönelik yapılan, verilerle veya veri işlemle konu bağlantısı olan suçları bilişim suçları" olarak tanımlamıştır.

Bilişim suçu için Dülger (2013: 69), "verilere ve/veya veri işleme bağlantısı olan sistemlere veya sistemin düzgün ve işlevsel işleyişine karşı, bilişim sistemleri aracılığıyla işlenen suçlar" tanımında bulunmuştur.

"Bilgisayar ve İnternet teknolojilerinde yaşanan hızlı gelişmeler nedeniyle bu alanda işlenen suçlarının tanımlanmasında tek bir tanım yeterli olamamaktadır. Bu konuda Birleşik Devletler Ceza Usul Komisyonu (U.S. Sentencing Commission) bünyesinde oluşturulan 'Bilişim Suçları Çalışma Grubu'nun hazırladığı raporda bilişim alanındaki suçlar açısından suçun tanımının ortaya konmasının önemi belirtilmiştir. Özellikle

tanımlama yapılırken klasik yöntemlerle de işlenen bazı suçların bilgisayarlarla işlenmesi durumunda 'Bilişim Alanı'na giremeyeceğinin belirtilmesi gerektiği vurgulanmıştır." (Taber, 1979'dan aktaran Durmaz, 2005: 68).

Dönmezer ise bilişim suçları için tanımı, bilgisayarın kötüye kullanılması, bilgileri otomatik isleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar şeklinde yapmaktadır. Parker ise bilişim suçları tanımını, işlendiği takdirde faile çıkar sağlayacak bir şeyler kazandıran ya da kurbana kaybettiren, aynı zamanda bilgisayar kullanımı veya teknolojisi bilgisi içeren herhangi kasıtlı bir davranış olarak vermiştir (Boğa, 2011: 12).

Emin Aydın bilişim suçlarını; "elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekillerde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılması" şeklinde tanımlamıştır (aktaran Gözüşirin, 2011: 26).

Bir suçun bilişim suçu olabilmesi için Başoğlu (2008) dört kriter getirmiştir:

"İşlenmesinde ve soruşturmasında teknik bilgi gerekir, bilgi paylaşımı son derece hızlı ve geniş kapsamlıdır,

· Soruşturma aşamasında kanuni ve teknik zorluklar kaçınılmazdır,

· Olası suç yöntemleri hayal gücü ile sınırlıdır,

· Sınır ötesi suçlardan olduğu tartışılmazdır."

Bilişim suçlarına ilişkin mutabık olunan bir tarif yoksa da ilk olarak uluslararası kabul gören tariflerden biri Avrupa Ekonomik Topluluğu (AET) Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu 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 davranıştır. Üyesi bulunduğumuz AET bir tavsiye kararında bu suçları beşe ayırmıştır.

Bunlar sırası ile:

a. Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,

b. Bir sahtekârlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

c. Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

d. Ticari anlamda yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,

e. Bilgisayar sistemi sorumlusunun izni olmaksızın konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmaktır.

Görüldüğü üzere yukarıdaki tanımların uzlaşabildiği bir tanım yoktur. Bu kavramsal boşluk ister istemez hukuki boşluklara da yol açmaktadır. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'nın 2012 tarihli kuruluş genelgesinde görev alanına giren suçlar tarifi yapılırken sadece Türk Ceza Kanunu'nda yer alan maddelere ve fıkralara atıf yapılmış ancak bunun da yetersiz ve belirsiz kaldığı uygulamalarda karşılaşılmaktadır.

Tüm bunların ardından bilişim suçundan ne anlaşılması gerektiği için öncelikle, suçu fail - eylem - araç - mağdur çerçevesinde değerlendirilirse, bilişim suçundan ne anlaşılması gerektiği konusunda daha uygun bir tanım geliştirilebilir.

Kimler fail olabilir? Fail, bilişim suçunun failinin üst düzey bilgisayar ve teknoloji bilgisi olması gerekir. Bununla birlikte bu bilgisini başka insanların hak ve özgürlüklerini ihlal etmek için kullanıyor olması ve bunun sonucunda da maddi veya manevi menfaat elde etmesi gerekir.

Hangi eylemler bu suçu oluşturabilir? Bilişim tanımında geçen iletişimi sağlanan ve işlenen verilere yapılan manipülatif eylemlerdir. Ancak bu eylemler, kablonun kesilmesi gibi basit eylemlerden ziyade yüksek bilgi ve yetenek gerektirir. Ancak bu fiil için gerçek zamanlı olmasına gerek yoktur. Örneğin, ileri bir tarihte aktif olacak virüslü bir

web sitesi skripti hazırlayan hacker, ölümünden sonraki bir tarihte o skripti kullanan tüm web sitelerinin kendi resmini yayınlamasını sağlayabilir.

Bilişim suçunu işlemek için kullanılan araç ise sisteme müdahale edebilen, verilerin girdisini ve çıktısına zarar verebilen her şey olabilir. Bilgisayar olma zorunluluğu yoktur. Bunlar örneğin zararlı yazılım bulunduran usb bellek, kablosuna keylogger donanımı eklenmiş klavye, akıllı telefonlar olabilir.

Bu suçun mağduru ise herkes olabilir. Fail ile bir yakınlığı veya ilişkisi olma zorunluluğu yoktur. Hatta aynı mekânda, aynı ülkede olmalarına dahi gerek yoktur. Hatta aynı dönemde dahi yaşamış olmaları bile gerekmez. Ancak mağdur olabilmenin tek şartı teknolojinin ve bilişim sistemlerinin hayatında yer almasıdır. Bu sebeple yeni doğan bir bebek bile, hastane veri tabanına yapılacak bir müdahale ile farklı anne babaya teslim edilebileceğinden ya da olmadığı bir hastalığın teşhisi konmuş gibi sistemde yer alabileceğinden, bu suçun mağduru olabilir.

Bilişim suçu nelerdir sorusuna yanıt ararken, neler bilişim suçu değildir sorusunu sormak da sınırların çizilmesinde yardımcı olacaktır. Bu konuda Emniyet Genel Müdürlüğü Asayiş Daire Başkanlığı'nın internet sitesinde 'Bilişim Yoluyla İşlenen Asayiş Suçları'nın yer aldığı bir sayfa bulunmaktadır.[21] Bu sayfada yer alan içerik şu şekildedir:

İntihara yönlendirme (TCK madde 84)

Cinsel taciz; (TCK madde 105) Cinsel amaçlı taciz internet veya görüntülü iletişim araçları ile yapıldığında şüpheliler genelde yakalanamayacaklarını zannetmekteler.

Tehdit; (TCK madde 106) Yüz yüze, mektup ya da telefonla yapılan tehditler günümüzde yakalanması ya da ispatlanması daha zor olur düşüncesiyle sosyal ağlar ve elektronik posta ile yapılmaktadır.

Şantaj; (TCK madde 107) Özellikle internet üzerinden temin edilen uygunsuz görüntülerin, yine internet üzerinden yayınlanacağından bahisle şantaj olayları sıkça meydana gelmektedir.

[21] http://www.asayis.pol.tr/Sayfalar/bilisim_suclari.aspx (Erişim tarihi: 17.01.2015)

Hakaret; (TCK madde 125/2) İnsanlar yüz yüze gelmelerinin zor olduğu ortamlarda daha rahat hakaret ediyorlar.

Fuhşa teşvik ya da aracılık; (TCK madde 227) Web siteleri üzerinden para karşılığı fuhşa teşvik ve aracılık yaygınlaşmakta ve kolaylaşmaktadır.

Müstehcenlik; (TCK madde 226) Çocuk pornografisi materyali üretme ve yayma internet teknolojisi ile daha kolay işlenebilen ve uluslararası bir suç haline gelmiştir.

Bu internet sayfasından da anlaşılacağı ve Birleşik Devletler Ceza Usul Komisyonu (U.S. Sentencing Commission) bünyesinde oluşturulan 'Bilişim Suçları Çalışma Grubu'nun tanımında da geçtiği gibi klasik yöntemlerle işlenen suçların aynı zamanda bilgisayar kullanılarak işlenmesi durumunda bu suçların salt bu sebeple bilişim suçu sayılmaması gerekmektedir. Eylemin işlenebilirliği açısından yeni teknolojinin vazgeçilmez olması gerekir.

Yukarıda bilişim suçu olup olmadığı konusunda soru işaretleri bulunan örneklerimize geri dönersek, "alacağını tahsil etmek için muhatabına e-posta atarak borcunu ödemezse çocuklarını öldüreceğinden bahisle tehdit etmek bilişim suçu mudur?" sorusu için failin teknik bilgisi konusunda bir fikir oluşmamaktadır. Eylemdeki verilere müdahale e-posta servisi sağlayıcı şirketin kullanıcıya sunmuş olduğuyla sınırlıdır. Aynı zamanda Türkiye'deki mobil aboneler dâhil internet kullanıcı sayısının 40 milyonun üzerinde olduğunu düşünürsek, e-posta atmak herkesin gerçekleştirebileceği bir işlem olduğu için yüksek bilgi ve yetenek gerektirdiği söylenemez. Kullanılan araç, büyük ihtimal bilgisayar veya akıllı telefon gibi bir cihazdır. Yani bilişim suçu için elverişli bir cihazdır. Mağdur ise teknolojiyi kullandığı için bu suça muhatap kalarak mağdur olmaktadır. Ayrıca son kriter olan yeni teknolojinin vazgeçilmezliğinden bahsetmek ise mümkün değildir. Bu açıklamalardan sonra bu eylemin bilişim suçu olduğunu söylemek doğru olmaz.

Diğer örnek ise "Sahibinden.com isimli internet sitesi üzerinden araba almak isteyen kişinin, tanımadığı kişiye önden kapora göndererek, daha sonrasında hiçbir şekilde ulaşamayarak dolandırılması, bilişim suçu mudur?" Failin kullanıcı sayısı milyonlarla ifade edilen bir sitede ilan verebiliyor olması onun bilgisinin üst düzeyde olduğunu göstermez. Eylem ise verilerin işlenmesine ve iletilmesine bir müdahale niteliği

taşımamaktadır. Kullanılan araç internete erişim sağlayabilen bir araçtır. Bu eylem internet olmadan da gazeteye ilan vererek, emlakçılar kullanılarak da gerçekleştirebildiğinden yeni teknoloji olmazsa olmaz değildir.

Son örnek ise; "Facebook isimli sosyal medya sitesinden eski eşinin müstehcen fotoğraflarını herkesin görebileceği şekilde yayınlayarak eski eşini etiketleyen adamın gerçekleştirdiği fiil bilişim suçu mudur?" Failin ileri düzey bilgisayar bilgisine sahip olması gerekmemektedir. Eylemde aynı şekilde verilerin iletimine veya işlenmesine müdahale değildir. Kullanılan araç facebook internet sitesine bağlanabilen bir araç olduğu için teknolojiktir. Aynı zamanda bu suçun işlenebilmesi için yeni teknoloji şarttır. Ancak yeni teknolojinin gerekliliği, ileri düzey bilgi birikimi gerektirmediğinden bilişim suçunu oluşturmamaktadır.

Kısaca bilişim suçunun en önemli faktörü teknolojidir. Fail ve mağdurun en önemli ortak noktası teknolojinin hayatlarında yer almasıdır. Bir cinayet olayı için katil ve maktul aynı mekânda olması gerekirken, bilişim suçu için teknoloji olmazsa olmazdır.

Tüm bu tanımlardan ve örneklerden yola çıkıldığında bilişim suçu için; 'üst düzey teknolojik bilgi kullanılarak; bir sisteme ait verilerin işlenmesine iletişimine müdahale edilmek suretiyle kişi veya kurumların hak kaybına yol açan eylemlerdir.' tanımı kullanılabilir.

4.4. Bilişim Suçlarının Tarihsel Gelişimi

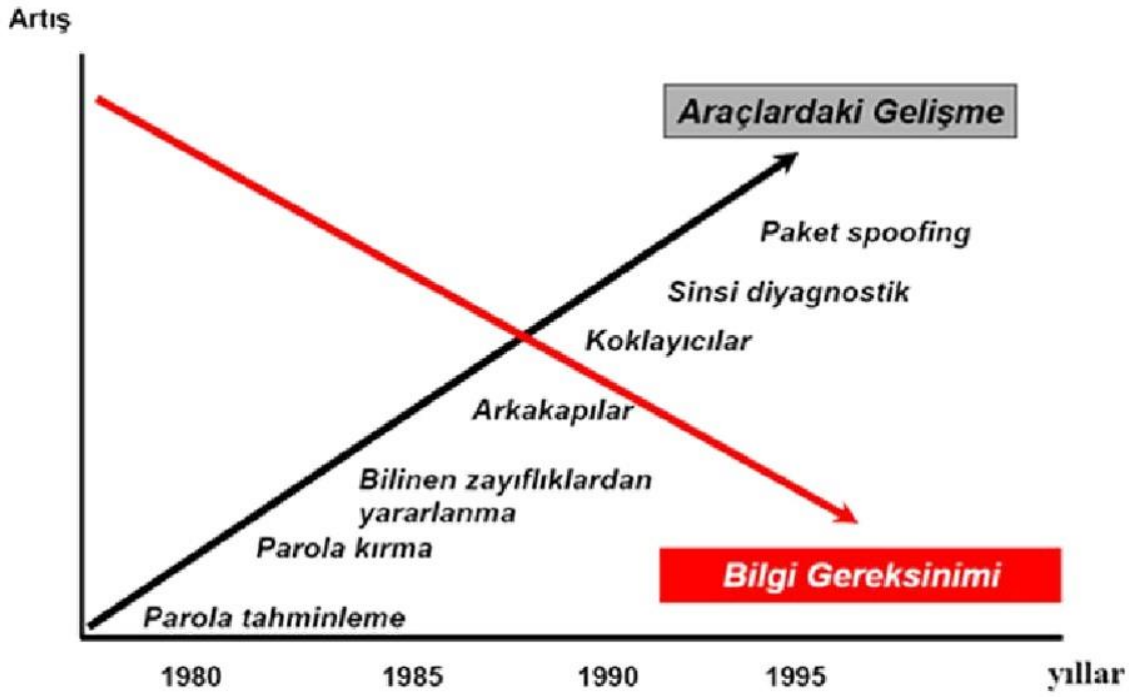
Bilişim suçlarının her geçen gün yeni işlenme şekillerinin ortaya çıkması gerek kamu hukuku gerekse özel hukuk açısından birçok sorunu da beraberinde getirmiştir. Dülger'e göre (2004: 220), özellikle internetin yaygın olarak kullanılmaya başlaması, ceza hukuku açısından düzenleme yapılmasını gerektirmiştir. Gelişen teknoloji, bilişim ürünlerine yönelik talebin artmasına ve gündelik yaşamdaki birçok eylemin dijital araçlarla yapılmasına olanak sağlamıştır.

Geleneksel masaüstü bilgisayarlara ek olarak mobil cihazlarda (akıllı cep telefonları, tablet bilgisayarlar vs.) da internet erişiminin mümkün kılınması sanal ortamlara bağlanmanın göreceli maliyetini azaltmış, ortama bağlantı kuran insan sayısı ve

ortalama bağlı kalma süresini arttırmıştır. Teknolojide yaşanan bu olumlu gelişmeler kötü niyetli insanlar için de yeni fırsatlar doğurmuştur.

Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır (Kurt, 2005: 157). Bunun yanı sıra Dülger (2004: 220) de ABD'de bazı gençlerin uzun mesafeli telefon konuşmalarını yapmak için sistemde yer alan boşluklardan yararlanarak bedava telefon konuşmaları yapmalarını bilişim suçlarının başlangıcı olduğunu belirtmektedir.

1990'ların başında internetin bireysel kullanıma açılması ve bireylerin kendi bilgisayarlarına sahip olmaları nedeniyle bilişim suçlarında bir artış olmuştur. Günümüzde terör örgütleri, propagandalarını internet üzerinden yapmakta ve eleman toplama faaliyetlerini yine internet üzerinden gerçekleştirebilmektedir. Aynı şekilde organize suç örgütleri gelirlerini arttırmak amacıyla internet üzerinde kredi kartı dolandırıcılığını suçunu işlemektedir.



Şekil 4.1. Bilişim Suçlarındaki Yıllara Göre Bilgi Gereksinimi[22]

[22] http://www.ekizer.net/bilisimsuclari-sibersuclar/ (Erişim tarihi: 03.02.2015)

Şekil 4.1'de Bilişim suçları işlenirken gereken bilginin yıllar geçtikçe azaldığını göstermektedir. Bilişim suçu işlemedeki araçların gelişmesi, bilişim suçu meraklılarının işini gittikçe kolaylaştırmaktadır. Araçların gelişmesi ve yaygınlaşması bilişim suçlarının da niceliksel ve niteliksel olarak artmasına sebep olmuştur. Bunun bir diğer sonucu da bu fiili işlemeyi haiz olan kişilerin teknik seviyelerindeki düşüşle birlikte yaşlarında da düşüş görülmektedir. Hatta kimi zaman çocuk olarak nitelendirebilecek olan bu kişiler, işlediği fiilin suç olduğunun farkında bile olmadan bu fiilleri gerçekleştirmektedir.

Bilişim yolu ile işlenen suçlarının her geçen gün artması ve bu yolla işlenen yeni suç türlerinin ortaya çıkması suçların soruşturulması ve aydınlatılmasında bilişim teknolojisinin kullanılmasının önemini her geçen gün artırmaktadır.

Ceza kanunlarının mülkiliği ilkesinin genel ilke olması, evrensellik ilkesinin ise çoğu ülkede mülkilik ilkesine göre tali ve tamamlayıcı nitelik göstermesinden dolayı bilişim suçlarının soruşturma ve kovuşturulması için uluslararası işbirliğini sağlayacak düzenlemeler hayati önem taşımaktadır (Topaloğlu, 1997: 19). Bilişim suçlarının gelişimine ilişkin olarak yapılacak olan temellendirme de "internet ile sunulan hizmetin ulusal sınırları aşarak herhangi bir kitle haberleşme aracına kıyasla daha fazla etki yapması" bilişim suçlarının kapsamını bir hayli genişletmiştir (Gercke, 2009). Şüphesiz Başlar'ın da belirttiği gibi, internet uluslararası hukukun kaynakları ve aktörleri üzerinde oldukça etkili olmuştur.

1981 yılında AET (Avrupa Ekonomik Topluluğu şimdiki adı ile Avrupa Birliği-AB) tarafından düzenlenen "Bilgisayarlaşan Toplumda İhlaller" adlı toplantıda belirlenen kavramlar, günümüzde de geçerliliğini ilk günkü öneminde korumaktadır (Akıncı ve diğerleri, 2004: 171). 1985 yılında Avrupa Topluluğu Suç Problemleri Komitesi, bünyesinde, bilişim suçları alanında çalışmalar yapması ve üye devletlere tavsiye bulunması amacıyla bir alt komisyon oluşturulmuş (Yazıcıoğlu, 1997: 131, Akıncı vd., 2004: 171), yine aynı yıl içerisinde Milano'da 7'incisi düzenlenen Birleşmiş Milletler (BM) Toplantısında bilgisayar suçlarının sonuçları tartışılmıştır (Yazıcıoğlu, 1997: 19).

1988 yılında, topluluk bünyesinde bilişim suçları ile ilgili olarak bir toplantı düzenlenmiş ve bu toplantıda komisyon tarafından yapılan 3 yıllık bir çalışmaya ilişkin

üye devletlere tavsiye kararlarında bulunmuştur (Helvacıoğlu, 2004: 277). Topluluğun 1989 yılında yapmış olduğu ve "Bilgisayarla İlgili Suçlar Üzerine Uzman Raporu" adlı bildiride, toplantıda alınan kararlar özetle bilgisayar sahtekârlığı ve bilgisayar dolandırıcılığını da içine alan elektronik suçlarla mücadele için etkili yasal önlemler alınmasını önermektedir (Gercke, 2009).

1990 yılında Küba'da yapılan BM 8'inci Toplantısında bilişim suçlarının hızlı bir şekilde artışı, bu suçların aydınlatılmasındaki zorlukları, bu tür suçların işlenmesinin klasik suçlara nazaran kolay olması ve ekonomik olarak ele alınan zararları da göz önüne alan birtakım kararlar üye devletlere sunulmuştur (Yazıcıoğlu, 1997: 131, Akıncı vd., 2004: 171). Kongrede alınan kararları şu şekilde özetlemek mümkündür (Chik, 2010);

-İç hukukta yer alan düzenlemelerin ve prosedürlerin güncellenmesi,

-Bilgisayar güvenliği ve suç önleme tedbirlerinin geliştirilmesi,

-Bilgisayar ile ilgili suçların önlenmesinin önemi ve bilgisayarla ilgili suçlardan doğabilecek problemlere karşı; halkın, yargıçların ve kanun uygulayıcılarının duyarlı hale getirilmesi,

-Bilgisayar ile ilgili suçlara ilişkin olarak suçun soruşturma ve kovuşturma aşamasında yer alacak ve suçun önlenmesinde sorumlu bulunan kolluk kuvvetlerine, yargıçlara ve savcılara konu ile ilgili eğitim verilmesi,

-Bilgisayar suçu mağdurlarına ilişkin politikaların benimsenmesi,

-Bilgisayar kullanımına ilişkin etik ilkelerin hazırlanması ve bu ilkelere bilgisayar eğitimlerinde yer verilmesidir.

