T. C.

İSTANBUL ÜNİVERSİTESİ - CERRAHPAŞA

ADLİ TIP ENSTİTÜSÜ

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ HIZIR ASLIYÜKSEK

BİLİŞİM SUÇLARININ BİLİRKİŞİLİK UYGULAMALARI YÖNÜNDEN DEĞERLENDİRİLMESİ

SOSYAL BİLİMLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

Avukat Nazlı Nur AKYOL ÇINAR

İSTANBUL, 2019

İstanbul, 11 Haziran 2019

İ.Ü.ADLİ TIP ENSTİTÜSÜ MÜDÜRLÜĞÜ
SOSYAL BİLİMLER ANABİLİM DALI BAŞKANLIĞINA

Lisansüstü Öğretim Yönetmeliğinin 36.maddesi uyarınca Enstitünüz Sosyal Bilimler Anabilim Dalı'nın yüksek lisans öğrencisi Nazlı Nur AKYOL ÇINAR'ın,

"Bilişim Suçları ve İnternet Aracılığıyla İşlenen Suçların Yasal Mevzuatımız ve Bilirkişilik Uygulamaları Yönünden Değerlendirilmesi"

Adlı tezi jürimizce tetkik edilmiş ve kendisine tez savunması yaptırılmıştır.

Yukarıda adı geçen tez başlığının **"Bilişim Suçlarının Bilirkişilik Uygulamaları Yönünden Değerlendirilmesi"** şeklinde değiştirilerek tezin ve tez savunmasının kabul edilmesine oy birliğiyle karar verilmiştir.

Prof. Dr. Ümit Naci GÜNDOĞMUŞ
Jüri Başkanı

Doç. Dr. Neylan ZİYALAR
Üye

Doç. Dr. Abdurrahman SAVAŞ
Üye

Dr. Öğr. Üyesi Hızır ASLIYÜKSEK
Danışmanı

Dr. Öğr. Üyesi Y. Tunç DEMİRCAN
Üye

ÖNSÖZ VE TEŞEKKÜR

Bilişim teknolojileri 20. yüzyılın ortalarından itibaren büyük bir hızla ekonomik ve sosyal hayat içerisine girmiştir. Süreç içerisinde günlük yaşam ve iş hayatını önemli ölçüde değiştirmiş; etkileri tüm insanlık kültürünü kapsayacak bir biçimde geniş yelpazede yaşanmıştır.

Bilişim ve internetin hayatın her alanında ortaya çıkan bu müdahalesinin yalnızca olumlu anlamda ilerleme ve gelişmeye yönelik olmadığı; bunun yanı sıra müeyyide ile sonuçlanacak kurallardan sapma eylemleri olarak niteleyebileceğimiz suç davranış ve yöntemleri yönünden de yeni alternatifler doğurduğu, böylelikle ortaya yeni suçlu ve mağdur profilleri çıkarttığı söylenmelidir. Bilişim suçları ve internet aracılığıyla işlenen suçlar bakımından adli tıp uygulamalarının etkinliğinin değerlendirilmesi, ihtiyaç duyulan yeni düzenlemelerin ortaya konulması, artan ve çeşitlenen suç tiplerinin tespiti ve mücadele önerilerinin sunulmasının adli sürecin isleyişine olumlu katkılar sağlayacağı değerlendirilmektedir.

Bu amaçla, adli bilişim pratiğindeki iyileştirme çabalarına bir nebze de olsa katkı sağlayabilmek hissiyat ve temennisiyle kaleme aldığım çalışmama desteğini esirgemeyen değerli hocamız İstanbul Üniversitesi Cerrahpaşa Adli Tıp Enstitüsü Müdürü Prof. Dr. Faruk Aşıcıoğlu'na ve çok değerli fikirleri ile bana yön veren danışmanım Dr. Öğretim Üyesi Hızır Aslıyüksek'e, yüksek lisans eğitimim süresince derslerine katıldığım İstanbul Üniversitesi Adli Tıp Enstitüsü'nün çok değerli öğretim üyelerine ve son olarak tezime sağladığı değerli katkılarından ötürü Araştırma Görevlisi Dr. Filiz Ekim Çevik'e saygı ve minnetlerimi sunarım.