Ancak bilişim suçları konusunda şu ana kadar yapılan en etkin hukuki düzenlemenin, Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suçlar Sözleşmesi olduğu söylenebilir. Hazırlanan sözleşmenin hedefi "ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi" ve uluslararası işbirliğinin geliştirilmesidir. Türkiye, Avrupa Konseyi Siber Suçlar Sözleşmesine 10 Kasım 2010 tarihinde imza koyarak taraf

olduğu hâlde, Sözleşmeyi iç hukukun parçası hâline getirecek işlemleri tamamlayıp, Sözleşmeyi iç hukuka aktaramamıştır. 22 Nisan 2014 tarihinde mecliste yürürlüğe girmiştir, ancak sözleşmenin iç hukuka entegrasyonunda ve uygulanmasında sıkıntılar devam etmektedir.Bilişim suçlarının tarihsel gelişimine baktığımızda yaklaşık 40 yıllık süre içerisinde bu duruma gelinmiştir. Bilişim suçlarının bu kadar önemli olarak kabul edilmesinin bir diğer sebebi geçmişinde meydana getirdiği tehlikelerdir.

4.5. Bilişim Suçlarının Hukuki Boyutu

4.5.1. Ülkemizde bilişim suçlarına yönelik hukuki düzenlemeler

İnternet, her gün büyümeye ve gelişmeye devam etmektedir. Fikir ve ifade özgürlüğünün internet sayesinde hiç olmadığı kadar gelişti. Bu yeni özgürlük alanı, bir yandan da dev bilgi deposu olarak gelişimini sürdürmektedir. Öte yandan internetin bu nitelikleri suiistimal edilerek suç da işlenmektedir. Ancak bu sadece internete özel bir durum değildir. Suç ve suçlu hayatın her alanında vardır. Bilişim suçlarında; kötü olan, zararlı olan internet değildir, interneti suç işlemek için kullanan suçlunun kendisidir.

Küreselleşme, son yıllarda üzerinde en çok tartışılan, çok farklı anlam ve değerler yüklenen, çok farklı tanımlamalara ve nitelemelere konu olan kavramların başında yer almaktadır. Kısaca, "dünyanın tek bir mekân olarak algılanabilecek ölçüde sıkışıp küçülmesi anlamına gelen bir süreci" (Tutar, 2002: 2) ifadesiyle tanımlanan küreselleşme, ekonomik, siyasal, sosyal ve kültürel değerlerin ve bu değerler çerçevesinde oluşmuş birikimlerin ulusal sınırlar dışına taşarak dünya geneline yayılması şeklinde değerlendirilmektedir. Bu gelişmeler sonucu dünya küresel köy olmaya daha da yaklaşmıştır. Özellikle internet medyasının getirdiği özgür ve geniş alan, sosyal medyanın en büyük paylaşım alanı olmasını sağlamıştır.

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi sonucunda "internet" denilen kavram da ortaya çıkmıştır. Faydalarının yanı sıra internet; art niyetli kişilere ulaşılması kolay, izlerinin diğer suçlara göre daha zor bulunacağı, sanal bir suç işleme ortamı sunmuştur (UNESCO, 2004).

Siber suçlar yaygın olarak; sahte internet siteleri (phishing[23], pharming[24] amaçlı) oluşturma, kişilerin şifreleri ve kullanıcı bilgileri ele geçirme, web sitelerine ve sunucularına yönelik saldırılar düzenleme (defacement-bozma), virüs taşıyan e-postalar (spam mail) yollayarak elektronik saldırılar yapma şeklinde gerçekleştirilir. Mağdurun bilgisi ve rızası dışında ele geçirilen şifre, kullanıcı adı, resim, görüntü gibi bilgi ve dokümanlar şahsa karşı; karalama, şantaj gibi suçları işlemek üzere kullanılır.

Bilişim alanında suçların en önemli özelliği suçlu ile mağdur arasında mekânsal mesafenin bulunmasıdır (Öztürk, 2007: 16). Ayrıca, bilişim teknolojisinin işleyiş tarzı sebebiyle, suç çoğu zaman birçok ülkeyi ilgilendirebilmektedir (Berber ve diğerleri, 2004: 151). Gerçekten, bilişim alanında suçların temel özelliği, sınır tanımamalarıdır. Artık kaçakçılık, insan ticareti, organize suçlar gibi sınır aşan suçların başında gelmektedir. Siber suçları tespit etme ihtimali geleneksel suçlara göre daha düşüktür (Kara vd., 2014: 74). Siber suçu ortaya çıkartmaya yarayacak delillerin türü ve formatı, bir de bunları elde etme yöntemleri geleneksel suçlara nazaran farklıdır (Kara vd., 2015: 154). Delillerin işlenmesi ve bunların mahkemeler tarafından kabule hazırlanması gerekmektedir.

İfade edilen suçlara karşı çeşitli güvenlik yaklaşımları, yöntemleri ve teknikleri geliştirilmiştir. Teknolojinin hızla gelişmesi ile güvenlik tabanlı unsurlar, siber suçlar karşısında uygulamada yaşanan sıkıntılar ve mevcut hukuki düzenlemelerin yeterliliği ise tartışma konusu oluşturmaktadır (Kara, 2015: 2).

4.5.2. Türk Ceza Kanununda bilişim suçları

Bilişim suçları 5237 sayılı yeni TCK'da, Bilişim Alanında Suçlar ve Özel Hayatın Gizli Alanına Karşı Suçlar bölümlerinde ele alınmıştır. Bu bölümlerde düzenlenen suçlara konu olan fiiller özellikle bilişim sistemleriyle işlenebilir ve genellikle günümüzde bilişim sistemleri dışında işlenebilme olanakları çok kısıtlıdır. Dolayısıyla klasik

[23]Phishing (password harvesed fishing): başka bir internet sitesini taklit ederek, o siteye kullanıcı tarafından girilen parolaları ve diğer bilgileri elde etmek.

[24]Pharming: kullanıcıya ait parolaları ve diğer bilgileri elde etmek için hedefin DNS ayarları değiştirilerek, ulaşmak istediğinden farklı bir siteye yönlendirmek.

suçların yanında yalnızca bilişim suçu olarak nitelendirilebilecek suç tipleri de ortaya konulmuştur. Sayılan suçlarla beraber, TCK'nın farklı bölümlerinde bilişim sistemleriyle işlenebilmesi mümkün olan suç tiplerine yer verilmiştir. Ancak yeni suç işleme modellerinin ve gelişen teknolojinin sıkça görülmesi nedeniyle bu tür suçlar arasında net ve kesin bir ayrım yoktur.

Bilişim suçları ile ilişkili olan mevzuat; bilişim suçları, bilişim vasıtalı suçlar, fikir ve sanat eserleri kanunu, kaçakçılık ile mücadele kanunu ve ceza muhakemesi kanunu olmak üzere beş ana başlık altında toplanmış ve ilgili başlıklar altında aşağıdaki gibi listelenmiştir.

Kanunda ele alınan bilişim alanındaki suçlar şunlardır:

- TCK (Türk Ceza Kanunu) (Bilişim Suçları)
  - MADDE 243. Yetkisiz erişim –Sisteme girme
  - MADDE 244. Hacking, verileri engelleme, bozma, değiştirme, yok etme
  - MADDE 245. Kredi kartı ve bankaya karşı işlenen suçlar.
  - MADDE 246. Tüzel kişiler hakkındaki tedbirler

- TCK (Bilişim Vasıtalı Suçlar)
  - MADDE 124. Haberleşmenin engellenmesi
  - MADDE 125. Hakaret
  - MADDE 132. Haberleşmenin gizliliğini ihlal.
  - MADDE 133. Kişiler arası konuşmaların dinlenmesi ve kayda alınması.
  - MADDE 135. Kişisel verilerin kaydedilmesi.
  - MADDE 136. Verileri hukuka aykırı olarak verme veya ele geçirme.
  - MADDE 138. Verileri hukuka aykırı olarak verme veya ele geçirme.

- MADDE 142. Nitelikli hırsızlık.
- MADDE 158. Nitelikli dolandırıcılık.
- MADDE 226. Müstehcenlik.

❖ Fikir ve Sanat Eserleri Kanunu

- MADDE 71. Manevi haklara tecavüz.
- MADDE 72. Mali haklara tecavüz.
- MADDE 73. Diğer suçlar.

❖ Ceza Muhakemesi Kanunu

- MADDE 134. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma

4.5.3. Bilişim alanında suçlar açısından Türk Ceza Kanununun 243, 244 ve 245. maddelerinin değerlendirilmesi

TCK gerekçesinin bilişim sistemi tanımı aslında bilişim sisteminden çok bilgisayar tarifine yakındır. Kısaca bilişim suçu olarak isimlendirilen eylemler "Bilgisayar, cep telefonu, taşınabilir hard-diskler, müzik çalar, hafıza kartı, sim kart, modem, encoder, tablet gibi manyetik, elektronik, optik, dijital veri depolayabilen, işleyebilen, iletebilen her türlü araçlarla bunları veri iletişimi için birbirine bağlayan soyut ya da somut ağlar üzerinde işlenebilmektedir." TCK'nın bu suçları 243, 244 ve 245. maddeleriyle düzenlenmiştir (Kara, 2015: 151).

4.5.3.1. Bilişim sistemine girme

Türk Ceza Kanunu madde 243'teki hükümde;

Madde 243- (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. ibaresi yer almaktadır.

Birinci fıkrada korunan hukuksal değer Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde "Her taraf, iç hukukuna uygun olarak, bir bilişim sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişimi suç haline getirmek için gerekli görülen yasal tedbirleri almayı kabul eder." şeklinde de belirtildiği üzere bilişim sistemlerinin güvenliğidir.

Ancak burada dikkat çeken fark Türk Ceza Kanunu'nda "… giren ve orada kalmaya devam eden kimseye…" şeklindeyken; Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde ise "kasten ve haksız olarak erişimi" suç kılmaktadır. Yani bizim kanunumuzda 'girme' eyleminin tek başına bu suçu oluşturmadığı ancak ve ancak 'orada kalmaya devam etme' eylemiyle suçun sübuta ereceği anlaşılmaktadır. Bu açıdan madde "suç = yetkisiz erişim + kalmaya devam etme" şeklinde formüle edilebilir, bunun anlamı da anlık yapılan yetkisiz erişimin suç sayılmaması gerektiğidir (Karagülmez, 2005: 167).

Maddenin ikinci ve üçüncü fıkrasında nitelikli halleri tanımlanmış, bedeli karşılığında yararlanılan sistemlere karşı işlenmesi halinde örneğin, bir internet sitesinin belirli bir ücret karşılığında müşterilerine sunmuş olduğu dergi, gazete vs. abonelik hizmetine yetkisiz erişim sağlayarak, sunuluna hizmetten yararlanmak eylemi bu suçun nitelikli halini oluşturacaktır. Ancak dikkat edilen nokta bu hal suçun artırıcı değil hafifletici

Aynı şekilde bu yapılan yetkisiz erişimden dolayı verilerin değişmesi veya silinmesi söz konusu olursa da bu suçun nitelikli hali olacak ve cezası artacaktır.

Dikkat edileceği üzere buradaki korunan değer sisteme sağlanan erişimle sınırlıdır. Bilişim sistemine girişlerin cezalandırılması için verilerin ele geçirilmesi şartı kaldırılmakta ve veri ele geçirilsin ya da geçirilmesin bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınmaya devam edilmesi yani bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmektedir (Dülger, 2013: 319). Zaten verilerin ele geçirilmesine ilişkin Türk Ceza Kanunu'nun 135. maddesinde 'Kişisel verilerin kaydedilmesi' ve 136. maddesinde 'Verileri hukuka aykırı olarak verme veya ele geçirme' başlıkları altında daha ayrıntılı şekilde düzenlenmiştir.

Bu maddede suç olarak belirtilen eylemin diğer bilişim suçlarından en büyük farkı, kendi başına en sık karşılaşılan bilişim suçu olduğu gibi, diğer bilişim suçları için de araç niteliği taşımaktadır. "bu eylem öğretide geleneksel suçlardaki konut dokunulmazlığının ihlali suçuna benzetilmektedir. Bu suç yalnızca hedeflenerek gerçekleştirilebileceği gibi, bilişimle ilgili olsun ya da olmasın başka bir suç işlemek için 'araç suç' olarak da işlenebilir. Bu yönüyle hukuka aykırı erişimin konut dokunulmazlığı suçuna daha fazla benzerlik gösterdiği ifade edilmektedir." (Erdoğan, 2012'den aktaran Dülger, 2013: 321).

Bu maddede dikkat çeken eksiklik ise; bu eylemin işlenmesini caydırma konusundaki yetersizliği denilebilir. Bir bilişim sistemine girme fiili suç olarak tanımlanmışken, bu fiili kolaylaştırıcı, hazırlayıcı fiiller suç olarak tanımlanmamıştır. Bu suçun işlenmesinde sıklıkla virüs, solucan gibi kötücül yazılımlar aracı kullanılmakta ve bu yazılımların oluşturulmasının amacı sadece zarar vermektir. Ayrıca bu yazılımların oluşturulması çok daha fazla teknik beceri istediğinden bilişim sistemine girme suçu failleri genelde başka biri tarafından oluşturulmuş olan ve piyasaya reklam vs. gibi sebeplerle sunulmuş olan kötücül yazılımları kullanmaktadır. Ancak kanunun bu maddesinde veya herhangi bir maddesinde bu amacı belli olan yazılımların oluşturulmasını veya paylaşılmasını cezalandıran bir hüküm bulunmamaktadır. Ancak Alman Ceza Kanunu'nda 202c paragrafında yer alan 'Veri Casusluğunun ve Verilerin İletilirken Ele Geçirilmesinin Hazırlığı' başlığı altında bu tür eylemler düzenlenmektedir. Bu hükümde: "… belirtilen suçların işlenmesini hazırlamak üzere, 1. verilere giriş yapmayı sağlayan şifre ve sair güvenlik kodlarını veya 2. bu tür fiilleri işlemeyi amaçlayan bilgisayar programlarını, üretir, kendisine veya bir başkasına sağlar,

satar, bir başkasına verir, yayar veya sair bir şekilde ulaşılabilmesini sağlarsa bir yıla kadar hapis cezası veya adli para cezasına ile cezalandırılır." (Dülger, 2013: 322).

4.5.3.2. Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Türk Ceza Kanunu'nun 244. madde hükmünde:

Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

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

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

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

Maddenin ilk iki fıkrasında hangi eylemlerin bu suçu oluşturacağı belirtilmiştir. İlk fıkrada sistemi korumayı hedeflerken, ikinci fıkrada korunan değer sistemin içindeki verilerdir. Bu açıdan bakıldığında ilk fıkrada soyut yazılım ve veri gibi değerlerin yanında, bunu muhafaza eden sistemlerin somut yani donanımsal özelliklerinin de korunduğunu görmekteyiz.

Dülger bu kanun maddesiyle korunan değerin önemini şöyle açıklamıştır:

> "Günümüzün modern yaşam düzeninin ana konularını oluşturan ekonomi, sağlık, eğitim, bilimsel araştırmalar, idare, savunma gibi pek çok yaşamsal alanda bilişim sistemleri vazgeçilmez alanlar olmuşlar, bu alanların pek çok yerinde geri dönülmez şekilde insanların yerini almışlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin geçici süreyle de olsa çalışmaması çok büyük zararlara neden olabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsleri, kurtçuklar, Truva atları gibi zarar verici

> yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana sokan faillerin dahi öngördüğünden daha fazla zarara yol açabilmektedir. Benzer bir şekilde web sitelerini çökertmek için DDoS saldırıları gibi eylemler pek çok kamu hizmetinin alınmasını önleyebilmekte ya da saldırıya uğrayan siteyi kullanan şirketin ticaret yapmasını engelleyebilmektedir. Yasa koyucu da bu büyük tehlikeyi öngörerek sisteme ve/veya verilere zarar verme eylemlerini bu maddeyle suç haline getirmiştir." (Dülger, 2013: 386).

Bu suçun gerçekleşmesini sağlayan eylemler ele alındığında, birinci fıkrada "… engelleyen veya bozan …" ibaresi geçmektedir. Bilişim sisteminin işleyişini engellemek ile kast edilen sistemin faaliyetlerini geçici veya sürekli olarak durdurmasına sebep olmaktır.

Engel olma fiili bilişim sisteminin geneline yönelik olabileceği gibi, onun çalışmasına destek olan, katkı sağlayan başka bir unsura da yönelik olabilir. Bu diğer unsura yapılan müdahalenin suça konu olan bilişim sisteminin işleyişini kısmen veya tamamen engellemiş olması bu suçun oluşması için yeterlidir (Karagülmez, 2005: 188).

Bozma eylemi ise, aslında bilişim sisteminin kendisinin veya alt unsurlarından birinin yapılan yetkisiz müdahale sonucu zarar görmesi ve bunun neticesinde de sistemin genelinde sağlıksız çalışma meydana gelmesidir. Aslında nihai olarak bu eylem de bir engellemedir. Karagülmez (2005: 189)'in de dediği gibi Türk Ceza Kanunu'nun 244. maddesinde 'bozan' ibaresi kullanılmadan da, sadece 'engelleme' ibaresi ile yetinilebilirdi. Çünkü sistemin bir kısmının veya tamamının bozulması aynı zamanda sistemin bir kısmının veya tamamının işleyişini engelleyeceğine göre bu sonuca varılması mantıklıdır.

Suçu işleniş amaçları ele alındığında, ilk fıkranın ikinci fıkradan en büyük farkı, veri kavramından ziyade sistem kavramının ön planda tutulmasıdır. İçindeki veriyi göz ardı ederek sistemlerin işlemesinin engellenmesinde amaç ne olabilir? Aslında bu kanun maddesinde genellikle doğrudan maddi menfaat temini için ileride daha detaylıca ele alınacak olan ikinci fıkranın sübuta ermesi daha olasıdır.

Birinci fıkradaki suçun bilişim sisteminin işleyişinin engellenmesi veya bozması fiilinin doğrudan maddi menfaat temini odaklı olmadığından dolayı, gerçekleştirilmesinin en büyük sebebinin 'prestij' ya da 'sesini duyurmak' olduğunu söyleyebiliriz. İnternet sitelerinin de bir bilişim sistemi olduğunu düşünürsek, sırf internet site hacklemelerinin duyurulduğu internet sitelerinin varlığı, bu suçun gerçekten de 'prestij' maksatlı yapıldığının göstergelerinden biridir. Dünya çapında veya ulusal çapta önemli şirketlerin internet siteleri ya da devlete ait kurumların internet siteleri hacklenerek, siyasi ya da ideolojik mesajların verilmesi olayı yani 'sesini duyurma' maksatlı bu suçun işlenmesi de sıklıkla meydana gelmektedir. Bu maksatla gerçekleştirilen bu olaya hack ve aktivizm kelimelerinin birleşiminden oluşan 'hacktivizm' denilmektedir.

Diğer sebepler ise kişinin kendini deniyor olması, eğlence maksatlı ve ticari kaygılarla yapılan hedef şirketin itibarına zarar vermek amaçlı saldırılardır.

Bu maddenin ikinci fıkrasında ise verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılma sisteme veri yerleştirilmesi ve verileri başka yere gönderilmesi suçları yer almaktadır. Burada korunan veriler ve verilerin güvenliğidir. Ancak bu kanun maddesinde kast edilen veri, sistemin işleyişine doğrudan etkisi olmayan veriler olduğu ilk fıkradaki eyleme göre daha az ceza gerektirmesinden anlaşılmaktadır. Benzer görüşte Erdoğan da (Dülger, 2013: 389) "… bir bilişim sisteminde yer alan her veri, sistemin işleyişini bozmayacağı ve engellemeyeceği için 1. fıkradaki suça nazaran daha az ceza ile cezalandırılmaktadır. Dolayısıyla bu suç tipiyle de verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmaktadır. …bir başka deyişle 2. fıkra ile sistemin içinde yer alan; ancak sistemin yapı taşı olmayan veriler korunmaktadır."

Maddenin 4. fıkrasında kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde ibaresi geçmektedir. Bu eylemin gerçekleşmesinde kasıt genellikle verilere ve bu sayede de verilerin sahibine zarar vermek olabileceği değerlendirilmektedir. Çünkü bu verilerin maddi değere sahip para veya ona eş değer olabilecek kredi, kontör vs. hakkında işlenmesi durumunda Türk Ceza Kanunu'nu 142/2-e bendinde geçen bilişim sistemine girmek suretiyle nitelikli hırsızlık suçunu oluşturacağı, aynı şekilde elde edilen verilerin kişisel veri niteliğinde olması durumunda ise kanunun 136. maddesindeki Verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı değerlendirilmektedir. Ancak Yargıtay Ceza

Genel Kurulu tarafından manyetik telefon kartlarının üzerindeki verilerin değiştirilerek herhangi bir ücret ödemeksizin ankesörlü telefonların kullanılmasını bu suç kapsamında değerlendirmesine yönelik 2007 yılındaki kararın gerekçesinde:

> "Sanığın telefon kulübelerinden topladığı kredisi bitmiş telefon kartlarına barkod ve manyetik bant yapıştırmak suretiyle kontör yükleyip bunları diğer sanık S.. T.. ile birlikte katılan Kurum' ait kulübelerde bulunan telefon cihazlarına sokup kullandıkları, bu yöntemle kısa süre içinde toplam 35210 kontörlük görüşme yapıldığı dosyadaki kanıtlardan anlaşılmaktadır…
>
> Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır. Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkot numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi vs.) bünyesinde topladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkod numaraları dahi bu sayede tespit edilmiştir. Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı takdirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30 kontör kredi yüklemesi yapmak suretiyle kullanıma hazır hale getirmekte, kullanım süresince yaptığı hesaplamaların sonucuna göre kalan kredi miktarını saptayıp manyetik karta işlemektedir. Başka ifadeyle

sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir.

Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişiklerle, sistemin verileri farkı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklemesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasası'nın 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğü giren 5237 sayılı Türk Ceza Yasası'nın 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır…" (Yargıtay Ceza Genel Kurulu, Kt. 19.06.2007; E.2007/6-136, k. 207/150'den aktaran Dülger, 2013: 414).

Bu karardan da anlaşılacağı üzere, suça konu müdahalenin sadece bilişim sistemine yönelik olma şartından ziyade, ona veri girişi yapan etkenlerdeki manipülenin de bilişim sistemine müdahale eylemi meydan gelecek ve bu sayede elde edilen menfaatin de bilişim sistemindeki verilerin değiştirilerek çıkar sağlama suçunu oluşturacaktır.

4.5.3.3. Banka veya kredi kartlarının kötüye kullanılması

Türk Ceza Kanunu'nu 245. maddesinde:

"(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.

(5) (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." ibaresi geçmektedir.

Bu maddeyle korunan hukuksal değer, hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarında korunan hukuksal değerler ile aynıdır. Çünkü bu suç işleniş biçimine göre bu fiillerin birini veya birkaçını kapsayabilmektedir. Düzenlenen hırsızlık ve dolandırıcılık suçlarıyla malvarlığı, güveni kötüye kullanma suçuyla kişilerin birbirine duyduğu kişisel güven sahtecilik suçuyla ise devlet tarafından bireylere yüklenilen hukuk alanında inandırıcılığı olan belgelere güven korunmak istenmektedir (Dülger, 2013: 427). Ama asıl korunan değer, failin suçu işlemedeki olası saiki da göz önüne alındığında malvarlığı olduğunu söylemek yanlış olmaz.

Bu suç işleniş bakımından banka kartı veya kredi kartına yönelik olması gerekmektedir. Banka kartı: kişiye bankadaki hesabıyla ATM türü vezne işlemi gören cihazlar üzerinden doğrudan bağlantı kurması için üzerindeki manyetik şeritte verilere sahip ve verilerin doğrulanması için de şifreye ihtiyaç duyan kartlardır. Günümüzde para çekme işleminin yanında, alışverişe de imkân sağlamaktadır.

-Kredi kartı: Banka tarafından müşterisine kısa süreliğine genellikle alışveriş için kredi imkânı sağlayan manyetik şeride ve günümüzde çiplere sahip

kartlardır. Borçlanma imkânı sağladığı için olası maddi zarar kapasitesi daha yüksek olup, fiziki alışverişlerde imza yerine pin, internet üzerinden alışverişlerde ise son kullanma tarihi, güvenlik kodunun yanı sıra 3D[25] güvenlik kullanılması yaygınlaşmıştır.

Bu suç tipi, bu kartların fiziksel olarak elde edilmesi, bu kartların kopyalanması ve internet üzerinden alışveriş için yeterli bilgilerin elde edilmesi suretiyle gerçekleşmektedir.

-Kartların fiziksel olarak elde edilmesi: Kanun maddesinde her ne suretle olursa olsun ibaresi geçtiğinden, bu eylemi geniş düşünmek gerekmektedir. Sadece hukuka aykırı olarak elde etme değil, kişinin rızası dâhilinde veya işi veya görevi gereği bu kartı elinde bulunduran üçüncü kişi de bu suçu işleyebilmektedir. Kişinin restoranda ödeme yapmak için kartını verdiği garsonun ya da bankalar tarafından üretilmiş olan kartı, sahibine ulaştırması için verilmiş kurye kartı elinde bulundurma açısından hukuki bir eylem içerisindedirler.

Diğer yandan ise, hukuka aykırı olarak elde etme diyebileceğimiz hırsızlık veya cebir veya tehdit kullanarak yağma ile gerçekleşmesi durumunda da bu kartın fiziksel olarak elde edilmesi mümkündür. Bir diğer yöntem ise ATM cihazlarına yerleştirilen kart yuvasında kartın sıkışmasını sağlayan düzenekler vasıtasıyla kartın fiziksel olarak elde edilmesidir.

-Kartların kopyalanması: Bu yönteme 'skimming' denilmektedir, bu yöntem ATM'lere yerleştirilen düzenek veya POS cihazlarını[26] kullanan kasiyerler veya işyeri sahipleri tarafından aynı zamanda 'skimming' yapabilen başka bir cihazdan geçirilmesi ile mümkün olmaktadır. Bu kopyalama cihazları kartlarda bulunan manyetik şeridi hafızasına almaktadır. Manyetik şeritte bulunan track data 1 ve track data 2 bilgileri sahte üretilen farklı bir karda kaydedilmektedir; ancak bu kartların kullanılabilmesi için kullanıcının karta ait şifresinin de ele

[25]3D güvenlik: internet üzerinden alışverişlerde, o işleme özel oluşturulan kodun müşteri tarafından teyidi ile sağlanan güvenlik (OTP - one time password).

[26]POS (Point of sale) cihazı: kredi ve banka kartlarının işlem yapabilmesi için bankayla iletişime geçen cihaz.

geçirilmiş olması gerekmektedir. Ülkemizde çipli kartların kopyalanmasına ilişkin bir olaya henüz rastlanılmamıştır.

-İnternet üzerinden alışveriş için gerekli bilgilerin elde edilmesi: Bu işlem için kredi kartının üzerinde yer alan kart numarası, son kullanma tarihi ve güvenlik kodu bilgileri yeterlidir. Bu bilgilerin temini ise fiziki kartın elde edilmesi, fiziki kartın fotoğraflanması ya da phishing dediğimiz yöntemle gerçeğinin aynısı gibi görünen taklit sitelere veya kontör, fatura ödeme vb. amaçlı görünen sitelere kişinin kart bilgilerini girmesi suretiyle elde edilmektedir. Bu tip suçlara karşı alışveriş siteleri ve bankalar tarafından kullanıcıya işleme özel onay kodu gönderilmesi olan 3D güvenlik ile tedbir alınsa da bunların da aşıldığı olaylara sıkça rastlanılmaktadır.

4.5.4. Topluma karşı suçlar - genel ahlaka karşı suçlar

Madde 226. Müstehcenlik

-Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

-Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

-Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,

-Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,

-Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

-Bu ürünlerin reklamını yapan, Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

Bu suç türünün günümüzde en çok sirayet ettiği alan internet olmuştur. Daha çok insana, daha anonim olarak bu tip içerikler sunulabilmektedir. Özellikle çocuğun kullanılması sonucu oluşan müstehcen içeriklere ilişkin, ulusal ve uluslararası çapta tedbirler alınmaktadır. Küresel çapta mücadeleler sürdürülmektedir. Birçok uluslararası şirket, kullanıcı mahremiyetini sadece bu suç tipi için bozmakta, ABD'de yer alan NCMEC (National Center for Missing and Exploited Children) koordinesinde ihbarlar ilgili ülke birimlerine iletilmektedir. Ülkemizde ise Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı irtibat noktası görevini yürütmektedir. Gelen ihbarları, gereği yapılmak üzere taşra birimlerine sevk etmektedir.

4.5.5. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunu'na göre, film, müzik CD'leri, yazılım programı vs. her türlü eseri tamamen veya kısmen kopyalama, çoğaltma; çoğaltılmış nüshalarını kiralama, ödünç verme, satma ve diğer yollarla dağıtma hakkı sahibine aittir. İzinsiz olarak bunları kullanmak, kopyalamak, dağıtmak ve satmak suçtur. Bunun yanı sıra, bir bilgisayar programının yetkisi olmayan kişilerce çoğaltılmasını önlemek amacıyla oluşturulmuş programları etkisiz hale getiren program veya teknik donanımları üretmek ve satmak da suçtur.

Kanundaki cezai yaptırımlar öngören maddelere kısaca baktığımızda,

Madde 71. Manevi haklara tecavüz

-Yazılımı kamuya sunma hakkı,

-Yazılım sahibinin adını belirtme hakkı,

-Değişiklik yapılmaması hakkı

Madde 72. Mali haklara tecavüz

-Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek,

Madde 73. Diğer suçlar

Şeklinde düzenlenerek bu hakları koruma altına almayı hedeflemiştir. Bu suçların işlenmesi yıllardan beri süre gelmektedir; ancak son yıllarda bu tip ihlallerin yapılması daha çok internet üzerinden gerçekleşmektedir. Özellikle peer-to-peer[27] paylaşım programları, film-dizi siteleri, e-kitap paylaşımı yapan siteler sıkça karşılaşılan aynı zamanda çok fazla da tercih edilen internet siteleri olarak yayın yapmaktadırlar.

4.5.6. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

2007 Mayıs ayında Resmi Gazetede yayınlanarak yürürlüğe giren ve internet üzerinden yapılan yayınları düzenleyen bu kanun ve üç yönetmeliği ile birlikte ülkemizde bilişim ve internet alanının hukuki yapısının düzenlenmesi yönünde büyük bir adım atılmıştır. 24 Ekim 2007 tarihinde yayınlanan ilk yönetmelikte sitelere yer sağlayıcılar ve erişim sağlayıcılara ait düzenlemeler yapılarak internet servis sağlayıcı şirketler olan TTNET, Superonline gibi şirketlerle, siteler için barınma imkânı sağlayan hosting şirketleri için düzenlemeler getirilmiştir

1 Kasım 2007 tarihinde Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan yer olarak tanımlanmış olan toplu kullanım sağlayıcılarına ilişkin düzenlemeler getirmiştir.

Son yönetmelikte ise, sitenin yayınladığı içeriklere ilişkin düzenlemelere yer verilmiş ve içerik sağlayıcıların içeriğinde suç barındıran içeriklerin kontrolü ve bunun sorumluların tespiti ve suçun soruşturulmasına ilişkin yenilikler getirilmiştir.

Ayrıca kanun bu internet sitelerinin yayınladıkları içeriklerle herhangi bir suça sebebiyet vermesi veya toplum ahlakı ve sağlığı açısından tehdit oluşturması durumunda ilgili siteye erişimin engellenmesini sağlamaktadır. İnternet sayfası üzerinden işlenebilecek olası suçların, daha sonra takip edilebilmesi ve kim tarafından nasıl gerçekleştirildiğinin bilinmesi amacıyla internet sayfalarına erişen tüm kullanıcılara ilişkin kayıtlarının tarih bilgisi ile tutulmasını ve saklanmasını

[27]Peer-to-peer: istemciler arasında veri paylaşmak için kullanılan bir ağ protokolüdür.

istenmektedir. Tüm erişimlerinin kayıtlarının en az 6 ay en fazla 2 yıl süreyle tutulması gerekmektedir.

Alaca'nın (2008: 78) da belirttiği gibi kanunun ilk defa düzenlediği konular;

1. İnternet ortamındaki yayınlardan kanunda katalog suçlar olarak nitelendirilen 8 suçla ilgili olarak erişim engelleme kararlarını ve

Madde 8 - (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

-İntihara yönlendirme (madde 84),

-Çocukların cinsel istismarı (madde 103, birinci fıkra),

-Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

-Sağlık için tehlikeli madde temini (madde 194),

-Müstehcenlik (madde 226),

-Fuhuş (madde 227),

-Kumar oynanması için yer ve imkân sağlama (madde 228), suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

2. Erişimin engellenmesi kararı ve yerine getirilmesi usulleri belirlenmiştir.

3. İnternet ortamında oynanan kumar konusunda bir özel düzenleme yapılmıştır.

4. Erişimin engelleme işlemlerine itirazın usulü belirlenmiştir.

5. İnternet ortamındaki yayınlara ilişkin olarak cevap ve düzeltme hakkı getirilmiş ve bunun usul ve esasları belirlenmiştir.

6. İnternet ortamındaki yayınların ilkeleri belirlenmiştir.

7. İnternet aktörleri tanımlanarak bu aktörlerin hak, sorumluluk ve yükümlülükleri belirlenmiştir.

8. Erişim ve yer sağlayıcıların faaliyet belgesi almalarına ilişkin usul ve esaslar belirlenmiştir.

9. İnternet aktörlerinin tutmaları gereken trafik bilgilerine ilişkin bir düzenleme gelmiştir.

10. İnternet toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları belirlenmiştir.

11. Ticari amaçla internet toplu kullanım sağlayıcıların izin belgeleri almalarının usulü, yükümlülük ve sorumlulukları ile denetleme usulü belirlenmiştir.

12. Ticari amaçla internet toplu kullanım sağlayıcıların sahibi veya sorumlu müdürün mülki idare amirliklerinin koordinesinde alacakları eğitim belirlenmiştir.

13. Türkiye'de internet filtreleme konusunda usul ve esaslar belirlenmektedir.

14. İnternet filtrelemesine ilişkin üretilen donanım ve yazılımın kriterleri belirlenmektedir.

15. Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen 8 suça ilişkin şikâyetlerin yapılabileceği bilgi ihbar merkezi kurulmuştur.

16. İnternet kurulunun mevzuat düzenlemesi yapılmıştır.

17. Bilişim ve internet alanında uluslararası koordinasyonda bulunacak görevli kuruluş belirlenmiştir.

18. İnternet ortamındaki yayınları izleme hususu düzenlenmiştir.

19. Ticari amaçla internet toplu kullanım sağlayıcılarda hangi tür oyunların oynanabileceği hangi tür oyunların oynanamayacağı düzenlenmektedir.

4.5.7. 5271 Sayılı Ceza Muhakemeleri Kanunu

Bilişim yolu ile işlenen suçlarda en etkin usul yöntemlerinden biri olan 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134 üncü maddesinde bir suç dolayısıyla yapılan soruşturmada delil elde etmek amacıyla şüphelinin kullandığı bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilebileceği belirtilerek, dijital verilerin maddi delil haline getirilebileceği düzenlenmiştir.

Madde 134 – (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının 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 hâline getirilmesine hâkim tarafından karar verilir.

Madde 134 – (1) inci maddesinde; bilgisayar, bilgisayar programları ile bilgisayar kütükleri iadelerinin kullanılması uygulama da ikilemlere sebep olmuş, cep telefonları ve veri depolayan diğer cihazların (CD, DVD, USB Bellek vb.) durumları farklı değerlendirilerek farklı uygulamalar getirilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesinin 'Saklanan bilgisayar verilerinin aranması ve bunlara el konulması' başlıklı 19 maddesinde bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan veriler ile bilgisayar verilerinin saklandığı cihazlar denilerek geniş bir kapsam sunmuş ve ikilem çıkmasını engellemiştir.

Belirtilen 'başka surette delil elde etme imkânının bulunmaması halinde' maddeden çıkartılması daha uygun olacaktır. Çünkü bu cümle dijital materyallerden elde edilen delilleri sanki son çareymiş gibi yansıtmaktadır. Oysaki bazı durumlarda, suç konusu delil elde edilmesi sadece dijital materyal olduğu durumlarla da mevcuttur. Ayrıca şüphelinin kullanmış olduğu materyaller kavramına değinilmiştir. Ancak kanunda üçüncü kişilerin (mağdur, maktul, şikâyetçinin) dijital materyalleri ile alakalı hiçbir düzenleme olmadığından gerekli düzenlemeler yapılarak konunun netliğe kavuşturulması gerekmektedir (Kara, 2014: 157).

Cumhuriyet Savcısının istemi üzerine şüphelinin kullanmış olduğu materyallerden kopya alma işlemi için alınan kararlarda arama saati sınırlandırıldığından olay yerinde şüpheli şahsa ait dijital materyallerin kopya alma işlemi, kopyası alınacak materyallerin adedine ve kapasitesine göre değişebilmekte ve belirtilen saat aralıklarında kopya alma işlemi mümkün olmayabilmektedir. Ayrıca kopya alma işlemi olay yerinde yapılması uygulamada aksaklıklara neden olmaktadır (Kara, 2014: 154).

Uzmanlar tarafından olay yerinde kopya alma işleminde kullanılan cihazlar için gerekli sistem alt yapısının mevcut olması gereklidir. Kopya alma işlemi Tableau TD1 (Disk Adli Kopyalama Cihazı) cihazı ile yapıldığından kullanılan TD1 cihazının elektrik adaptörünü UPS (kesintisiz güç kaynağına) bağlı cihazdan alınması yaşanabilecek elektrik kesintisi sonucu kopya alma işleminde oluşabilecek vb.). Bu bakımdan kopya alma işlemi el konulma işlemi sonucunda Adli Bilişim Laboratuvarlarında yapılması daha uygun olacaktır. Bu sebeple kanun maddesine kopya alma işleminin nerede ve nasıl yapılacağının açık bir şekilde tanımlanması yapılması gerekmektedir. Zorunlu durumlarda örneğin ticari bir şirketteki sunucunun kopyası alınması gibi bir durumda olay yerinde kopya alınabilir. Ancak rutin bir ev ya da işyeri aramasındaki dijital materyallerin kopyasının Adli Bilişim Laboratuvar ortamında alınması şeklinde kanuni düzenlemeye ihtiyaç duyulmaktadır (Kara, 2014: 157).

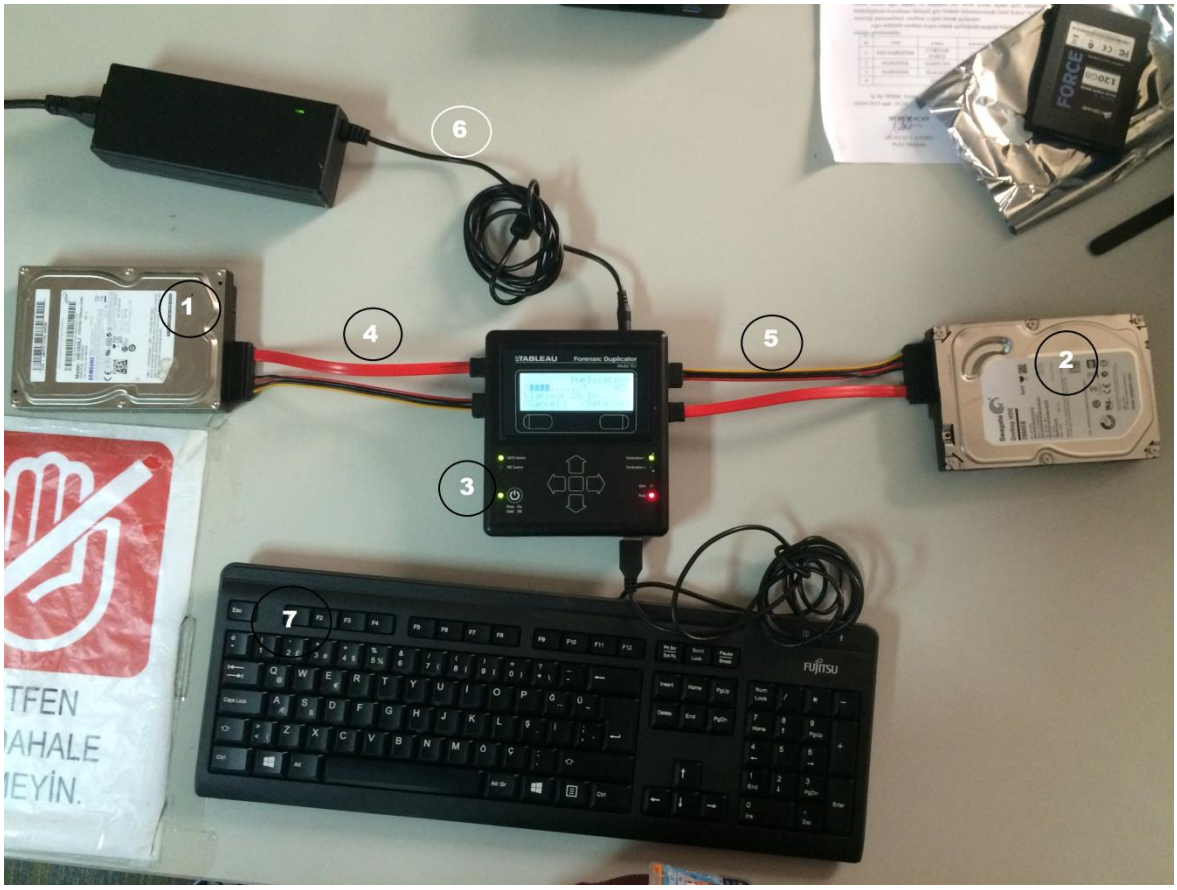
Üzerinde durulması gereken diğer bir konuda uluslararası boyutta ve ülkemizde adli bilişim uzmanlarının kullanmış olduğu bit to bit imaj olarak isimlendirilen sadece görünen alanların değil tüm diskin birebir kopyasının alınması yoluna gidilmektedir. Bu imaj alma işleminin süresi de imajı alınacak diskin kapasitesi ve durumuna göre 500 GB bir materyalin imaj alma işlemi 3-4 saat sürebilmektedir. Yani bir soruşturma kapsamında olay yerine giden adli bilişim uzmanlarının karşısına 500 GB kapasiteli sabit bir diski olan 10 (on) adet bilgisayar çıkmış olsa imaj alma işlemi en iyi ihtimalle 30-40 saat gibi bir süre alacaktır (Kara, 2014: 154).

Madde 134 – (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.

Şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş verilere ulaşılamaması durumunda çözümün yapılabilmesi veya kopyanın alınabilmesi için el koyma işleminin yapılacağı belirtilmiştir. Bu durum uygulama da bazı sıkıntılara yol açmaktadır. Öncelikle bir dijital materyalde yer alan bilgiler üzerinde şifre olup olmadığını belirlemek için olay yerinde inceleme yapmak gerekliliği şarttır. Diğer taraftan dijital materyallerde kullanılan işletim sistemleri kendi özelliklerine has olmak üzere bir bilgisayar kullanıcısının normalde göremeyeceği alanlar içerir. Bu alanlarında inceleme aşamasında araştırılması gerekir.