Bu süreçte bana sonsuz destek veren, bilgisayar mühendisliği alanındaki tecrübelerini benimle paylaşan, her daim yanımda olan eşim Özgür Erdem Çınar'a, daha iyi ve başarılı bir insan olmam için beni varlıklarıyla motive eden sevgili çocuklarım Eren ve Doğa'ya, hayatımın her evresinde kararlarımın arkasında duran sevgili annem ve babama, ve son olarak; hayattayken öğrettikleriyle bana halen yol gösteren rahmetli dedem Kemal Akyol'a sonsuz sevgi, saygı ve minnetle.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLO DİZİNİ

KISALTMALAR DİZİNİ

ATK	Adli Tıp Kurumu
FİD	Fizik İhtisas Dairesi
ABİD	Adli Bilişim İhtisas Dairesi
CMK	Ceza Muhakemesi Kanunu
TCK	Türk Ceza Kanunu
ETCK	Eski Türk Ceza Kanunu
HUMK	Hukuk Usulü Muhakemeleri Kanunu
T.C.	Türkiye Cumhuriyeti
EGM	Emniyet Genel Müdürlüğü
JGK	Jandarma Genel Komutanlığı
VPN	Virtual Private Network
TCP	Transport Central Protocol
IP	Internet Protocol
CERN	European Organization For Nuclear Research
ARPA	Advanced Research Project Agency
TÜBİTAK	Türkiye Bilimsel Ve Teknolojik Araştırma Kurumu
ODTÜ	Orta Doğu Teknik Üniversitesi
WEB	World Wide Web
HTML	Hyper Text Mark Up Language
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
URL	Uniform Resource Locators
MSN	Microsoft Network
IRC	Internet Relay Chat

DNS	Domain Name System
DOS	Denial Of Service
LAN	Local Area Network
WAN	Wide Area Network
INTERNET	Interconnected Networks
CD	Compact Disc
DVD	Digital Versatile Disc
HDD	Hard Disc Drive
ATM	Automatic Teller Machine
FBI	Federal Bureau Of Investigation
CIA	Central Intelligence Agency
LTO	Linear Tape Tecnology
DLT	Distributed Ledger Tecnology
DAS	Direct Attached Storage
NAS	Network Attached Storage
SAN	Storage Area Network
FTK	Forensic Toolkit
ENCE	Encase Certified Examiner
CCE	Certified Computer Examiner
CCCI	Certified Computer Crime Investigator
CFCE	Certified Forensic Computer Examiner
CIFI	Computer Information Forensics Investigator
PCI	Peripheral Component Interconnect

ÖZET

Günümüz teknoloji dünyasında en hızlı ilerleme ve değişimi bilişim sistemlerinin kullanımında yaşamaktayız. Öyle ki içinde bulunduğumuz bu zaman diliminde, sanal dünyanın tüm insanlığın kaderini tek başına belirlemeye muktedir bir güç haline geldiğini gözlemlemekteyiz. Bu etkinin pek çok yüzü ve açısı olduğu bir gerçekse de, bizce varlığını en etkileyici bir şekilde insanlığın suç eylemlerini icrası yönünden hissettirmektedir ve gelecekte de maalesef şiddetini arttırarak hissettirmeye devam edecektir. Bu ilerlemeye karşı hızlı ve etkili bir biçimde önlemler alınması ve yaptırımlar getirilmesi zaruridir.