CMK 134 üncü madde kapsamında yapılan ev aramalarında kopya alma ve el koyma ile ilgili el konulacak ve incelenmek üzere kopyaları alınacak dijital materyallerin olay yerinde kopyasının alınmasının çok uzun zaman aldığı bu zamanın kimi zaman 24 saati geçebileceği, ayrıca el konulan materyallere el konulma işlemi yapılmadan olay yerinde kopyası alınacak olan dijital materyallerin kapasitesinin bilinmemesinden dolayı Cumhuriyet Savcılıklarından uygun kopya diski talebi yapılmamaktadır. (Uygun kopya diski talebini hangi kurum tarafından karşılayacağı da henüz netleşmemiştir.) Ayrıca ülkemizin bazı bölgelerinde terör faaliyetleri olduğu göz önüne alındığında olay yerinde kolluk kuvvetinin hem kendi hem çevresindekilerin güvenliğini bu kadar uzun sürede koruyabilmesi büyük bir gayret gerektirmektedir (Kara, 2014: 157).

Bu nedenle CMK 134'de Suç kapsamında dijital materyallere el koyma ve inceleme ile ilgili kolluk kuvvetlerinin çalışmasını kolaylaştıracak değişikler yapılması gerekmektedir.



Resim 4.1. Kopya Alma İşlemi Tableau TD1 (Disk Adli Kopyalama Cihazı)

1) Şüpheli Diski, 2) İmajın Alınan Kopya Diski, 3) Tableau TD1(Disk Adli Kopyalama Cihazı), 4) Veri İletim Kabloları, 5) Güç İletim Kabloları 6) Tableau TD1 Cihazı Şarj Kablosu, 7) Klavye.

El konulan materyalin şifresinin çözülmesi veya kopyalamanın yapılabilmesi halinde söz konusu materyalin derhal geri teslim edileceği belirtilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesinin 'Saklanan bilgisayar verilerinin aranması ve bunlara el konulması' başlıklı 19. maddesinin 3. fıkrasının d bendinde yetkili mercilere erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesi yetkisinin verilmesi gereğinden bahsedilmiştir. Yani içerisinde çocuğun cinsel istismarı ile ilgili görüntü ve resimler gibi içerik bakımından suç unsuru bulunan verilerin geri getirilemeyecek şekilde silinmesi veya erişilemez kılınması yetkisi tanınmıştır (Kara, 2014: 154).

Hukuki mevzuatımızda bu konu ile alakalı herhangi bir düzenleme olmadığından uygulamada farklılıklar mevcuttur. Soruşturma aşamasında suç unsuru bulunan dijital materyalin şüpheliye geri teslim edildiği veya suç eşyası olarak adli emanete alındığı uygulamalar görülmektedir.

Çocukların cinsel istismarı veya kredi kartı kopyalama olayları ile ilgili olarak elde edilen materyallerin kopyası alındıktan sonra olay yerinde şüpheli şahsa teslim edilmeli midir? Bu gibi olaylarda ve incelenen materyalde başkaca suç unsuruna rastlandığında ne yapılacağının detaylandırılması gerekmektedir (Kara, 2014: 154).

İmajı alınan ve şüpheliye ait olan materyallerin şüpheliye veya müştekinin yazılı talebi üzerine kanunla yedeklemesi yapılan kopyanın verilmesini istenilmemesi durumunda nasıl bir yol izleneceğinin belirlenmesi gerekmektedir.

Sonuç olarak; CMK tanımlar kısmında; şüphelinin, mağdur, maktul veya şikâyetçinin kullanmış olduğu dijital materyaller kavramına değinilmiştir. Uygulamada yeknesaklığın sağlanabilmesi için bu kavramlar ayrıntılı olarak tanımlanması zorunludur. CMK madde 134 bahsedilen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde" tabiri yerine 'Bilgisayar, cep telefonu, taşınabilir hard-diskler, müzik çalar, hafıza kartı, sim kart, modem, encoder, tablet gibi manyetik, elektronik, optik, dijital veri depolayabilen, işleyebilen, iletebilen her türlü araçları' kapsayacak şekilde ve Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesindeki tanıma uygun bir tanımlamanın yapılması anlam kargaşasını ortadan kaldıracağı değerlendirilmektedir (Kara, 2014: 154).

CMK 134. maddesinin 2. fıkrası kapsamında kolluk tarafından söz konusu suç materyalinden kopya alınırken şüpheli veya avukat hazır bulunup bulunmadığı kanunda belirtilmemiştir. Bu durumda yapılan işlemler hakkında şüpheli veya avukatının çekinceler oluşturarak soruşturmanın selametini etkilemektedir. Şüpheli veya müşteki kopya alma işleminde hazır bulunmuyorsa el konulan materyallerin kopyası alınırken kamera ile kayıt altına alınması konu hakkında ileride doğabilecek sıkıntıları ortadan kaldırması için önemli bir çözüm olabilir. Bu bağlamda uygulamada iş ve işleyişin sağlanması için CMK 134. maddesi aşağıdaki hali ile uygulanması öngörülmektedir.

CMK 134. maddesinin 4. fıkrasında 21/02/2014 tarihli ve 6526 sayılı Kanunun 11 inci maddesiyle dördüncü fıkrasında yer alan "istemesi halinde, bu" ibaresi "Üçüncü fıkraya göre alınan" şeklinde değiştirilmiştir. Bu değişiklikle birlikte imajı alınan her soruşturma konusu ile ilgili olarak şüpheli veya vekiline alınan imajın kopyasının verilmesinin zorunlu hale getirdiği, bu da özellikle çocuk pornografisi ve kredi kartı dolandırıcılığı gibi suçlarda zaten mağdur olanların mağduriyetini daha da artırmaktadır. Bu durumların önüne geçilmesi için ikili bir ayrıma gidilerek katalog suçların oluşturulması, oluşturulan katalog suçlarda yer alan suç türlerinin daha fazla mağduriyetlere yol açmaması için alınan imajın kopyasının verilmemesi veya Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesinde de yer alan (Bu sözleşme, Türkiye'nin de yer aldığı taraf devletlerinin imzasıyla onaylanmıştır. Onay sonucu taraf devletler en kısa sürede iç hukukuna entegre çalışmalarını yapması gerekmektedir.) silinerek verilmesi uygundur. Ya da yine kanunla yapılacak bir düzenlemeyle Şüphelinin kullanmış olduğu cihazlardan yapılan incelemeler sonucunda, incelenen cihazlarda hukuka aykırı içeriğin bulunduğu durumlarda verilerin kopya alındıktan sonra katalog suç ayrımına gidilmeyecekse doğrudan savcılık talimatıyla kolluk kuvvetleri tarafından silinmesinin uygun olacağı değerlendirilmektedir.

4.6. Bilişim Alanındaki Kanunların Toplum Üzerindeki Etkisi

İnternet kanunu terimiyle, akıllarda 'biri bizi gözetliyor' ve 'internet sansürü' algıları oluşmaktadır. Bir nevi devletin asimetrik olan tahakkümünü yine, yeniden halka karşı kullanması durumu ortaya çıkmaktadır.

Marx'ın dikkat çektiği sistematik izleme olarak da geçen gözetim hususu aslında, emek ve sermayenin etkileşiminin sonucudur. Eski tip köleliğin yerini gözetim ve denetim faktörüyle emekten azami düzeyde faydalanılması yer almıştır. Foucault'un da bahsettiği gibi 'Panopticon hapishanesi' aslında sürekli gözetim altında olduğu hissiyatının çok güzel bir ifadesidir. Birey olarak sürekli ziyaret ettiği internet sitelerinin birileri tarafından takip ediliyor olma ihtimali, internetin kendine has özerk, denetimsiz ve anonim yapısıyla çelişmektedir. İnternetin asıl işlevleri, toplum içinde oluşan algı yüzünden yeterince sağlıklı işlememektedir (Bozkurt, 2010).

Bilişim hukuku ya da bilişim suçları denildiğinde internetle birlikte bilişim sistemleri teknolojisi ve kullanımının günümüzde ulaşmış olduğu boyut itibarıyla ilk bakışta kuşkusuz çok geniş bir alan akla gelmektedir. Ülkemizde bilişim alanındaki yasal düzenleme çalışmaları Telekomünikasyon İletişim Başkanlığı'nın kurulması ile birlikte çok hızlı bir şekilde gelişme göstermiştir. Bilişim alanında suçlar, ülkemiz bakımından ilk olarak, Fransız hukukunun bu konudaki düzenlemelerinden de etkilenerek 6 Haziran 1991 yılında o zamanki 765 sayılı TCK'ya yapılan eklemelerle yaptırım altına alınmıştır. 2005 yılında yürürlüğe giren 5237 sayılı yeni TCK ile bilişim alanında suçlar, bizde ve batı hukukunda yaşanan gelişmeler doğrultusunda bütünüyle yeniden düzenlenmiştir.

Ülkemizde internet üzerinden yapılan yayınlar yoluyla işlenen suçlarla mücadele için 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a ihtiyaç duyulmuştur. Bu kanunun Anayasa madde 41'de geçen 'Ailenin korunması ve çocuk hakları' ve madde 58' de geçen 'Gençliğin korunması' amir hükümleri gereğince düzenlenmiştir. Asıl amaç internet ortamında belli başlı suçların işlenmesinin önlenerek, internet üzerinde yayınlanan zararlı içeriklerden çocuk ve gençlerin korunmasıdır.

5651 sayılı kanuna ilişkin yukarıda yer alan bölümde belirtilen içerikleri barındıran siteler için erişimin engellenmesine hükmedilebilmektedir. Ayrıca son yıllarda yapılan değişikliklerle, erişim engellenmesi hallerini genişletilmiş, özel hayatın gizliliğini ihlal ve kişilik haklarına saldırı hallerinde gerçek kişiler tarafından içeriğin kaldırılmasını talep edebilme hükmü düzenlenmiştir.

Bu sayede internet üzerinde yayınlanan içerikler neticesi mağduriyetlerin önüne geçilmesi hedeflenmiştir. Bu kanun değişikliklerinden önce bireylerin hakkını aramaları hususunda hukuki eksiklikler bulunmaktaydı, yapılan düzenlemeler sayesinde kişilerin izlemesi gereken adımlar açıkça belirtilmiştir.

Öte yandan, Kanun'da 2014 yılındaki değişikliklerden sonra medyada çokça yeni internet kanununun özgürlüklere müdahalesiyle ilgili haberlere yer verilmiştir. TİB'in yetkilerinin artması ve hâkim onayına sunulmadan önce gecikmesinde sakınca bulunan

hallerde re'sen karar alabileceği alanların genişletilmesinden dolayı bu tip tepkilerle karşılaşılmıştır.

Kanun gereğince, bir internet sitesi erişime engellendiğinde, mağdur, suçlu, üçüncü kişi gibi kavramlar tanımlanamaz duruma gelmektedir. Bir internet sitesinde, bir kullanıcının paylaşımı kanun gereğince suç unsuru içermesi durumunda, site tamamen erişime engellendiğinde o sitenin diğer içerik sağlayanları, üyeleri ve ziyaretçileri mağdur olmaktadır. Ayrıca her erişim engelleme, diğer bireylerin düşünce ve ifade özgürlüğüne bir müdahale oluşturmaktadır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da değinilmesi gereken ilk husus ismi her ne kadar 'Suçla Mücadele' denilse de kanunun içeriği incelendiğinde suçla 2015 yılındaki değişikliklere kadar nasıl mücadele edileceği hususu netlik kazanmamıştır. 2015 Mart ayındaki değişikliklerle suçun önlenmesi ve failin tespitine ilişkin hükümler getirilmiştir.

Böyle bir kanuna toplum düzeni açısından ihtiyaç olduğu aşikârdır. Tepkilerin devletin ideolojik aygıtlarından olan medyalardan gelmesi ve bu tedbirlerden en çok etkilenecek unsurlardan biri olmasından ötürü bu tepkilerin homojen olarak toplumun tamamının kabul ettiğini varsaymak doğru olmayacaktır. Çünkü tüm tedbirler veya suça ilişkin yaptırımlar, hâkim veya mahkeme kararına ihtiyaç duymaktadır. Bu sebeple bağımsızlığı Anayasal güvence altında olan yargılama organlarına güven hususu esas olmaktadır.

Ama her ne kadar kanun esasında yargı organlarının bağımsızlığından temel alsa da, idari tedbirlerin fazlalığı bazı konularda soru işaretlerini akla getirmektedir. Öte yandan internetteki içeriklerin erişimlerinin engellenmesine ilişkin bir kanunun mevcudiyeti de ister istemez akıllara ifade özgürlüğüne ilişkin sorunları getirmektedir.

Sosyolojik olarak ele aldığımızda da bu kısıtlamaların aslında ters tepmesi de çok muhtemeldir. Kontrol teorilerinde kontrolü elinde olmayan bireyin, kontrolü eline almak için suça yönelebileceğinden bahsedilmektedir. Daha sonraki bölümlerde daha detaylı ele alınacak olsa da, kişiler bu baskılara karşı kısıtlamaları ihlal yönünde fiiller içinde bulunabilmektedirler.

Batır'ın (2005: 158) dediği gibi internet kendine has özelliklerinden dolayı gerçek dünya hukukuyla düzenlenemez, yeni hukuki düzenlemelere ihtiyaç duyulmaktadır. Çünkü gerçek dünyadaki kanunların sınırları kanunu çıkartan devletin egemenlik sınırları iken; internetin tabi olabileceği böyle bir sınır söz konusu değildir. Bu sebeple internetle ve içeriğiyle mücadeleden söz edebilmek başlı başına bir soru işaretidir.

Gelişen ve yaygınlaşan teknolojiye uyum sağlamak için her alanda yasal düzenlemeler yapmak tabii ki bir zorunluluktur. Özellikle teknoloji araçlığıyla yürütülen işlemlerin güvenli şekilde yapılması ve bilişim suçlarından dolayı mağduriyetinin yaşanmaması için düzenlemelerin yapılması gerekmektedir.

Diğer yandan gelişen ve giderek yaygınlaşan sosyal medya; sadece bireyler için değil aynı zamanda kurumlar ve markalar için de yükselen bir yıldız haline gelmiştir. Özellikle 2000'li yılların başlarından başından itibaren sosyal medya; kurumsallaşmış şirketler ve markalar için vazgeçilmez bir iletişim aracı haline gelmiş ve artık son dönemlerde sosyal medyada varlık göstermek artık bir zorunluluk halini almıştır.

Sonuç olarak; internette gerçek anlamda bir sansürün ve denetimin uygulanması imkânsızdır. Bu durum aslında internetin tümüyle kontrol edilemezliğini ortaya koyan bir gerçektir. Fakat bu durum internetin kontrolsüz olduğu anlamına gelmemektedir. İnternetin kendi kendine oluşturduğu ve hala oluşturmaya devam ettiği bir oto kontrol mekanizması vardır. Bu bakımdan gerek bilişim ve iletişim teknolojileri genelinde, gerekse internet özelinde geliştirilecek kanuni düzenlemelerin bu özgürlüğü tehdit etmeyecek, tersine koruyacak bir anlayışla yapılması gereklidir.

4.7. Sosyal Medyanın Suçta Kullanılması

Sayısal olarak bilişim suçlarının çoğu sosyal medya araçları üzerinden işlenmektedir. Bunun en önemli sebebi, suçun öğelerinden mağdurun bilişim sistemlerini kullanması veya içinde olması gerekmektedir. İnsanları da en çok müdahil oldukları ve en çok dışarıya açıldıkları (saldırıya açık oldukları) alan sosyal medya araçlarıdır.

Her ne kadar neredeyse her insan cebinde artık birer akıllı telefon olarak bilişim sistemi taşıyor olsa da; bu cihazlar kendi içinde güvenlik sistemini barındırmakta dışarıdan saldırılara karşı daha kapalı durumda olmaktadır.

Sosyal medya araçlarında ise durum biraz daha farklıdır. Dünya'nın önde gelen şirketleri olan Facebook, Google gibi şirketler de sundukları sosyal medya hizmetlerinde güvenliği azami düzeyde tutmak için çalışmalar yapmaktadır. Tarayıcı değiştirdiğinde uyarı, güvenlik sorusu cevabından ziyade kişisel sorulara istenilen cevaplar gibi yeni güvenlik tedbirleri güncellemelerle getirilmektedir.

Her bilişim sisteminin olduğu gibi, sosyal medya araçlarının da en zayıf unsuru insandır. Sosyal medya araçları üzerinden işlenen suçların hemen hemen hiç biri bu dünya devi şirketlerinin açıklarından kaynaklanmamaktadır. İşlenebilecek suçlara işlenme yöntemlerine göre sınıflandırarak bakarsak bunun daha net olduğu ortaya çıkacaktır.

İlk olarak sosyal mühendislik (social engineering) yöntemi, bilişim suçlarının tarihsel gelişimi bölümünde ismi birçok kez geçen Kevin Mitnick tarafından yazdığı kitaba verilen ve bu sayede popüler olan bu kavram, yöntem olarak sıkça kullanılmaktadır. Bu yöntemde suçu işlemek için, sistemden ziyade kişi hedef alınmaktadır. Bu eylemdeki amaç istemedikleri bir şeyi yapmaya veya gizli bilgilerini vermeye ikna etmektir.

Bu yöntemin suç işlemek için kullanılmasına örnek verecek olursak: fail, A kişisinin Facebook hesabını ele geçirerek arkadaş listesindeki kişilerle iletişime geçip onları A kişisiymiş gibi davranıp dolandırmayı hedefleyebilmektedir. Öncelikle A kişisinin Facebook hesabını güvenlik sorusu olan 'anne kızlık soyadın nedir?' sorusunun yanıtını elde etmek için, fail A kişisiyle karşıt cinsiymiş gibi ya da uzaktan akrabasıymış gibi iletişime geçerek dayısının adını ve soyadını öğrenmeye çalışır. Bunu temin ettikten sonra artık Facebook hesabı ele geçmiştir. Bir sonraki aşamada ise A kişisini arkadaş listesindeki kişilerle iletişime geçerek onlardan sözde büyük bir şirketin çekilişinde onları da dahil etmek için telefon numaralarını ve gelecek mesajı onaylamalarını ister. Bu şekilde mobil ödeme yöntemiyle yapılacak olan alışverişi onaylamış olurlar. Bu her iki sosyal mühendislik yöntemiyle iki farklı suçu sosyal medya üzerinden işlemiş olur.

Phishing yöntemini de sosyal mühendislik olarak değerlendirebiliriz. Bu yöntemde de kişileri kendi sayfalarına yönlendirmek veya kendi bağlantılarına tıklayarak tuzak siteye yönlendirmek ve burada kişisel bilgilerini, kredi kartı numaralarını veya parolalarını elde etmek sosyal mühendislik sayılabilir.

Sosyal medya araçları üzerinden işlenebilen bir diğer suç ise siber zorbalıktır (Cyberbullying). Bu gerçek hayattaki zorbalık niteliğindeki eylemlerin sosyal ağlar üzerinden gerçekleşmesidir. Bu fiilin genellikle ön şartı sosyal mühendislikteki karşısındaki tanıma çabasının aksine zaten tanıyor olmaktır. Bir kişiyi rencide edici paylaşımlar ve yorumlarda bulunmak, onu arkadaşları içinde küçük düşürmek, tehdit etmek veya ona hakaret etmek suçları siber zorbalık olarak değerlendirilebilir.