Çalışmamızda; bilişim suçları kapsamına; bilişim alanındaki suçlar, internete özgü eylemler ve internet aracılığıyla gerçekleştirilen eylemler dahil edilmiştir. Çalışmamızın genel bilgiler kısmında, öncelikle tanımlamalar yönünden açıklamalar yapmak yoluna gidilmiş; bilişim ve bilişim sistemleri kavramları açıklanarak bilişim alanında işlenen suçlara dair izahatlara yer verildikten sonra, internet kavram ve tarihçesine, ardından internete özgü eylemler ile internet aracılığıyla işlenen suçlar konularına değinilmiştir. Devamla, adli bilişim kavramı, çalışma alanları ve safhaları üzerine incelemelere yer verilmiş; mevzuatımızdaki adli bilişime dair düzenlemeler ile bilirkişilik uygulamaları irdelenmiştir.

Bu kapsamda; 2009 -2011 yılları arasında Adli Tıp Kurumu Fizik İhtisas Dairesi tarafından bilirkişilik hizmeti verilen dosyalar istatistik yöntemi kullanılmak suretiyle tek tek incelenmiştir. Özellikle suçun bu süreç içerisindeki artışı ve suçlu profili, suç tipinin teknik bilgi gerektirip gerektirmediği, işlenen suç tipi, ihlal edilen hak ve zarar

nevi, suçun işlendiği yer, suçta kullanılan materyal gibi bulgular yönünden bunların dağılımlarına dair tespitler ile verilen hizmete göre ekspertiz sayısı, dosyanın gönderildiği merci, dosyanın geldiği yer, hizmet verilip verilemediği ve gelen dosyalar için hizmet verilememe nedenine ilişkin daha çok bilirkişilik uygulamalarını ilgilendiren noktalara dair tespit ve değerlendirmeler yapılması amaçlanmıştır. Aynı zamanda adli bilişim alanındaki bilirkişilik hizmetleri yönünden uygulamada eksiklikler barındıran, iyileştirilmesi gereken hususlara işaret edilmeye çalışılmıştır.

Bu istatistiklere, Adli Tıp Kurumu Fizik İhtisas Dairesi'ne adli bilirkişilik hizmeti talebiyle 2012 – 2016 yılları arasında gönderilen dosyalara ait sayısal veriler ile 15 Temmuz 2016 darbe girişimi sonrası savcılık ve mahkemelerde adli bilişimle ilgili resmi bilirkişilik talebinin çok fazla artması nedeniyle kurulmuş olan Adli Tıp Kurumu Adli Bilişim İhtisas Dairesi'ne 2017-2018 yılları içerisinde gelen dosyalara ait sayısal veriler de çalışmamız kapsamına alınmıştır. Bu suretle; 2009 – 2018 yıllarını kapsayacak 10 yıllık bir sürece yayılan adli bilirkişilik talebindeki artışın tespit edilmesi amaçlanmıştır.

Temennimiz, çalışmamızın ortaya çıkardığı veriler ile anlamlı ve kayda değer sonuçlar sunabilmek, bilakis suç artışını göz önüne serebilmek ve özellikle bilirkişilik uygulamalarının iyileştirilmesi ve bu hizmetlerin sağlıklı olarak icra edilebilmesi için olmazsa olmaz gerekliliklerin tespiti ve temini yönünde fikir üretebilmeyi başarmaktır.

Anahtar Kelimeler: Bilişim Suçları, İnternet Suçları, Adli Bilişim, Bilirkişilik Uygulamaları, Adli Tıp Kurumu

ABSTRACT

In today's techology world, we're experiencing the fastest progress and change in the use of information systems. So we are observing that in this time of our existence, the virtual world has become a force capable of determining the fate of all mankind alone. Although this effect has many facets and angles, it makes us feel its presence most actively in the way of the criminal acts of humanity. In the future, unfortunately, it will continue to make the impression of increasing its severity. It is imperative to take precautions and sanctions quickly and effectively against this progress.

In our work; firstly, the concepts of computer and computer systems and the crimes committed in the field of information were explained. Then, explanations were made in terms of definitions and legal regulations. After the concept of internet and its elements were mentioned, crimes committed through internet were examined.