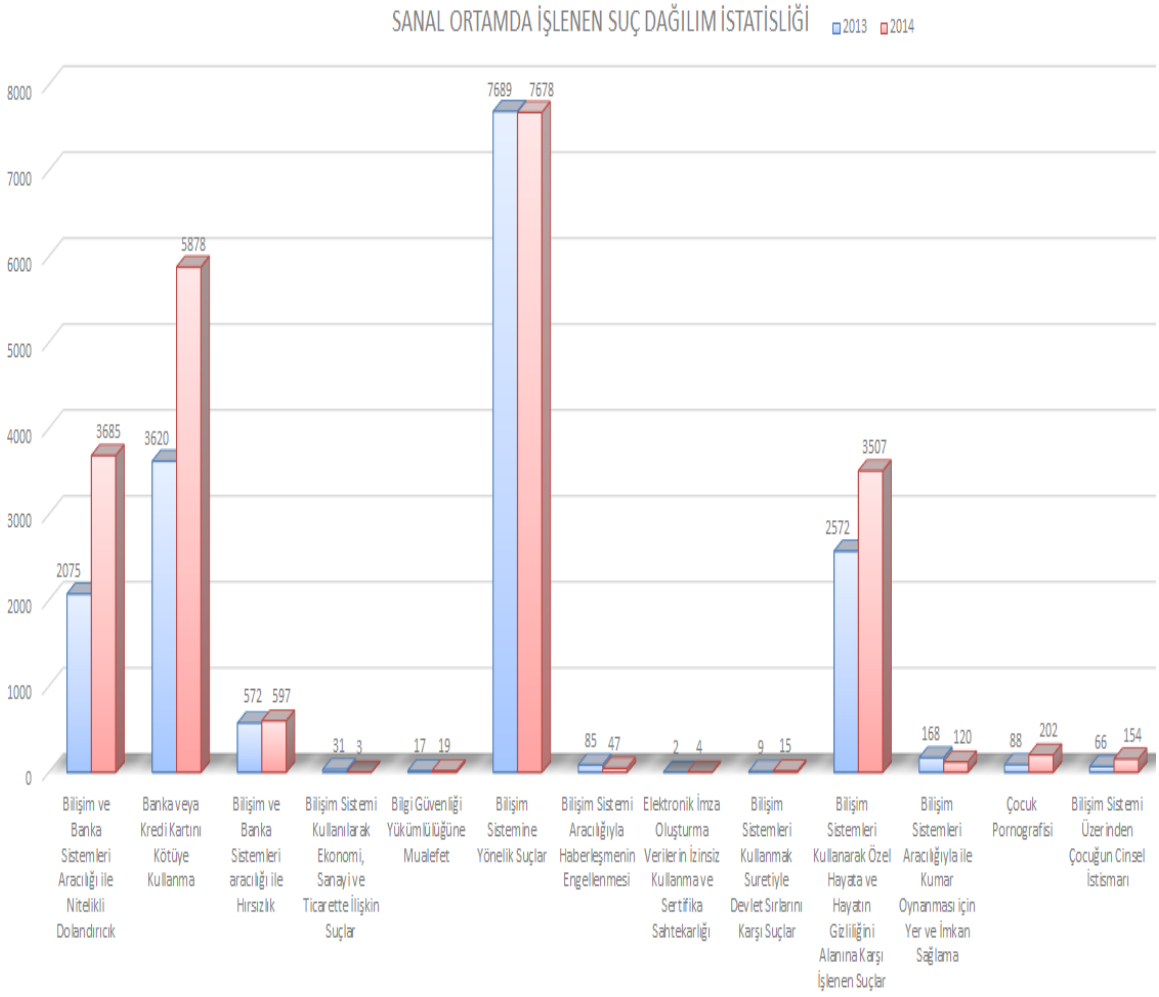
Sosyal medya araçları üzerinden yayın yoluyla işlenen suçlar ise başta 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da düzenlenen İntihara yönlendirme (madde 84), Çocukların cinsel istismarı (madde 103, birinci fıkra), Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), Sağlık için tehlikeli madde temini (madde 194), Müstehcenlik (madde 226), Fuhuş (madde 227), Kumar oynanması için yer ve imkân sağlama (madde 228) suçları ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar olmak üzere Fikir ve Sanat Eserleri Kanunu'na muhalefet suçları olarak sıralayabiliriz.

Görüleceği üzere, sosyal medya araçları kullanılarak birçok ciddi suç işlenebilmektedir. Bu yüzden sosyal medya araçlarını kullanırken veya çocuklara kullandırtırken tüm sosyolojik, psikolojik ve kriminolojik etkilerini dikkate almak çok önemlidir. Çünkü bu alanın içinde olan herkes tüm bu suçların potansiyel mağdurudur. Bunun için bu araçları kullanırken bilinçli birer kullanıcı olmak ve maruz kaldığımız her türlü içeriğe ve muhataba şüpheci yaklaşmak temel bir tutum olarak benimsenebilir.

4.8. Sanal Ortamda İşlenen Suçların Türkiye'deki Durumu

Ülkemizde suç işleme eğilimi sosyoekonomik toplumsal bir olgu olmakla beraber bu durumun sanal ortamda işlenmesinde dikkat çekici bir şekilde giderek artma eğilimindedir. Burada bilişim sistemlerini kullanmak suretiyle özel hayata ve hayatın

gizliliğini alanına karşı işlenen suçlar başlığı altında; Facebook, Instagram ve Twitter gibi sosyal medya siteleri kullanarak kişisel verilerin gizliliğini ihlal ederek, kişinin rızası olmadan resim, video veya diğer kişisel bilgilerinin paylaşılması suçları bulunmaktadır.



Şekil 4.2. Türkiye'de Sanal Ortamda İşlenen Suçların 2013-2014 Yılları Arasındaki Değişim Grafiği

Kaynak: Kara ve Şahin, 2015: 166.

Türkiye'de 2013 yılında 2014 yılına sanal ortamda işlenen suçların toplam sayısında %28,9 gibi çok yüksek boyutta artışı dikkat çekicidir. Burada bilişim sistemine yönelik suçlar en çok işlenen suç türünü oluşturmaktadır. 2013 yılında bilişim sistemine yönelik

suçlar toplam bilişim suçlarının %45,2'sini oluştururken, 2014 yılında sayısal olarak %0,01'lik düşüşle 2014 yılı suçlarının %35'ini oluşturmaktadır.

Türkiye'de sıkça karşılaşılan diğer bir suç tipi Banka veya Kredi Kartlarının Kötüye Kullanılması suçu 2013 yılında toplam suçların %21,3'üne tekabül ederken, 2014 yılında %62,4 artış gerçekleştirmiş ve 2014 yılındaki toplam bilişim suçuna oranı %26,83'e yükselmiştir.

Bilişim Sistemleri Kullanarak Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar için ise 2013 yılındaki oranı %15,1'dir. Bu sayı 2014 yılında %36,4 artmış ve 2014 yılı suçlarının %16'sını oluşturmuştur.

Banka ve Bilişim Sistemleri Aracılığı ile Nitelikli Dolandırıcılık suçu ise 2013 yılında 2075 kez karşılaşılmış ve %12,2'lik bir orana ulaşmıştır. Bu sayı 2014 yılında 1610 artarak 3685'e ulaşmıştır. Bu %77,6'lık artış, 2014 yılındaki oranının %16,8'e çıkmasına sebep olmuştur.

Bir diğer mal varlığına karşı suç türü olan Bilişim ve Banka Sistemleri Aracılığı ile Hırsızlık ise 2013 yılındaki oranı %3,3 iken, 2014 yılındaki sayısı %4,4 lük artmıştır. 2014 yılındaki oranı ise %2,7 olmuştur.

Son olarak, Türkiye'de bilişim sistemi üzerinden çocuğun cinsel istismarı suçu %133 artışla en çok artan suç türü olmuştur. Çocuk pornografisi suçu ise %129 artışla en çok artan ikinci suç türüdür.

Çocuk istismarı, karmaşık nedenleri ve trajik sonuçları olan, tıbbi, hukuki, gelişimsel ve psiko-sosyal kapsamlı ciddi bir halk sağlığı sorundur (Ziyalar, 1999: 31, Polat, 2002: 85). Grooming (Ayartma), bir kişinin cinsel istismar fiilini gerçekleştirmeye hazırlık yapmak için çocukla internet ortamında cinsel içerikli sohbet etmesi olarak tanımlanmaktadır (Kara, 2015: 151). Diğer bir ifadeyle çocuklara cinsel istismarda bulunmak amacıyla bilişim sistemleri ile arkadaşlık kurmak, güvenlerini kazanarak çocukla buluşarak fiziksel istismar bulunmaya çalışmak olarak da ifade edilmektedir.

Bu arkadaşlık çocukla cinsel bir etkileşime gerçekleştirebilmek için kurulan duygusal arkadaşlık bağını ifade etmektedir. Ayrıca bu fiilin, çocuklara cinsel etkinliklere ve çocuk pornografisini özendirmek amacıyla kullanıldığı bilinilmektedir (Kara, 2015: 2).

Grooming birbirinden farklı çocuklara yönelik suçların hazırlık hareketi olarak değerlendirildiğinden birçok ülkede (Avustralya, Kanada, Kosta Rika, Hollanda, Birleşik Krallık) suç olarak kabul edilmesine rağmen ülkemizde yasal bir düzenleme bulunmamaktadır (Kara, 2015: 151).

Bilişim alanında delil toplamanın güçlüğü dikkate alınarak bilişim suçları aracılığıyla suçların işlenmesi durumları ve yeni suç türleri tanımlanarak gerekli yasal düzenlemeler yapılmalıdır. Ayrıca ülkemizde bu suçlar mücadele konusunda tüm uzmanlar ve yasal mercilerle birlikte değerlendirilerek mutlaka ortak bilgi paylaşımın yapılabildiği uluslararası işbirliğine gidilmeli ve imzaladığımız Avrupa Konseyi Siber Suçlar Sözleşmesi'nin iç hukuka entegrasyon çalışmaları tamamlanmalıdır. Bu konu hakkında yasal düzenlemeler ivedilikle yapılması, toplumun sosyokültürel yapısının korunması için çok önemlidir.

5. Sonuçlar ve Öneriler

Bu çalışmanın sonuçlarından da anlaşılabileceği üzere mevcut teknolojilerle hızla adapte olan bilişim sistemleri, geri dönülmez bir şekilde hayatın her alanına girmiştir. Artık hayatlar dijitalleşmiş, günlük ihtiyaçların giderilmesi yanı sıra sosyalleşme için dahi başta internet ve sosyal medya araçları olmak üzere bilişim teknolojileri günlük yaşamın vazgeçilmezi olmuştur.

Bilişim teknolojilerinde yaşanan hızlı gelişmeler, yaşamımızın her alanında getirdiği kolaylıkların yanında, suç işleyen kişiler için yeni suç yöntemleri üretmede ve suçları işlemede kolaylık sağlamaktadır. Bunun sonucunda ise ülkemizde sanal ortamda işlenen suçlar giderek artış göstermektedir.

Türkiye'deki 2013-2014 yılları arasındaki bilişim suçlarının %28,9 arasında arttığı görülmüştür. Ayrıca 2006'dan beri bu bilişim suçlarının sayısı yaklaşık 40 kat artmıştır. 2013 ve 2014 yılları arasındaki en dikkat çekici yükselişin %133 artış ile çocuğun cinsel istismarı ve %129,5 ile çocuk pornografisi suçunda olması da aslında tehlikenin hassasiyetini de ortaya koymuştur.

Tüm dünyada yaşanan hızlı sosyal değişim sürecinin, aynı boyutlarda suçluluk alanında da yaşandığı görülmektedir. Mevcut istatistikler genel olarak, sosyal medya üzerinden suç ve suçluluğun ülkemizde eğiliminde bir artış eğilimi içinde olduğunu göstermektedir. Sosyal medya üzerinden işlenen suçlarda görülen değişimler, yalnızca rakamsal ölçekte olmamış, değişen sosyal ve kültürel şartlar, farklı suç türlerini de beraberinde getirmiştir. Artık suçlular teknolojik ilerlemenin getirmiş olduğu imkânlarla daha farklı alan ve yöntemleri kullanmaya başlarken suçlu ile mücadele de evrensel tedbirler almak zorunlu hale gelmiştir.

Çalışma bulgularına göre sosyal medya, kullanıcılar hakkında en mahrem olan bilgileri pazarlanmakta, elde edilen bilgiler sayesinde şirketler yeni müşteri profilleri oluşturmakta gerekse bireylerin benlik ve kimliklerine büyük zarar verme olasılığını artırmaktadır. Modernleşme sürecinde ülkemizde internet kullanıcılarının artması ile yaşanılan sorunları toplumun iç dinamikleri ve hukuki merciler alacağı tedbirlerle bireysel gelişim ve toplumsal farkındalığın artmasını sağlanmalıdır. Sosyal medya ortamında güvenli kullanımı için alınan tedbirlerin başarısını zaman gösterecektir.

Sosyal medya kullanımının her geçen gün yaygınlaşmasıyla bu teknolojilerin suç işleme amaçlı kullanımına yönelik yapılan araştırmalar önem kazanmaktadır. Sosyal medya araçları, suç ve suçluluk kültürünü ve uygulamalarını değiştirmekte, toplumları tehdit eder hale gelmektedir.

Sosyal medya ile ilgili araştırma sonuçları, kötü niyetli kullanımların dışında söz konusu araçların öğrenenlerin bilgiyi bulma, oluşturma, paylaşma ve iletişim kurma becerilerini olumlu yönde etkilediğini göstermektedir. Sosyal medya, öğrenciler arasında eğitimsel bilginin aktarımı için kullanılmakta, çevrimiçi öğrenme bağlamında öğretmen-öğrenci, öğrenci-kaynak, öğrenci-öğrenci arasında dinamik bir ilişki oluşturmaktadır (Sistek-Chandler, 2012: 78).

5.1. Önleme ve Mücadele Önerileri

Bilişim suçlarının yıllık küresel maliyeti yaklaşık 445 milyar dolardır.[28] Bu suçların kurbanı olmamak için kişi ve devlet bazında bir takım önlemlerin alınması gerekmektedir.

Kişisel bazda alınabilecek önlemler, bilinçli birer kullanıcı olmakla başlamaktadır. Kullandığımız veya içinde olduğumuz teknolojinin farkında olmak gerekir. Özellikle çocukların ebeveynlerine göre teknolojiye daha yatkın olması ve teknolojiyle daha çok vakit geçirmesi ebeveynlere daha büyük sorumluluklar yüklemektedir. Çocuklar için evde bilgisayar başında olmaları güvende oldukları anlamına gelmemektedir. Çocuklar internet ile dünyaya açılabilmektedirler ve yetişkinlerin bile günlük hayatta muhatap almak istemeyeceği insanlarla, küçük yaştaki çocuklar muhatap olabilmekte ve bu tip insanlardan gelebilecek uygunsuz içeriğe maruz kalabilmektedir. Türkiye'de birçok çocuğun internetten tanıştığı kişiler tarafından buluşmaya çağrıldığı ve hatta kimi vakalarda istismar edildiği bilinmektedir. Bu sebeple ebeveynlerin alması gereken tedbirlerin başında çocuğunun yaptıklarının ve kullandığı teknolojinin farkında olmak, onu sanal âlemde de gözetim ve koruma altında tutmak gelmektedir.

[28] http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609#hx3xD7usqjjM4WIT.97 (Erişim tarihi: 23.11.2015)

Kurumsal açıdan bilişim sistemlerinin güvenliği için alınabilecek tedbirleri Değirmenci (2002: 106 - 108) yedi ana başlıkta toplamıştır: İdari ve kurumsal güvenlik, personel güvenliği, fiziksel güvenlik, iletişim ve elektronik güvenliği, donanım güvenliği, yazılım güvenliği ve işlem güvenliğidir.

Devlet tarafından mücadele ve önlem olarak uygulanması gereken politikalar aşağıda başlıklar halinde daha detaylı olarak ele alınmıştır.

5.1.1. Eğitim

İlk olarak vatandaşların internete ve bilişim teknolojilerine farkındalığının sağlanmasıyla başlanılmalıdır. Bu eğitim için halk eğitim merkezleri ve diğer eğitim birimleri kullanılabilir. Bu eğitimin içeriğinde bilgisayar, akıllı telefon ve diğer bilişim cihazlarının kullanımı ve yetenekleri gösterilmelidir. İnternet kullanımı ve sosyal medya kullanımına ilişkin bilgilendirmelerin yanı sıra bilinçli birer kullanıcı olmak için internet ve sosyal medya araçlarının fırsat ve tehditleri sunulmalıdır. Özellikle ebeveynlerin çocuklarını koruması için sanal dünyanın risklerine ve uygunsuz içeriklerine karşı bilinç uyandırılmaya yönelik içerikler oluşturulmalıdır.

Müfredata alınarak ilkokuldan itibaren öğrencilerin bilinçli kullanıcı olmalarına ilişkin uygun düzeyde medya okuryazarlığı eğitimleri verilmelidir. İnternette karşılaşılan içeriklerin ne mahiyette olduğu, güvenilirliği, amacı bu medya okuryazarlığı kapsamında düzenlenebilir. İnternette sakıncalı içeriklerle karşılaşan öğrencilerin ihbar mekanizmalarını bilmesi en azından öğretmeni veya velisiyle paylaşmasını sağlayacak ortam oluşturulmalıdır. Burada dikkat edilecek nokta, yaş gruplarına göre içerikler belirlenmeli, bu kadar yeniliğe açık beyinlerin muziplik amacıyla da olsa yanlış, etik dışı hatta suç barındıran fiiller içine girmelerine yol açacak bilgiler verilmemelidir. İngiltere[29] ve Güney Kore[30] örnekleri gibi ilkokulda yazılım dersleri konularak, bireylerin küçük yaştan itibaren teknolojik farkındalığın oluşması da sağlanabilmelidir.

[29] http://www.milliyet.com.tr/ilkokulda-yazilim-gelistirme-dersi/gundem/gundemdetay/18.11.2012/1628845/default.htm (Erişim tarihi: 23.11.2015)

Eğitimin diğer ayağı da bilişim suçlarıyla mücadele eden devlet görevlilerinin eğitilmesidir. Her yıl on binlerce açılan soruşturma delil yetersizliğinden, failin tespit edilememesinden veya 'şüpheden sanık yararlanır' ilkesinden dolayı sonuca ulaşamamakta veya fail cezasız kalmaktadır. Bilişim suçuyla mücadele eden görevlilerin, etkili bir mücadele gerçekleştirebilmeleri için failler düzeyinde veya onların neler yaptığının farkında olacak düzeyde bilişim teknolojilerine vakıf olması gerekmektedir.

Vasıflı personel ihtiyacının giderilmesinin ilk ayağı başta polis ve jandarma olmak üzere kolluk kuvvetleridir. Soruşturmacı personelin fail tarafından suçun nasıl işlendiği ve delilleri nereden toplayabileceği konusunda yeterli bilgi ve donanıma sahip olması gerekmektedir. Aynı şekilde adli bilişim olarak adlandırılan dijital delillerin tespiti, toplanması, adli kopya alınması, muhafazası, incelenmesi ve raporlanması aşamalarından oluşan sürecin de sağlıklı yürütülmesi gerekmektedir. Adli bilişimle ilgili olarak Siber Suçlarla Mücadele Daire Başkanlığı tarafından uluslararası standartların takip edildiği ve personelin gerek yurt içi gerekse yurt dışı eğitimlere katılımlarının sağlandığı bilinmektedir. Ancak dünyada önde gelen ülke kolluk birimlerinin mücadele yöntemlerinin bilinerek uluslararası işbirliğinin kurulması gerekmektedir.

Kolluk birimlerinde ender bulunan ve zorlukla yetiştirilen vasıflı personelden en etkili şekilde faydalanılması gerekmektedir. Emniyet teşkilatı örneğinde üst düzey bilgisi olan personel, bilgisi ne olursa olsun rütbesine göre görevlendirilmekte ve değerlendirilmektedir. Aynı şekilde mesai saatlerinin fazlalığı ve diğer birçok mesleki zorluklar bilişim suçuyla mücadelede negatif etki oluşturmaktadır. Bilişim suçlarıyla mücadele eden personelin sahip olduğu bu yeteneklerin aldığı maaşa da herhangi bir etkisinin olmamasından dolayı vasıflı personellerin daha iyi çalışma koşullarıyla daha yüksek ücreti aldığı özel şirketleri tercih ettiği bilinmektedir. Bu sebeple bilişim suçlarıyla mücadele eden teknik kapasitesi yüksek vasıflı personelin emniyet mensubu olmaması ya da emniyet mensubu olsa da farklı statüde istihdam edilmesi uygun olacaktır.

---

[30] http://www.ntv.com.tr/teknoloji/yazilim-dersi-ilkokulda-zorunlu-olacak,PS_7TVRy_EKYENQihpdJKQ (Erişim tarihi: 23.11.2015)

Yargı organları olan hâkim ve savcıların da bilişim suçları konusunda bilgilendirilmesi gerekmektedir. Hakim ve savcılar genellikle temel düzeyde dahi olsa bilgi sahibi olmadıkları için soruşturma ve kovuşturmanın akıbeti, bilirkişiler ve kolluk ekseninde belirlenmektedir (Dülger, 2013: 702).

5.1.2. Denetim

Ülkemizde internetin denetlenmesi kavramıyla akıllara gelen 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanundur. Bu kanun ile internetteki içeriklerin kontrol edilmesi ve içerik sağlayıcıların içeriklerinden dolayı sorumlu kılınması hedeflenmektedir. Hatta kanunda 5237 sayılı Türk Ceza Kanunu'nda yer alan;

-İntihara yönlendirme (madde 84),
-Çocukların cinsel istismarı (madde 103, birinci fıkra),
-Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
-Sağlık için tehlikeli madde temini (madde 194),
-Müstehcenlik (madde 226),
-Fuhuş (madde 227),
-Kumar oynanması için yer ve imkân sağlama (madde 228) suçları ile

5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlarını oluşturan içerikler hakkında erişimin engellenmesi hükmünü getirmiştir.

Öte yandan aynı kanun talep edilmesi halinde içerik sağlayıcılarının, yer sağlayıcılarının ve erişim sağlayıcılarının sahip olduğu bilgileri paylaşmasını da hükme bağlamıştır. Bunun anlamı da yetkilileri (editör vb.) Türkiye'de olan bir siteye bağlanıyorsak veya Türkiye'de sunucuları bulunan bir siteye bağlanıyorsak ya da internete bağlanmak için bir TTNET, Turkcell, Superonline gibi Türk şirketini tercih etmişsek; bizim bilgilerimiz Telekomünikasyon İletişim Başkanlığı tarafından ulaşılabilir anlamına gelmektedir. Türkiye'deki internet kullanıcısının çokluğu ve bağlantıların yaklaşık 12 basamaklı bir sayı bloğu olan IP adresleriyle gerçekleşmesinden ötürü bireysel takibin çok kolay olmadığı bilinse de teknik olarak imkânsız olmadığı ve belirli bir kişinin internet aktivitelerinin kontrol altında tutulabileceği göz ardı edilmemelidir.

Devletin bu şekilde denetim kabiliyeti bulunmaktayken peki bu denetim yerinde midir ve yeterli midir soruları gündeme gelmektedir. Böyle bir denetim Dülger'in (2013: 702) belirttiği gibi kişi mahremiyeti ve iletişim özgürlüğü gibi bazı demokratik toplumların olmazsa olmaz değerlerini zedeleyebilmektedir. Bunların ihlali söz konusu olmasa bile toplumda böyle bir algının varlığı, kişi nezdinde devlete olan güvenden şüphe edilmesine yol açmaktadır. Çok hassas bir noktada bulunan bu durum için kişilerin mahremiyeti ve iletişimi mevcut yasalarla güvence altına alınarak, Anayasa'da belirtildiği gibi belirli istisnai durumlarda ve belirli kanunlar uyarınca ihlal edilebilmelidir. Ceza Muhakemesi Kanunu madde 135'de iletişimin tespiti ve dinlenmesi hususları hükme bağlanmıştır. İnternet iletişimine ilişkin bir tespit gerekiyorsa da bu madde hükümlerince hareket edilmesi uygun olacaktır.

Bu tarz bir denetim yeterli de değildir. Çünkü failler genellikle bağlantı sağlanan IP'ler ile tespit edilmektedir; kullanılan bilgisayar veya kullanıcıyla değil. Bunun sebebi küresel sistemin bu şekilde işliyor olması ve internet üzerindeki veri alışverişinin belirli protokollerle (IP) gerçekleşiyor olmasından kaynaklanmaktadır. Elde edilen IP sonucu ulaşılan şüpheli de olayın failinden ziyade internet aboneliğinin sahibidir. Özellikle günümüzde ticari kaygılarla internet aboneliklerinin ve gsm hatlarının yoldan geçenlere neredeyse kontrolsüz dağıtılmasının sonucu olarak, fail hiç tanımadığı ve ilgisi olmadığı birinin adına temin ettiği hat ile bağlantı sağlayarak suç işleyebilmektedir. Bunun nihai sonucu olarak da tespit edilen şüpheli olayla hiçbir ilgisi olmayan kimlik bilgileri kullanılmış biri çıkmaktadır. Bu sebeple internet abonelikleri veya gsm hatlarının kullanımına ilişkin düzenlemeler geliştirilerek sıkı sıkıya uygulanmasının sağlanması gerekmektedir.

Bir diğer denetlenmesi gereken husus da 5651 sayılı kanunda toplu kullanım sağlayıcıları olarak geçen internet hizmeti sunan kurum ve şirketlerdir. Özellikle internet kafelerin birçok suç soruşturması sonucunda ulaşılabilen son nokta olması, olayın gerçek faillerinin meçhul olarak kalmasına sebep olmaktadır. Her ne kadar log kayıtları tutuluyor olsa da, hangi bilgisayarın hangi gerçek kişi tarafından kullanıldığının kayıt altına alınamamasından dolayı suçlar faili meçhul kalmaktadır. Buna karşı alınabilecek önlem olarak log kayıtlarıyla birlikte kimlik bilgilerinin tutulması akla gelse de böyle bir bilginin devlet tarafından tutuluyor olması bile şüphe

uyandırırken internet kafe işletmecisi tarafından tutulmasının ne kadar güvenli olacağı sorusuyla karşı karşıya kalınmaktadır. Bu sebeple toplu kullanım sağlayıcıları için ulusal bir kontrol sistemi geliştirilerek belki e-devlet üzerinden denetimi sağlanabilir. Örnek olarak geçici internet hizmetini almak isteyen kullanıcı bilgisayar ile doğrudan e-devletin paneline yönlendirilerek, kişinin sistemde kendi üzerine olan telefon numarasına gelen onay ile internet erişimi sağlaması sunulabilir. Bu mekanizmanın devlet dışında herhangi farklı bir şirket tarafından kontrol edilen programlarla sağlanması ciddi bilgi güvenliği riski oluşturacağı göz ardı edilmemelidir.

5.1.3. Uluslararası işbirliği

İnternetin getirdiği yeniliklerden biri, bireyler için mevcut kimliklerinden bağımsız, toplum ve kanun baskısı olmaksızın hareket edebilme kabiliyetine olan inançtır. Çünkü kanunlar genelde koyuldukları devletlerin egemenlik sınırları içinde geçerlidir; ancak internetin tabi olduğu bu tip bir egemenlik alanı mevcut değildir. Bu sebeple internet belirli bir ülkenin malı değil, tüm dünya insanlarının veri alışverişinde kullanabildiği ülkelerin sınırlarında bağımsız ağlar ağıdır.

Ülkemizde faaliyet gösteren çeşitli internet siteleri (oyun siteleri vb.) yaygın olarak kullanılmaktadır. Facebook, Instagram ve Twitter gibi sosyal paylaşım siteleri art niyetli kişilerce, bireysel ve kamu kurumlarına karşı bilişim suçunun işlenmesinde aracı olarak kullanılmaktadır. Bu durum göz önüne alındığında sosyal medya kuruluşlarının ülkemizde resmi temsilciliklerinin bulunmasının zorunluluğu aşikârdır. Çünkü bürosu olmayan bu kuruluşlarda suç soruşturmalarında bilgi ve belge talep edildiğinde kolluk kuvvetlerinin verilere ulaşması güçleştirmektedir. Bu sebeple bu tip internet sitelerini barındıran ülkelerle kurulacak kanallarla suçun aydınlatılmasına yönelik bilgi ve belge taleplerinin karşılanması sağlanabilir.

Bilişim suçları nitelik itibariyle mekândan bağımsız bir karakterdedir. Fail ile mağdurun aynı ortamda bulunma zorunlulukları da yoktur. Hatta aynı şehir, aynı ülke ve aynı kıtada bile olmayabilirler. Bu sebeple bilişim suçları, kaçakçılık gibi sınır aşan bir suç eğilimindedir. Yürütülen soruşturmalarda tespit edilen IP yurt dışında kalıyorsa çoğu zaman soruşturma sekteye uğramaktadır. Yurt içi çıkan IP'lerde dahi soruşturmanın

süresi aylarla ölçülürken, yurt dışında olması durumunda bu sürenin yılı aşkın sürelere çıkması muhtemeldir. Bu sebeple uluslararası işbirliklerin etkili ve hızlı biçimde delil niteliğindeki bilgi ve belgenin transferi oluşması yönünde kurulması gerekmektedir.

5.1.4. Mevzuat

Elde edilen veriler göstermektedir ki; son iki yılda ülkemizde bilişim sistemi üzerinden çocuğun cinsel istismarı suçu, en çok artış gösteren suç türü olmuştur. Bu nedenle bu alanda yasal düzenlemelerin kapsamlı bir şekilde artırılması ve Grooming kavramı tanımlanarak Çocukların Cinsel İstismarı TCK madde 103, Cinsel Taciz TCK madde 105, Müstehcenlik TCK madde 226/3, Çocukların Kullanıldığı Pornografik Materyal maddesi kapsamına eklenmesi zorunlu hale gelmiştir. Görülmektedir ki bilişim suçları ile mücadelede bilişim teknolojileri ve hukuki düzenlemelerin beraber kullanımı sayesinde neticeye ulaşmak mümkün olacaktır.

Ayrıca Türk Ceza Kanunu'nda bilişim suçlarına ilişkin düzenlemelere yukarıda yer verilmiştir. Bu maddelerin suçları daha iyi tanımlamaları ve cezai tedbirlerin orantılı olacak şekilde caydırıcılık düzeyleri artırılmalıdır. 243. maddesinde düzenlenen bilişim sistemine girme suçunun ilk fıkrasında "…hukuka aykırı olarak giren ve orada kalan…" şeklinde düzenlenmesi suçun gerçekleşmesi için sisteme girmenin tek başına yeterli olmayacağını orada kalmanın da gerekliliği anlamını taşımaktadır. Bu düzenlemenin "…hukuka aykırı olarak giren veya orada kalan…" şeklinde düzenlenmesi daha uygun olacaktır.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nde 'Saklanan bilgisayar verilerinin aranması ve bunlara el konulması' başlıklı 19. maddesinde yetkili mercilere, erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesi yetkisinin verilmesi gereği belirtilmiştir. Suça konu materyal içerisindeki verilerin bulunmasının suçu devam ettirebileceği, yeni mağduriyetlere yol açabileceği durumlarda bu tip verilerin silinerek şüpheliye verilmesi daha uygun olacağı değerlendirilmektedir. Özellikle çocuk pornografisi ve kredi kart bilgilerinin kullanılması suçlarında verilerin hali hazırda bulundurulmasının zaten suç olduğu ve

yeni mağduriyetlere yol açabileceğinden içindeki verilerin silinmesine yetki sağlayacak düzenlemelerin iç hukukumuza entegre edilmesi gerekmektedir.

5.2. Sosyolojik ve Kriminolojik Önlemler

5.2.1. Durumsal suç önleme

Felson, durumsal suç önleme ile "suçluların illegal faaliyetlerini yürütmek için kullandıkları suç fırsatlarını azaltarak suçun önlenebilmesi için kullanılan bir dizi tekniği" ifade etmektedir (aktaran Dolu, 2010: 130). Bu teorinin en temel özelliği, suçludan ziyade suçu oluşturan faktörleri ele almasıdır. Bu sebeple muhtemel suçlu, uygun hedef ve suça karşı yetenekli bir koruyucunun yokluğu ile suçun meydana geldiğini öne süren rutin aktivite teorisini temel almaktadır.

Bu durumsal suç önlemeyi bilişim suçlarında nasıl etkili olabileceğini ortaya koymak için hangi faktörlerin etkili olduğunu irdelemek gerekir. Muhtemel suçlu, yeterli bilgi ve teknik donanıma sahip, suç işleme kastı olan kişidir. Uygun hedef olarak, teknoloji hayatının içinde olan her bir birey bu suçun mağduru olabilir. Koruyucular ise başta kolluk kuvvetleri olmak üzere bilişim suçuyla mücadele eden görevlilerdir. Bu üç faktör bilişim suçlarının durumsal önlenmesi konusunda ayrı ayrı ele alınacaktır.

Bireyin muhtemel suçlu olabilmesi için uygun şartların oluşması gerekmektedir. Bireyin teknik bilgiye sahip olması iyi niyetli düşünüldüğünde hem birey hem toplum için artı değerdir. Bu sebeple teknik bilgi konusunda fırsata engel olmadan söz edilemez. Diğer fırsat ise yeterli donanıma sahip olması, bu genellikle bir bilgisayar veya benzer işlevli bir cihaz ve internet bağlantısı ile sağlanmaktadır. Bu her iki öğeden de bireylerin mahrum bırakılması gibi bir durum söz konusu değildir. Ancak kişinin internete bağlanırken anonim olduğu konusunda şüpheleri varsa, suç işlemedeki motivasyonunda azalma olacaktır. Yukarıda da belirtildiği gibi muhtemel suçlu denetim mekanizmasının işlemesinden dolayı internet kafeye gittiğinde bulunma korkusu taşıyorsa, bu bir fırsat yoksunluğudur. Aynı şekilde, sınır aşan bir eylem içerisindeyse; ancak uluslararası işbirliği failin kolayca tespit edilip, yargı huzuruna çıkarabilecek düzeydeyse yine muhtemel suçlu için negatif bir durum söz konusudur. Diğer bir husus, yakalanması

durumunda, alacağı cezaların yaptırım gücü de muhtemel suçlu üzerinde caydırıcı etki yaratabilecektir.

Uygun hedef adayları, teknolojiyi hayatında yer eden her bireydir. Hedefleri uygunluktan çıkartmak için, ilk uygulamaya sokulması gereken eğitim faaliyetleridir. Bireylerin, bilişim teknolojileri ve internet konusunda düzenlenecek eğitimlerle hem kendileri hem de aile bireyleri için bilinçli birer kullanıcı haline getirilmeleri gerekmektedir. Bunun yanı sıra kişisel ve kurumsal ölçekte alınacak sistemsel tedbirlerle suçun işlenme ihtimali minimize edilebilir.

Suça karşı yetenekli koruyucuların başında kolluk birimlerinin bilişim suçlarıyla mücadele birimlerinde çalışan görevlileri gelmektedir. Bu polis teşkilatında Siber Suçlarla Mücadele Daire Başkanlığı ve taşra birimleri tarafından icra edilmektedir. Temelde suç soruşturma, suç önleme ve adli bilişim olarak üç farklı alanda mücadele gerçekleştirilmektedir. Yetenekli koruyucuların varlığı ancak bu birimlerde çalışan personelin kalifiye olmasıyla sağlanabilir. Bu personelin de kendi alanlarıyla ilgili eğitilmesi gerekmektedir. Bu sayede gerek suç oluşmadan önce tedbirlerle, gerek suç sonrası soruşturma işlemlerinde, gerekse suça konu dijital materyallerin incelenerek delil olarak kabul edilip raporlanması işlemlerinde başarı oranı artacak ve muhtemel suçlu için yakalanmama ihtimali düşecektir. Diğer yandan, koruyucuların bu yeteneklerini daha etkili kullanabilmeleri için de, oldukça önemli diğer bir husus da mevzuatın sağladığı yetkidir. Tüm mücadele işlemleri belirli bir mevzuata dayanarak yerine getirilmektedir. Mevzuatın da birey bazında kişisel hak ve özgürlükleri ihlal etmeden ancak bu suçla da en etkin mücadeleyi sağlayacak şekilde optimize edilmesi gerekmektedir.

Bilişim suçlarının durumsal önlenebilmesi için yukarıda belirtilen üç faktöre göre de fırsatların değerlendirilerek, suç oluşumu için asgari düzeye çekilmiş olması sağlanmalıdır.

5.2.2. Suça karşı öğrenme

Suçun açıklanmasına ilişkin bir diğer görüş de, suçun öğrenilen bir davranış olduğudur. Akers, Amerika Birleşik Devletleri'ndeki suç önleme ve suçlunun ıslahına ilişkin

uygulanan programlarda ister yetişkin suçlu olsun, isterse de çocuk suçlu olsun istenilen yönde davranış değişikliği yapabilmek için öğrenme teorisinin prensiplerinden yararlanıldığını belirtmiştir (aktaran Dolu, 2010: 254). Suça karşı bu öğrenme süreçleri üç aşamada ele alınabilir: aileden ve çevreden öğrenme, suçun mutlak cezalandırılacağı ve suçlunun ıslahıdır.

Bilişim suçları için de bu süreçlerin kısmen geçerli olduğu söylenebilir. Suçlu davranış ilk olarak ailede öğrenilir. Bilişim suçu bir şiddet suçu olmasa da, yine de etik davranış kalıpları açısından aileden öğrenebileceği bir takım davranışlar mevcuttur. Örneğin, aile içinde görünüş itibariyle kimseye zararı olmayan bazı sapkın davranışlar hoş karşılanıyorsa veya meşru görülüyorsa, çocuklar bu durumdan olumsuz etkilenebilir. Baba, beyaz yaka suçlarından birini işliyorsa yine benzer şekilde ileride mal varlığına yönelik bilişim suçları da çocuk için meşru olarak görülebilir. Toplumda siyasi ve ideolojik amaçlarla işlenen suç fiilleri aile içinde destekleniyorsa yine bu aile çocuğu için hacktivist eylemleri gerçekleştirmek yetiştiği ortam için çok aykırı davranış olmayacaktır.

Suçun karşılığında mutlaka cezalandırılacağı inancı toplum içinde yaygın olması gerekmektedir. Bunun tersi durumda fail, işlediği suçun yanına kar kalacağını düşünürse, suç için daha çok motive olması muhtemeldir. Bunun için de toplumda ne boyutta olursa olsun suç olarak tanımlanmış davranışların cezalandırılacağı inancının yerleşmiş olması gerekmektedir. Bilişim suçlusu için yakalanmama inancı ve yakalansa dahi alacağı cezanın az olacağı veya ceza almayacağı inancı güçlü birer motivasyondur. Bu motivasyonların kırılması için bazı tedbirlerin alınması gerekir. Yakalanmama inancı ancak bilişim suçu konusunda uzman kolluk kuvvetlerinin yetiştirilmesiyle kırılabilir. Bilişim suçlarıyla mücadele eden görevlilerin eğitilmesi büyük önem arz etmektedir. Diğer önemli husus da cezaların yaptırım gücüyle alakalıdır. Eğer kişi işlediği fiilden dolayı mutlak cezalandırılacağını bilirse, yine suçu işleme konusunda isteksiz olacaktır.

Suçlunun ıslahı da suça karşı öğrenmelerin bir sürecidir. Özellikle hapishanelerde bir arada duran mahkûmlar için bu ortamlar bir nevi suç okulları olmaktadır. Bu sebeple mahkûmların büyük gruplar halinde koğuşlarda değil de birer ikişerli hücrelerde kalmalarının sağlanması daha uygun olacaktır. Mahkûmların sosyalleşmesi ve topluma

yeniden kazandırılması için mesleki faaliyetler ile spor salonu, kütüphane gibi sosyalleşme ortamları sunulmalıdır (Dolu, 2010: 256). Bilişim suçluları için ise bu genel tedbirlerin yanında sahip oldukları bilgi ve beceriden yararlanarak, onları da toplumun karanlık tarafında değil, aydınlık tarafında mücadele etmeleri sağlanabilir.

5.2.3. Kontrol mekanizmalarının geliştirilmesi

Kontrol teorilerinin ortaya koyduğu suçu engelleyen faktörler iç ve dış olmak üzere ikiye ayrılmaktadır. İç kontrol mekanizmaları, bireyin çocukluğundan itibaren başta ailesinden ve diğer çevresel değişkenlerden etkilenerek birey tarafından içsel olarak geliştirilen mekanizmalardır. Dış kontrol mekanizmaları ise toplumsal değerler ve kısıtlamalar gibi bireyin dışındaki faktörlerin, birey üzerinde kontrol işlevi kazanmasıyla oluşur.

İç kontrol mekanizmaları yukarıdaki bölümde de bahsedildiği gibi ilk olarak ailede gelişir. Ailenin çocuk gelişiminde sağlıklı bir rol model üstlenmesi önem arz etmektedir. Hangi davranışların yanlış olduğu ve bu yanlışların düzeltilmesi ve cezalandırılması gerektiği ilk ailede öğrenilebilir. Ayrıca dünya görüşüne ilişkin ilk oluşumlar da ailede oluşmaktadır. Özellikle günümüzde tüketim toplumunun karakteristiği haline gelmiş, doyumsuzluk ve her şeyi elde etme arzusu insanları sınır tanımaz birer birey haline getirmektedir (Dolu, 2010: 289). Öz kontrolü yüksek bireylerin gelişmesiyle toplum içindeki suç oranlarının düşmesi muhtemeldir. Ancak böyle bir toplumun inşası için devlet eliyle ailelerin bilinçlendirilmesine ilişkin politikalar belirlenerek, uygulamaya sokulmalıdır.

Ayrıca, bireyden ziyade devlet veya benzer kuruluşlar eliyle yürütülmesi gereken diğer uygulama da gençlerin enerjilerini yanlış şeylere sevk etmesinin önüne geçmektir. Bu da gençleri sosyal veya sportif etkinliklere sevk ederek olabilir. Bilişim suçları için de bu çok önemli bir noktadır. Çocukluktan itibaren bilişim teknolojilerine yönelmiş bireylerin bilişim suçu faili olma ihtimalleri diğer bireylere göre daha yüksek olması beklenmektedir. Bilişim suçu işlemenin en büyük motivasyonlarından birinin popülarite ve diğerinin kişisel tatmin olduğunu düşünürsek, bilişim alanında, siber güvenlik veya benzeri konularla ilgili gençlere yönelik yarışmalar düzenlenerek hem gençlerin

enerjileri doğru bir kanala yönlendirilmiş olur, hem de suçla aradıkları popülarite gibi bir takım hazların da giderilmesi mümkün hale gelmiş olur.

Dış kontrol mekanizmaları ise toplumsal değerler ve toplumsal düzendir. Toplumsal değerler, toplumdan topluma değişmektedir. Bu toplumsal değer ve düzen için bazı normlar mevcuttur. Bireyler bunları içselleştirdiği ölçüde toplumsal düzenden bahsedilebilir. Bunların öğretisi de yine ağaç yaş iken eğilir misali ailede başlar; kişi topluma ait olduğunu hissettiği müddetçe bu dışsal faktörler etkili olacaktır. Benzer şekilde bu toplumsal normlar, eğer siyasi iktidar gibi birey üzerinde etkisi olan farklı gruplardan dolayı değiştirilip baskın şekilde uygulanıyorsa, suçun oluşması muhtemeldir. Bu şekilde değiştirilmiş normların içselleştirilmesi zorlaşırken hem de kendini baskı altında hisseden bireylerin ise gücü elde etmek veya gücünü göstermek için suç işlemesi muhtemeldir. Bu durum bilişim suçları için de geçerlidir. Buna örnek olarak ABD'de açılımı Merkezi İstihbarat Teşkilatı olan CIA'in yapılan saldırılar sonucu açılımı Merkezi Budalalık Teşkilatı olan CSA'ye çevrilmesi bu gücü elde edebilmiş olmanın bir göstergesidir (Jordan ve Taylor, 2010: 221). Bu sebeple toplumsal değerlerin içselleştirilmesi büyük önem arz ederken, toplumsal değerlerin baskıcı veya zorlayıcı şekilde değiştirilmesi de suça iten bir faktör olabilmektedir.

Sosyal medya; gerekli kurallara uyularak kullanıldığında yararı olduğu gibi bağımlılık boyutunda varan kullanıcılar için büyük zararları da bulunmaktadır. Özellikle ebeveynlerin çocukların sosyal medyanın kötü amaçlı kullanımlar için gerekli tedbirleri alması gereklidir. Bu amaçla özellikle online çocuk istismarı suçunun ülkemizde tanımlanması ve gerekli yasal düzenlemelerin yapılmalıdır. Bu araştırmanın temel amacını oluşturan toplumun her kesim ve her yaş grubundan kişilerin sosyal medyayı nasıl kullanması gerekliliği konusunda toplumsal kamuoyunda farkındalık yaratılması gereklidir.