After evaluating the types of crime, the concept of forensic computing, has been examined on the fields of work and the stages of the thesis. The legislative informal arrangements and expertise practices in our legislation have been mentioned. In this context; the expert service files between the years 2009 -2011, which are given by The Council Of Forensic Medicine has examined by using statistical method. In particular, the increase in the crime in this process and criminal profile, whether the crime type requires technical knowledge, the type of crime, violated rights and losses, the place where the crime committed, such as the material used in the findings of the distribution, the number of appraisal, the authority to which the file was sent, whether the service could be provided and the reason for not being able to provide service were determined and evaluated. At the same time, it has been tried to point out the issues that need

improvement in the field of forensic practice. Numerical data belonging to the files submitted to The Council Of Forensic Medicine between 2012- 2016 for the request of forensic expertise were added to these statistics. In addition, due to the fact that the demand for official expertise on judicial informatics in the public prosecutor's offices and courts after the coup attempt on July 15, 2016; numerical data of expert files which are included in The Council Of Forensic Medicine Department in 2017-2018 were added. In this way; the aim of this study is to determine the increase in the demand for forensic expertise, which was last for a period of 10 years covering 2009 – 2018.

Our desire is to be able to provide meaningful results with the data that our work reveals, but also to be able to take into account the increase in crime, and in particular to improve the practice of expertise and to generate ideas for the identification and characterization of the essential requirements for healthy execution of these services.

Keywords: Cybercrime, Computer Forensics, Expert, Council of Forensic Medicine

1. GİRİŞ VE AMAÇ

Bilişim suçu ve internet aracılığıyla işlenen suç kavramları; özellikle internet kullanımının ve kullanıcılarının tahmin edilenin çok ötesine geçen bir büyüme göstermesi karşısında gerek Türkiye bağlamında gerekse uluslararası düzeyde oldukça sık karşımıza çıkmaya başlamıştır (Norden, 2013). İlk genel kullanım amaçlı bilgisayarların 1940'lı yıllarda Amerika Birleşik Devletleri'nde hayata geçmesi ile başlayan bilişim çağı inanılmaz bir ilerleme ile dünya çapında bir iletişim ve paylaşım ağına dönüşmüştür (Dönmez, 2001). Pek çok alanda önemli kolaylıklara imkan sağlayan bu gelişim, diğer yönüyle insanın başlangıcından bu yana var olan 'suç' kavramının da değişik görünümlere bürünmesine; yeni suç tiplerinin doğmasına sebebiyet vermektedir. Öyle ki internet olgusu başlı başlına, "güvenlik", "risk" ve "tehdit" kavramlarına dair anlayışımızda değişiklik yaratmamızı gerektirecek denli etkili bir unsur haline gelmiştir (Singhal, Tandan & Miri, 2013). İlk olarak Amerika Birleşik Devletlerinde bir bilişim güvenliği uzmanı olan Don Parkerr tarafından 'bilgisayarın kötüye kullanımı' olarak nitelenerek kaleme alınan suç tipi zaman içerisinde "bilgisayarla ilgili suç", "bilgisayar suçu", "internet suçu", "dijital suç", "çevirimiçi suç" "teknolojik suç" gibi çok çeşitli görünüm ve tanımlara bürünmüştür. (Alkaabi, 2010)

Ülkemizde bilişim suçları olgusu ilk olarak 1991 yılında 765 Sayılı Eski Türk Ceza Kanunu (ETCK) metnine girmiş; 1 Haziran 2005 tarihinde yürürlüğe giren 5237 Sayılı Yeni Türk Ceza Kanunu (TCK) ile eski kanundaki bilişim suçlarına dair maddeler bir araya getirilerek 'Bilişim Alanında Suçlar' başlığı altında ceza mevzuatımızda yerini bulmuştur (Orta, 2015). Bu kısımda; bilişim sistemine girme;

sistemi engelleme, bozma, verileri yok etme veya değiştirme; banka veya kredi kartlarının kötüye kullanılması suçları yer almaktadır (Dülger, 2018).