Ekler Listesi

Ek 1. Kronolojik Olarak Önemli Bilişim Suçları

Şimdiye kadar meydana gelmiş adından söz ettirmiş bilişim suçu olaylarını ele alacak olursak 4 dönem halinde sınıflandırmak yerinde olacaktır.[31]

1. Dönem - 1970-1990

1971

John Draper, Cap'n Crunch isimli mısır gevreğinden çıkan düdüğün 2600 mHz'lik ses çıkarttığını ve bunun da telefonlarla arama yapmak için makineye atılan çeyreklikle aynı frekansta olduğunu keşfedip, bu şekilde ahizeye düdüğü üfleyerek makinenin çeyreklik atıldığını zannetmesini sağlıyordu. Bu şekilde ücretsiz görüşmeler yaparak, bir makine sistemine girip, kendisine ilk menfaati sağlayan kişi olarak kabul edilir. Bu yaptığı işleme o günlerde, günümüzde telefon hackleme[32] manasına gelen phreaking denilmekteydi.

Pennsylvania Demiryolu Merkez Şirketinin bilgisayarlarına yapılan yetkisiz müdahale sonucu, New York - Pennsylvania demiryolu hattındaki trenlerin rotasından sapmış ve her seferinde yaklaşık 60.000 $'lık zarara meydana gelmiştir.

1973

New York's Dime Yatırım Bankasındaki veznedar, 2 milyon $'ın üzerindeki parayı bilgisayar kullanarak zimmetine geçirdi.

1981

Kaptan Zap olarak bilinen Ian Murphy, bilişim suçundan dolayı mahkum edilen ilk suçludur. Murphy AT&T bilgisayarlarına sızarak, indirimli tarife saatlerini değiştirerek milyonlarca AT&T şirketi müşterisinin telefon faturalarının daha fazla gelmesine sebep olmuştur.

1982

---

[31] http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html (Erişim tarihi: 25.12.2014)

[32] Hack: sistemlerin doğasından kaynaklı açıklardan faydalanılarak sisteme sızılmasıdır.

Elk Cloner, AppleII boot virüsü[33] yazıldı.

1986

Ms-Dos[34]'u etkileyen ve oluşturulan en eski virüs olduğu düşünülen Pakistani Brain virüsü IBM bilgisayarlarını bulaştı.

1988

Kevin Mitnick, MCI ile DEC şirketlerinin güvenlik ile ilgili e-postaları gizlice izlemiştir ve bu yüzden 1 yıllık mahkumiyet sürdürmüştür.

Kevin Poulsen telefonlara müdahale etmekle suçlanır ve yakalanıncaya dek 17 ay kaçar.

Chicago Birinci Ulusal Bankası 70 milyon $'lık bilişim yoluyla hırsızlık olayının mağduru olur.

Cornell Üniversitesi'nden mezun olan ve NSA'de çalışan bir şef bilim adamının oğlu olan Robert T. Morris, Jr., ARPANET'e kendini çoğaltan bir solucan[35] (the Morris Worm) yollayarak 6000 bağlı bilgisayara yayılarak hükümetin ve üniversitelerin sistemini yavaşlatmıştır. 3 yıl hapis cezası ve 10.000 $ para cezasına çarptırılmıştır.

1989

İlk büyük ölçekli dolandırıcılık olayı soruşturması görüldü. AIDS virüsü ile ilgili test bahanesiyle kullanıcıların farkında olmadan indirdiği virüs, 500 $ ödememeleri halinde bilgisayarlarındaki tüm verilerin silineceğinden bahisle tehdit ediyordu.

Batı Almanya'daki hackerlar Amerika Birleşik Devletleri'nin kurumsal bilgisayarlarına sızarak işletim sistemi kodlarını KGB'ye satmaktan dolayı tutuklandı.

1990

[33]Virüs: zarar vermek amacıyla kendini programlara kopyalayan, kendini çoğaltan ve kendi çalışabilen yazılım.

[34]Ms-dos: Microsoft'un disk işletim sistemi (Microsoft-Disk Operating System).

[35]Solucan (worm): Sistemde kendi kendini çoğaltıp, çok geniş şekilde yayılabilen zararlı yazılım.

Legion of Doom ve Masters of Deception isimli hacker grupları telefon parazitleme, çağrıları görüntüleme, birbirlerinin kişisel bilgisayarlarına yetkisiz girme konularında online savaşa başladılar.

2. Dönem - 1991- 2000

1991

Kevin Poulsen askeri sırları satmaktan yakalandı.

1992

Dark Avenger, ilk polimorfik[36] virüsü saldı.

1993

Bir radyo arama yarışmasında, Kevin Poulsen ve arkadaşları telefon hatlarını kitleyerek yarışmaya kendilerinden başka kimsenin katılmasına müsaade etmediler. Bu sayede 2 Porsche, deniz turu ve 20.000 $ kazandılar.

1994

Data-Stream lakaplı 16 yaşındaki genç, Kore Atomik Araştırmalar Enstitüsü'ne, NASA'ya ve bazı ABD kurumlarına girmekten dolayı Birleşik Krallık'ta tutuklandı.

Aum Shinri Kyo tarikatının beş üyesi Mitsubishi Ağır Sanayi'nin ana bilgisayarına sızarak çok miktarda hassas veriyi çaldı.

1995

Rus Crackerları[37] Citibank'tan 10 milyon $ çaldılar. Çete lideri Vladimir Levin, paranın Finlandiya ve İsrail'e aktarılması için kendi laptopunu kullandığı tespit edildi. ABD'de yargılanıp 3 yıl ceza evinde yattı ancak bu paradan sadece 400.000 $'ı kurtarılabildi.

[36]Polimorfik: biçim değiştirerek tespit edilmeyi zorlaştıran.

[37]Crack: sistemlerin güvenlik duvarları veya şifreleri kırılarak zarar verilmesi eylemi.

Fransa Savunma Bakanlığı, uçak gemilerine ve denizaltılarına ait akustik kodların hackerlar tarafından çalındığını kabul etti.

Hackerlar federal internet sitelerini tahrif ettiler.

Macro virüsü ortaya çıktı.

Kevin Mitnik kredi kartı bilgilerini çalmaktan dolayı tekrar tutuklandı. Bilişim dolandırıcılığından ve Motorola ve SUN şirketlerinin verilerini izinsiz olarak almaktan dolayı 4 sene hapishanede kaldı.

1996

Kanadalı hackerlar, Kanadalı Tv şirketi olan CBC'ye girdi.

ABD Genel Muhasebe Ofisi, hackerların 1995 yılında Savunma Bakanlığı'na 250.000 saldırı olduğunu ve bunların yaklaşık %65'inin başarılı olduğunu açıkladı.

1997

Alman Kaos Bilgisayar Kulübü, Microsoft'un internet yazılımına ve mali yönetim programı olan Quicken'e girmenin ve hesap sahipleriyle bankaların haberleri olmaksızın yetkisiz para transferinin yapılabileceğini iddia etti.

FBI'ın Ulusal Bilgisayar Suçları şirketlerin %85'inin hacklendiğini ve bunların çoğunun haberi bile olmadığını rapor etti.

1998

The Dead Cow'un Tarikatı isimli hack grubu, Back Orifice at Defcon isimli Truva atı[38] programını saldı.

Timothy Lloyd, Omega Mühendislik şirketinin ağına mantık bombası[39] yerleştirerek milyonluk zarara yol açmakla suçlandı.

---

[38]Truva atı (trojan): iyi niyetli bir program gibi gözüken ya da onun için gizlenerek sisteme sızmaya çalışan zararlı yazılım.

[39]Mantık bombası (logic bomb): belirli değişkenleri takip ederek zamanı geldiğinde sistemde yıkıcı etkiler meydana getiren zararlı yazılım.

Hackerlar, New York Times'ın internet sitesinin adını HFG (Hacking for Girlies) olarak değiştirdi.

Basra Körfezi'ndeki tansiyonun yükseldiği dönemde, hackerlar Pentagon'un gizli olmayan bilgisayarlarına girerek yazılım programlarını çaldı.

L0pht isimli hacker grubu Senato'ya ulusal çapta internet erişiminin 30 dakikadan daha az sürede kapatılabileceğine dair ifade verdi.

1999

The Melissa solucanı salındı ve o güne kadarki en fazla zarar veren zararlı yazılım oldu.

ABD Savunma Bakanlığı günde 60 - 80 arası günlük saldırı aldığını onayladı.

Kevin Mitnick 1995'ten beri bilgisayar dolandırıcılığından alıkonuldu, savunma anlaşması imzaladı.

CIH virüsü dünya genelinde bilgisayar kullanıcılarını etkiledi. Sayı olarak the Melissa'dan azdı ancak CIH harddisklerin üzerine yazma ve onun içindeki her şeyi silme amaçlıydı.

David Smith, the Melissa virüsünü yazmaktan ve yaymaktan ötürü suçlu bulundu. Virüs yazmaktan dolayı ceza alan ilk insan olmuştur.

2000

Rus Crackerları, CD Universe isimli müzik dağıtım şirketini binlerce müşterisinin kredi kartı bilgileri yaymakla tehdit ederek 100.000 $ istedi.

Barry Schlossberg nam-ı diğer Lou Cipher, sunduğu Rus Hackerları yakalamaya çalışma hizmetinden dolayı CD Universe şirketinden 1.4 milyon $ aldı.

Mafia Boy lakaplı hacker tarafından gerçekleştirilen DoS[40] ataklar, ebay, Yahoo gibi diğer popüler sitelerin geçici olarak servis dışı kalmasına ve bunun sonucunda ciddi finansal zararlara uğramasına sebep olmuştur.

Pakistan ve Ortadoğu'daki aktivistler filistin ve Kaşmir'deki operasyonları protesto etmek amacıyla Hindistan ve İsrail hükümetlerine ait web sitelerinin ana sayfalarını değiştirmişlerdir.

Hackerlar, Microsoft'un şirket ağına girerek Windows'un ve Office'in son versiyonlarının kaynak kodlarını elde etmişlerdir.

Yahoo, eBay, CNN.com, Amazon.com, Buy.com, ZDNet, E-Trade ve diğer benzer sitelere Dağınık DoS[41] atakları düzenlendi.

"I Love You" virüsü etkilenmiş tüm bilgisayarların rehberindeki kişilere göndererek hızla yayılmıştır.

3. Dönem - 2001 - 2005

2001

Microsoft, bu yıl alan adı sunucularına yönelik yeni bir saldırı türüne maruz kaldı. DoS atak şeklinde olan bu saldırıda Microsoft internet sitelerinin DNS[42] yolunun bozulması sağlanmıştır. Bu saldırı saatler içinde tespit edilse de, milyonlarca kullanıcının iki gün boyunca sitelere erişimi engellenmişti.

L10 solucanının Bind[43]'in eski versiyonlarına saldırılar yapabildiği keşfedildi.

Hollandalı Cracker, Anna Kournikova virüsünü saldılar. Bu virüs, Rus Tenisçinin resimlerinin açılacağını vaad ederek birçok zararlı yazılımı kullanıcının bilgisayarına enjekte ediyordu.

---

[40]DoS (denial of service) atak: Sunucuya çok fazla istek göndererek kapasitesini aşmasına sebep olması bunun sonucunda sitemin işlemez hale gelmesi saldırısı.

[41]DDoS (distrubuted denial of service atak): DoS atağın birden fazla noktadan gerçekleştirilmesidir. Daha etkilidir, tespiti daha zordur.

[42]DNS (Domain Name System): Alan adı sistemi, ağ sistemini bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan sistemdir.

[43]Linux ve Unix işletim sistemi tabanlı bir alan adı sunucu yazılımı.

FBI Ajanı Robert Hanssen, bilgisayar yeteneklerinin kullanarak Rusya için casusluk yapmak ile suçlandı.

Code Red isimli ilk polimorfik solucan on binlerce bilgisayarı etkiledi.

Çin ve Amerika ilişkilerindeki yükselen tansiyondan dolayı, Çinli ve Amerikalı Hackerlar internet üzerinden tahrifat savaşına giriştiler.

Rus programcısı Dmitry Sklyrov dijital telif haklarını ihlal etmekten tutuklanan ilk kişi oldu.

Napster[44], kayıt şirketlerinin ve Metallica'nın yasal mücadelelerinin ardından kapandı.

Avrupa Birliği, hazırladığı Amerika Birleşik Devletleri, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda tarafından radyo, telefon ve internet bağlantıları üzerinden casusluk maksatlı kullanıldığı iddia edilen Echelon sitemine ilişkin rapor hazırladı. Bunun anlamı askeri ve savunma kullanımının yanı sıra, insanların özel hayatına çok büyük bir müdahalenin olduğu şüphesi vardır.

2002

Bir Amerikan yatırım şirketi olan UBS PaineWebber'ın sistem yöneticisi olan Roger Duronio, tahrifat ve tadilatıyla 3 Milyon dolardan fazla zarara sebep olan mantık bombası yazmıştır.

Klez.H solucanı etkilediği bilgisayar sayısıyla en büyük zararlı yazılım olmuştur; ancak verdiği maddi zarar çok değildir.

Shadowcrew'in internet sitesi kişisel bilgilerin dağıtıldığı forum sitesi olarak kuruldu.

2003

Ms SQL[45] sunucularını hedef alan SQL Slammer en hızlı yayılan solucan olarak tarihe geçti.

[44]Napster: internet üzerinden diğer kullanıcılarla müzik parçaları paylaşmaya yarayan program.

ABD, Kazakistan crackerlarını Bloomberg LP şirketinin bilgisayarlarına girip menfaat sağlamaya çalışmaktan suçladı.

Viewsonic şirketinin eski çalışanı şirketin bilgisayarlarını hackleyip, verileri silmekten dolayı tutuklandı.

MS Blaster[46] solucanı ve varyantları salındı. Microsoft şirketi kendi sitemlerine yönelik bu solucanı yazanların her birine 250.000 $ tazminat talep etti.

Bir solucan Ohio'da bulunan nükleer santralin kritik düzeydeki güvenlik sistemini işlemez hale getirdi.

İki kişi Michigan'da bulunan Lowe marketlerinin kablosuz ağına girerek kredi kart bilgilerini çaldı.

2004

Brian Salcedo isimli kişi Lowe's Home Improvement Stores isimli işyerini hacklemek ve müşterilerin kredi karı bilgilerini çalmaya teşebbüs etmekten 9 yıl hapis cezası aldı.

Şubat ayında MyDoom isimli solucanın farklı varyantları Microsoft başta olmak üzere NetSky, SCO, Bagel gibi şirketlere DoS atak gerçekleştirmek üzere salındı.

Amerikan Gizli Servisi Firewall isimli operasyonda ShadowCrew internet sitesini kontrolünü ele geçirmiş ve 8 eyalet ve 6 farklı ülkeden toplam 28 kişiyi ABD'yi dolandırmaya çalışmaktan tutuklanmıştır. Aynı operasyonda Nicolas Jacobsen T-Mobile şirketinin bilgisayar sistemini hacklemekten ve Gizli Servise ait dökümanları açığa çıkarıp, bir ajana postalamaktan suçlanmıştır.

2005

Paris Hilton'un T-Mobile cep telefonu hacklenmiş ve fotoğrafları, ünlülerin telefon numaraları internette yayınlanmıştır.

---

[45]SQL (Structured Query Language): yapılandırılmış Sorgu Dili, bir veri tabanı yönetim sistemi.

[46]MS Blaster kelime anlamı, 'Microsoft İmha Edicisi' olarak çevrilebilir.

Choicepoint şirketi meşru işadamları gibi görünen hırsızların sistemlerine erişerek 145 bin tüketiciye ait içinde kredi kartı bilgileri ve sosyal güvenlik numaralarının bulunduğu kayıtları ele geçirdiklerini açıkladı.

Bank of America 'dan 1,2 Milyon isim ve sosyal güvenlik numarası çalındı.

Juju Jiang, banka hesaplarına erişim için gizli bilgileri elde etmek üzere keylogger[47] yüklemekten dolayı 27 ay hapis cezası aldı.

LexisNexis isimli şirket mart ayında 32 bin insanın Sosyal Güvenlik numaralarını ve şifrelerinin hacklenerek ele geçirildiğini duyurdu.

Cisco sitesindeki açılanmayan güvenlik sorunundan dolayı kullanıcılarını küresel olarak şifrelerini sıfırlamaya zorladı.

Mart ayında DSW/Retail Ventures isimli şirketten 100 bin, Boston College'den ise 120 bin hesap hacklendi.

BJ's Wholesale Club'a ait 40 bin kredi kartı bilgisi taşeronluk yapan IBM şirketinden çalındı.

LexisNexis şirketinden nisan ayında ise 280 bin hesap bilgisi daha çalındı.

Nisan ayında DSW/Retail Ventures şirketinden 1,3 milyon daha hesap çalındı.

Wachovia/Bank of America/PNC Financial Group/ Commerce Bancorp şirketlerinden 670 bin hesap bilgisi çalındı.

Myspace'teki The Samy solucanı herkesi Samy'nin arkadaşı yaptı.

CardSystems Solutions isimli kredi kartı işlemi şirketi hackerların virüs yerleştirdiğini ve 14 milyon kredi kartına eriştiklerini kabul etti.

Mart ayında Tıfts Üniversitesi'nden 106 Bin hesap, Haziran ayında Hawaii Üniversitesi'nden 150 bin ve Connecticut Üniversitesi'nden 72 bin hesap, Temmuz

[47]Keylogger: hedef kullanıcının bilgisayarı ile yaptığı hareketleri kayıt altına alan ve faile gönderebilen zararlı yazılım veya donanım.

ayında Güney Kaliforniya Üniversitesi'nden 270 bin hesap ve Ağustos ayında Utah Üniversitesi'nden 100 bin hesap hacklenerek ele geçirildi.

US Air Force'un 33.300 hesabı hacklendi.

Zotob Solucanı, Windows 2000 kullanan bilgisayarlara saldırdı.

Microsoft, Spam[48] Kralı Scott Richter'den 7 milyon $ ödeme ve gelecekte spam işlemine son verilmesi kararı kazandı.

Guidance Software şirketinin internet sitesine yapılan saldırı sonucu 3.800 müşterinin kredi kartı bilgisi çalındı.

Titan Rain kod adlı Çin siber casusluk şebekesi, Birleşik Devletlerin askeri üslerini, savunma yüklenicilerini ve havacılık şirketlerini hackledi.

4. Dönem - 2006 - …

2006

Hackerlar, Department of Homeland Security'e ait bilgisayarlara erişerek, zararlı yazılım yüklemiş ve dosyaları bir Çin internet sitesine transfer ettiler.

Toplu e-posta göndericisi Snipermail.com'dan Scott Levine Acxiom isimli veri depolama şirketinden 1 milyardan fazla kişinin kayıtlarının çalmaktan 8 yıl hapis cezasına çarptırıldı.

Çalınan Boeing Laptopundan, 3600 çalışanın kişisel bilgileri yayınlandı.

Ohio Üniversitesi'nden 137 bin kişinin sosyal güvenlik numaraları çalındı.

Hackerlar, AT&T şirketinin online mağazasından DSL ekipmanları satın almış olan 20 bin müşteriye ait kredi kartı bilgilerini ve diğer kişisel bilgilerini çaldı.

[48]Spam: istenmeyen e-postalar.

Linden Lab isimli oyun şirketinin meşhur Second Life isimli oyununa ait veri tabanına erişilmiş ve kullanıcıların gerçek isimleri, iletişim bilgileri, şifreleri ile ödeme bilgileri ele geçirilmiştir.

Bir Gartner çalışmasına göre, 2006 yılında 1,5 milyon Amerikalı kimlik hırsızlığı kurbanı oldu. Bunun anlamı yaklaşık her iki saniyede yeni bir kişi mağdur oluyor.

2007

Ödeme servisi firması MoneyGram, sunucularına yapılan sızmalar sonucu 80 bin kişiye ait kişisel verilerinin açığa çıkarıldığını tüketicilerine bildirdi.

Nokia'nın Kanada internet sitesi XSS[49] atak yapılarak tahrif edildi.

Çin Hükümeti ve Ordusu Birleşik Devletler Pentagon'un bilgisayar ağı, İngiliz ve Alman kurumsal bilgisayarlarını hacklemekten dolayı suçlandı.

İçinde Polis Teşkilatı'nın, Maliye Bakanlığı'nın ve Parlementosu'nun da yer aldığı Estonya'nın çeşitli kurumsal internet sitelerine DoS atak gerçekleştirildi.

Monster.com ve diğer iş siteleri hacklendi ve çalınan bilgiler yayınlandı.

TD Ameritrade Şirketi, yetkili bir şirket bilgisayarına yapılan erişim sonucunda sahip oldukları 6,3 milyon müşteriye ait e-posta hesaplarının sızdığını bildirdi.

Amerikan Gizli Servisi, güvenlik danışmanı Max Ray Butler'ı ('Max Vision') CardersMarket isimli online kredi kartı sahteciliği ve kimlik hırsızlığı sitesini yönetmekten dolayı tutukladı.

Yer sağlayıcı[50] hizmeti sunan Layered Technology Şirketinin yardım masası işlevli yazılımındaki bilinen bir zayıflıktan dolayı içinde 6000 müşterisinin isimleri, adresleri, telefon numaraları ve e-posta adreslerinin bulunduğu bilgi sızıntısı meydana geldi.

Bir hacker sanal alışveriş sitesi eBay'ın kullanılmayan bir sistem yöneticisi fonksiyonundan yararlanarak, kullanıcıları engelledi ve satışları kapattı.

---

[49]XSS (Cross-site scripting): internet sitelerindeki skript kaynaklı açıklardan siteye sızılması.

[50]Yer sağlayıcı: İnternet ortamında, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir (5651 SK).

RBN[51] korumalı yer sağlayıcı hizmeti sunmaya başladı. Bu haklarında yasal mücadele olmasına rağmen yasadışı içerik barındıran siteleri bile kapsıyordu. Eylül ayında RBN sunucuları kullanılarak Bank of India'ya saldırı gerçekleştirildi.

Kanada'nın Pasaport başvuru sitesindeki hata, diğer insanların bilgilerini kullanarak pasaport başvurusu yapma imkanı sunuyordu.

Ünlü Rus zararlı yazılım çetesi olan RBN, SQL injection[52] kullanarak ABD'nin hükümet sitelerine girdi.

John Schiefer köle bilgisayar kullanarak en az 250 bin makineye yasadışı olarak yazılımı yüklediğini ve bu şekilde Windows kullanan kişilerin internet bankacılığı bilgilerini çaldığını kabul etti.

2008

İtalyan Bankası olan Banca Fideuram'ın giriş sayfası XSS kullanılarak değiştirildi.

Amerika Kayıt Enstitüsü Birliği'nin internet sitesi DoS saldırıya uğradı ve tahrif edildi.

CSRF[53] yöntemiyle Kore e-ticaret sitesi olan auction.co.kr hacklenmiş ve 18 milyon kullanıcıya ait veriler çalınmıştır.

MySpace ve Facebook'taki özel fotoğraflar URL manipülesi ile açık hale getirilebildi.

Hackerlar bir Amerikan alışveriş sitesi olan Hannaford'un müşterilerine ait 4,2 milyon kart bilgilerini ele geçirilmiş ve bu bilgiler 2000'in üzerinde dolandırıcılık olayında kullanılmıştır.

Pennsylvania Demokratik Önseçimlerinden hemen önce XSS kullanılarak Barack Obama'nın internet sitesini ziyaret edenler Hillary Clinton'un internet sitesine yönlendirildiler.

---

[51]RBN (Russian Businnes Network): çok yönlü bir Rus suç örgütü.

[52]SQL injection: sql ile hizmet sunan bir veri tabanına ek sql komutları göndererek gerçekleştirilen saldırı türüdür.

[53]CSRF (Cross-site request forgery): bu yöntemle kullanıcının internet sitesindeki yapmış olduğu manipüle ederek kullanıcının sitedeki yetkilerinden menfaat sağlamak veya istismar etmek.

ABD Kongresi tarafından desteklenen radyo yayımı ve iletişim kurumu olan Radio Free Europe (Özgür Avrupa Radyosu), DDoS saldırıya uğradı.

Kaynakça

Ahlqvist, Toni; Bäck, A., Halonen, M. ve Heinonen, S (2008). "Social media road maps exploring the futures triggered by social media". VTT Tiedotteita – Valtion Teknillinen Tutkimuskeskus (2454): 13. Retrieved 9 December 2012 aktaran http://en.wikipedia.org/wiki/Social_media (Erişim tarihi: 23.07.2014)

Akbulut, Bozdağan B. (2000). Bilişim Suçları, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı*, Konya, Sayı: 1 Cilt: 8, 88-200.

Akıncı, H.; Alıç, E. A. ve Er C. (2004). Türk Ceza Kanunu ve Bilişim Suçları, Atamer Y. (Ed.), *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 157-277.

Akser, M. (2015). The Revolotion Will Be Hacktivated: Turkish Marxist Hacker Groups. *Digital Transformaitons in Turkey*. (Ed: B. Akdenizli) Maryland, ABD: Lexington Books.

Alaca, B. (2008). Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle) (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Atalıç Taş, K. (2010). Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi Çukurova Üniversitesi: Sağlık Bilimleri Enstitüsü Adana: Yayımlanmamış Yüksek Lisans Tezi.

Aydın, E. D. (1992). *Bilişim Suçları ve Hukukuna Giriş*, Ankara: Doruk Yayınları.

Aydoğan, F. (2010). İkinci Medya Çağı'nda Gözetim ile Kamusal Alan Paradoksunda İnternet, *İkinci Medya Çağında İnternet*, (Ed: F. Aydoğan ve A. Akyüz) İstanbul, Alfa Yayınları.

Balaban, E., *Bilgi Toplumu* http://www.erdalbalaban.com/index.php?option=com_content&view=article&id=73:bilgitoplumu&catid=35:blogsayfam&Itemid=67 (Erişim tarihi: 15.04.2011)

Başoğlu, K. B. (2008). *Teknolojiye Boyun Eğmeyin*, Bilişim Suçlarına Genel Bakış 1. Sempozyum, Ankara.

Batır, K. (2005). İnternet ve Hukuk. *İnternet, Toplum, Kültür* (Ed: M. Binark ve B. Kılıçbay) Ankara: Epos Yayınları 156-176.

Baym, N. K. (2010). İzleyin ve Bağlanın: Pembe Diziler, Takipçileri ve Sanal Topluluklar *Sosyoloji* (Ed: A. Giddens) 401-410.

Berber Keser, L. (2004). *Adli Bilişim* (Computer Forensic), İstanbul: Yetkin Yayınları.

Binark, M. (2009). *Toplumsal Paylaşım Ağı Facebook: "Görülüyorum Öyleyse Varım"*, İstanbul: Kalkedon Yayınları.

Boğa, U. (2011). Bilişim Suçlarıyla Mücadele Yöntemleri, Yayımlanmamış Uzmanlık Tezi, Ankara: Radyo ve Televizyon Üst Kurulu.

Bozkurt, V. (1999). Sanal Cemaatler *Birikim Dergisi* (127) 65-72.

Bozkurt, V. (2000). Gözetim Toplumu ve İnternet *Birikim Dergisi* (127) http://www.birikimdergisi.com/birikim-yazi/2499/gozetim-ve-internet-ozel-yasamin-sonu-mu#.VkzAynYrJdg (Erişim tarihi: 18.11.2015).

Castells, M. (2013). *Ağ Toplumunun Yükselişi* (3. Baskı) (Çev: E. Kılıç) İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Cerf, V., Leiner, B. M., Clark, D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts L. ve Wolff S,. (2009). Brief History of the Internet. http://www.isoc.org/internet/history/brief.shtml (Erişim tarihi: 17.05.2015)

Chik, W. B. (2010). *Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore*. http://www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Erişim tarihi: 18.04.2015)

Cohen, S. (2014). Kriminolojinin Başarısızlıkları. *Ceza Hukuku ve Kriminoloji Dergisi*, (Çev: T. Topçuoğlu) 2(1-2), 269-280.

Çekiç, B. (2006). İnternet Aracılığı İle İşlenen Suçlar Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Çetin, M. ve Bel, A. (2014). Geleneksel medya Gündeminin Belirlenmesinde Sosyal Medyanın Rolü, *İletişim Kuram ve Araştırma Dergisi* Gazi Üniversitesi Hakemli Elektronik Dergisi.

Çoban, B. (2014). Sosyal Medya D\evrimi *Sosyal Medya Devrimi* İstanbul: Su Yayınları 9-21.

Çubukçu, B. (2000) *Teknoloji ve Endüstriyel İlişkiler*, http://antrak.org.tr/index.php?option=com_content&task=view&id=991 (Erişim tarihi: 16.10.2014)

Değirmenci O. (2002). Bilişim Suçları (Yayımlanmamış Yüksek Lisans Tezi), İstanbul, Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Değirmenci, A. C. ve Yenidünya, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul, Legal Yayıncılık.

Dilek, H. İ. (2007). Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri Dicle Üniversitesi Sosyal Bilimler Üniversitesi. Diyarbakır: Yayımlanmamış Yüksek Lisans Tezi.

Dülger, M. V. (2004). *Bilişim suçları*, Ankara: Seçkin Yayınları.

Dolu, O. (2010). *Suç Teorileri* Seçkin Yayınları: Ankara.

Dönmezer, S. (1981). *Kriminoloji*, İstanbul Üniversitesi Yayını, İstanbul, 62.

Durmaz Ş. (2005). Bilişim Suçlarının Sosyolojik Analizi – Gazi Üniversitesi Sosyal Bilimler Enstitüsü Ankara: Yayımlanmamış Yüksek Lisans Tezi.

Eralp, Ö. (2007). *Hukukçular İçin Bilişim Terimleri Sözlüğü* Avbil Yayınları: Ankara.

Eralp, Ö. (2012). *İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu*, Eralp Kitap: Ankara

Eriş, U. (2011) Türkiye'de Hacker Kültürü *Gümüşhane Üniversitesi İletişim Dergisi* 1 (2) http://egifder.gumushane.edu.tr/article/view/5000006422/5000006851 (Erişim tarihi: 20.09.2015).

Erkul, R. E. (2009). Sosyal Medya Araçlarının (Web 2.0) Kamu Hizmetleri ve Uygulamalarında Kullanılabilirliği Türkiye Bilişim Derneği Dergisi, Sayı 116, Aralık 2009, 96-101.

Gözüşirin, M. (2011). 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi, Kara Harp Okulu, Savunma Bilimleri Enstitüsü Ankara: Yayımlanmamış Yüksek Lisans Tezi.

Imhof, R. (2010). Cyber Crime and Telecommunications Law. Yüksek Lisans Tezi. Rochester Institute of Technology.

Irak, D. ve Yazıcıoğlu, O. (2012). *Türkiye ve Sosyal Medya* İstanbul: Okuyanus Yayınları, 18.

İlbaş, Ç. (2009). Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi, Başkent Üniversitesi, Fen Bilimleri Enstitüsü Ankara: Yayımlanmamış Yüksek Lisans Tezi.

Jordan, T. ve Taylor, P. (2010). Bilgisayar Korsanları Sosyolojisi *Sosyoloji* (Ed: A. Giddens) İstanbul: Say Yayınları, 221-239.

Kara, İ. , Sönmez, Ü. , Kaya, G. ve Kaymakçıoğlu, Ö. (2014). 5271 sayılı Ceza Muhakemesi Kanununun 134 üncü Maddesinin Uygulama Yönünden Değerlendirilmesi *Kazancı Hakemli Hukuk Dergisi*, Bahçeşehir Üniversitesi 2014; 73-81.

Kara, İ. ve Kaya, G. (2015). Türkiye'de Bilişim Alanında İşlenen Suçların Uygulama Bakımından Hukuki Boyutunun Değerlendirilmesi *Kazancı Hakemli Hukuk Dergisi* Bahçeşehir Üniversitesi 154-168.

Kara, İ. (2015a). Bilişim Sistemleri Aracılığıyla İşlenen; "Çocuk Cinsel İstismarı Suçu" *Hukuk ve Hayat Dergisi* 2015; Şubat Sayısı.

Kara, İ. (2015b). 5237 sayılı Türk Kanununun 243-246 ıncı Maddesinin Uygulama Yönünden Değerlendirilmesi *Kazancı Hakemli Hukuk Dergisi* Bahçeşehir Üniversitesi 2015 Nisan; 1-7.

Kara, İ. ve Şahin, E. (2015). Türkiye'de Sanal Ortamda İşlenen Suçların Değerlendirilmesi *Kazancı Hakemli Hukuk Dergisi* Bahçeşehir Üniversitesi 2015 Haziran, 165-170

Kara, T. ve Özgen E. (2012). *Sosyal Medya*. İstanbul: Beta Yayınları.

Karagülmez, A. (2005). *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara: Seçkin Yayınları

Karagülmez, A. (2009). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, (2'inci Baskı), Ankara: Seçkin Yayınları.

Karasar, N. (2005). *Bilimsel Araştırma Yöntemi: Kavramlar, İlkeler, Teknikler*. Ankara: Nobel Yayın Dağıtım.

Kaplan, A. ve Michael, M. (2010). "Users of the world, unite! The challenges and opportunities of social media". Business Horizons 53 (1). s. 61. doi:10.1016/j.bushor.2009.09.003. aktaran http://en.wikipedia.org/wiki/Social_media (Erişim tarihi: 23.07.2014)

Kaplan, A. ve Haenlein, M. (2009). The fairyland of Second Life: About virtual social worlds and how to use them, *Business Horizons*, 52(6), 563-572.

Kardaş, Ü. (2003). Bilişim Dünyası ve Hukuk, *Karizma Dergisi*, Ankara: Ocak Şubat Mart Sayısı, 7-19.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*, Ankara, Adalet Yayınevi.

Kızıltan, B. (2006). 5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Klieber, P. (2009). *Document Classification Through Data Mining Social Media Networks*, 8 https://www.researchgate.net/publication/287406899_Sports_Marketing_Social_Media, (Erişim tarihi: 10.04.2015).

Kurt, L. (2005). *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması*, Ankara, Seçkin Yayınları.

Lerman, K. (2007). *Social information processing in news aggregation. IEEE Internet Computing*, 16-28.

Murray, C. (2008) "Schools and Social Networking: Fear or Education?", *Synergy Perspectives*: Local, Vol. 6 Issue 1.

Onat, F., Aşman Ö. ve Kılıç A., (2008). Sosyal Ağ Sitelerinin Reklam Ve Halkla İlişkiler Ortamları Olarak Değerlendirilmesi *Journal of Yasar University*, 3(9), 1111-1143.

Özel, C. (2004). Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, Atamer Y. (Ed.), *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları no: 51, 341-363.

Özdilek, A. O. (2002). *İnternet ve Hukuk*, Ankara, Papatya Yayıncılık.

Önemli, M. (2004). İnternet Suçlarıyla Mücadele Yöntemleri, TODAİE Yüksek lisans tezi, Ankara, 29.

Özberk, V. Ö. (2002). " İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Soruları", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, İzmir, Sayı: 1, Cilt: 4, 101-159.

Öztürk, M. İ., (2007). Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Özutku, F.; Küçükyılmaz, M. M.; Çopur, H.; İlter, K.; Sığın, İ. Ve Arı, Y. (2014). *Sosyal Medya'nın ABC'si* İstanbul: Alfa Yayınları

Polat, O. (2002). *Çocuk ve Şiddet*. İstanbul: Der Yayınları, 85-97.

Polat, O. (2004). *Kriminioloji ve Kriminalistik Üzerine Notlar* Ankara: Seçkin Yayınları

Seymour, M. M. (2013). An Explanatory Model Of Motivation For Cyber-Attacks Drawn From Criminological Theoriesons Yüksek Lisans Tezi. Maryland, ABD: University of Maryland

Sınar, H. (2001). *İnternet ve Ceza Hukuku*, İstanbul: Beta Basım.

Sokullu-Akıncı, R. F. (2011). *Kriminoloji* İstanbul: Beta Basım.

Subaşı, N. (2005). İnternet ve Sanal Cemaat Tartışmaları. *İnternet, Toplum, Kültür* (Ed: M. Binark ve B. Kılıçbay) Ankara: Epos Yayınları 106-117.

Swingewood, A. (1998). *Sosyolojik Düşüncenin Kısa Tarihi* (Çev: O. Akınhay) Ankara: Bilim ve Sanat Yayınları.

Şehitoğlu, O. T. (2005). Bilgisayar ve Ağ üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal ve Güvenlik Boyutu (Yayımlanmamış Yüksek Lisans Tezi), Ankara, Kara Harp Okulu Komutanlığı Savunma Bilimleri Enstitüsü.

Tanşu, O. (2004). Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler, (Ed: Y. Atamer), *İnternet ve Hukuk*, İstanbul: Bilgi Üniversitesi Yayınları No: 51, 139-157.

Taş, O. (2007). Şebeke Toplumunda Direniş: Hacker Kültürü ve Teknoloji Etiği. *Yeni Medya Çalışmaları* (Ed: M. Binark) Ankara: Dipnot Yayınları 309-344

Tepe, İ. (2009). *Modern Ceza Hukuku Teorisinde İnternet ve İnternet Suçluluğunun Konumu*, (Ed: V. Ö. Özbek), *Ceza Hukuku Dergisi*, Ankara: Seçkin Yayınları, Yıl:4 Sayı:9, 259-273.

Tuncer, E. (2014). *Sosyal Medya İmaratorluğu - Patron* Akis Yayınları: İstanbul 15-17

Tutar, H. (2000). Küreselleşme Sürecinde İşletme Yönetimi, *Hayat Dergisi* İstanbul.

Topaloğlu, M. (1997). *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması*, İstanbul: Altan Matbaacılık,

Topaloğlu, T. (2014). *Adli Bilişim ve Elektronik Deliller* (Ed: H. Çakır ve M. S. Kılıç) Ankara: Seçkin Yayıncılık.

Uçkan, Ö. ve Beceni, Y. (2004). *Bilişim-İletişim Teknolojileri ve Ceza Hukuku*, (Ed: Y. Atamer), *İnternet ve Hukuk*, İstanbul: Bilgi Üniversitesi Yayınları No: 51, 2004, 363-433.

Yaycı, E. (2007). Bilişim Suçları (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile*, İstanbul: Alfa Basım Yayım Dağıtım

Ziyalar, N. (1999) *Çocuk istismarı ve ihmalinin önlenmesi*. Çocuk Forumu 2: 31-33.

İnternet Kaynakları

Gercke, M. (2009), Europe's Legal Approaches to Cybercirime. http://www.springerlink.com/index/f76171880840794.pdf (Erişim tarihi: 17.09.2014

Facebokk, Instagram, Whatsapp İstatistikleri (Erişim tarihi: 17.05.2015) http://pro.webrazzi.com

IAS Türkiye internet ölçülmesi araştırması/Yapısal Çalışması (Temmuz 2013), http://pro.webrazzi.com

Özgenç, İ., Yeni TCK'nun Hazırlanmasında Esas Alınan Suç Teorisi (2011), www.ceza-bb.adalet.gov.tr/makale/pp2.ppt

Sosyal Medya (14.01.2010), http://www.kurumsalhaberler.com/pr/sosyal-medya-nedir.aspx

Social Network Sites: Definition, History, and Scholarship (13.01.2010), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Sosyal Medya (14.01.2010), http://www.kurumsalhaberler.com/pr/sosyal-medya-nedir.aspx

Sosyal Medya (14.01.2010), http://tr.wikipedia.org/wiki/Sosyal_medya

Socialbakers-2015, http://pro.webrazzi.com

Tekin, M. ve Çiçek, E. (2006) Bilgi Çağında Bilgi Toplumu ve Bilgi Ekonomisi. http://www.bilgitoplumu. blogspot.com/ (Erişim tarihi: 05.04.2015)

Türk Dil Kurumu Resmî İnternet Sitesi http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.56775c57b3a548.07423531 (Erişim tarihi: 21.12.2015)

Türkiye Cumhuriyeti Gençlik ve Spor Bakanlığı- Gençlik ve Sosyal Medya Araştırması, 2013. http://pro.webrazzi.com

Türkiye'de Sosyal Ağların Yeri ve Sosyal Medyaya Bakış http://inettr.org.tr/inetconf14/bildiri/61.doc (14.01.2010).

Türkiye İstatistik Kurumu (TUİK) http://pro.webrazzi.com

Türksat http://pro.webrazzi.com.

UNESCO, (2004) *The COE International Convention on Cybercrime Before Its Entry Into Force*, UNESCO e-bülten Ocak-Mart 2004 http://portal.unesco.org/culture/en/files/19556/11515912361coe_e.pdf/coe_e.pdf (Erişim tarihi: 17.12.2015)

We are Social-Digital, Social&Mobile-2015, http://pro.webrazzi.com

http://www.alexa.com/topsites (Erişim tarihi: 25.12.2014)

http://www.statisticbrain.com/facebook-statistics/ (Erişim tarihi: 25.12.2014)

http://tr.wikipedia.org/wiki/Facebook#cite_note-5 (Erişim tarihi: 25.12.2014)

http://www.statisticbrain.com/twitter-statistics/ (Erişim tarihi: 25.12.2014)

http://tr.wikipedia.org/wiki/Vikipedi (Erişim tarihi: 06.09.2014)

http://www.socialmediatr.com/blog/turkiyede-internetin-kisa-tarihi/ (Erişim tarihi: 26.10.2014)

http://www.marketingturkiye.com.tr/index.php?option=com_content&view=article&id=7403:acarer-qtuerkiyede-55-milyon-internet-kullancs-varq&catid=65:guencel-haberler&Itemid=160 (Erişim tarihi: 26.10.2014)

http://www.danah.org/papers/JCMCIntro.pdf (Erişim tarihi: 06.09.2014)

http://www.asayis.pol.tr/Sayfalar/bilisim_suclari.aspx (Erişim tarihi: 17.01.2015)

http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html (Erişim tarihi: 25.12.2014)

http://www.asanet.org/about/presidents/Edwin_Sutherland.cfm (Erişim tarihi: 25.12.2014)

https://www.turkiye.gov.tr (Erişim tarihi: 25.12.2014)

http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609# hx3xD7usqjjM4WIT.97 (Erişim tarihi: 23.11.2015)

http://www.milliyet.com.tr/ilkokulda-yazilim-gelistirme-dersi/gundem/gundemdetay/18.11.2012/ 1628845/default.htm (Erişim tarihi: 23.11.2015)

http://www.ntv.com.tr/teknoloji/yazilim-dersi-ilkokulda-zorunlu-olacak,PS_7TVRy_EKYENQihpdJKQ (Erişim tarihi: 23.11.2015)

http://www.isoc.org/internet/history/brief.shtml (Erişim tarihi: 12.10.2014)