'İnternet aracılığı ile işlenen suçlar' kavramı; bilişim suçu kategorisinde değerlendirilmesi gereken, ancak birden fazla bilgisayarın birbirleri ile iletişim kurmasını sağlayan ve insan iletişiminin her türünü aynı sistem içinde toplayan bir hiper iletişim biçimi ve uluslararası bilgi iletişim ağı olan internet ortamında işlenen, bir kısmı klasik suç tiplerinden oluşan, bir kısmı ise internetin yapısına özel olan suçları içerisinde barındırmaktadır (Castells, 2013). Sövme, hakaret, iftira gibi bazı klasik suç tipleri internet aracılığı ile işlenebileceği gibi; internetteki bir yayını bozmak, elektronik posta sistemini kullanarak kişilere ait bilgisayarlara virüs bulaştırmak gibi internet kullanımı ile doğrudan ilişkili bir grup yeni suç tipi de internetin kullanımının yaygınlaşması ile orantılı olarak hayatımıza girmektedir (Özbek, 2002).

Bilişim suçları ve internet aracılığı ile işlenen suçların adli mercilere intikalleri halinde en önemli süreç; artık yerel ölçekte düşünülemeyecek ve sınır aşan bir kavram olarak karşımıza çıkan bu suç ve suçluların tespit edilmesi, suçlu ile mağdur arasında bağlantı kurulması, suça konu eşya olarak addedilen çok çeşitli bilişim sistemlerinin çözümü, değerlendirilmesi ve raporlandırılması ile başlamaktadır (Casey, 2011).

Bilişim suçları ile ilgili olarak resmi bilirkişilik hizmeti veren kurumların başında Adli Tıp Kurumu (ATK) gelmektedir. ATK, tüm Türkiye genelinde bilirkişilik dosyalarının en çok gönderildiği, resmi bilirkişilik hizmeti sağlayan tüm kurumlar arasında en önemli yere sahip olduğu söylenebilecek bir noktada bulunmaktadır. Öyle ki, 2015 yılında yapılan bir anket çalışması “Ceza dosyalarınız uygulamada genellikle aşağıda yazan birimlerden hangisine gönderilmektedir?” sorusuna 75 hakimden oluşan

anket grubunun % 93'ünün; 75 avukattan oluşan anket grubunun ise % 80'inin 'Adli Tıp Kurumu' olarak cevap verdiğini ortaya koymuştur (Şenel, 2015).

ATK bünyesindeki Fizik İhtisas Dairesi (FİD) Bilişim ve Teknoloji Suçları ile Ses ve Görüntü İnceleme Şubeleriyle, 15 Temmuz 2016 darbe girişimi sonrası çok fazla artan resmi bilirkişilik talebine cevap vermek için 15.08.2016 Tarih ve 674 Sayılı KHK ile düzenlenen ve 10.11.2016 Tarih ve 6758 Sayılı Kanun ile bahse konu şubeleri bünyesinde toplayarak yeni bir ihtisas dairesi olarak kurulan Adli Bilişim İhtisas Dairesi (ABİD) temel olarak; adli mercilerce gönderilen elektronik ve dijital veriler üzerinde çalışmakta; bilgisayar kasaları, sabit diskler, harici sabit diskler, modemler, disket, Compact Disc'ler (CD), Digital Versatile Disc'ler (DVD), flash diskler ve elektronik devreler üzerinde inceleme yaparak bilirkişilik hizmeti sunmaktadır (Adli Tıp Kurumu, 2012). Bu kapsamda; mahkemeler ile hakimlikler ve savcılıklar tarafından talep edilen bilişim ile ilgili konularda "gerekli incelemeleri yapmak ve sonuçlarını bir raporla tespit etmek"le görevlidir (https://www.atk.gov.tr/adli-tip-ihtisas-daireleri.html).

Bu çalışmanın amacı; adli bilişim alanındaki bilirkişilik uygulamalarına konu suç tiplerinin, diğer bir değişle internet ve bilişim suçlarının yıllar içerisinde gösterdiği yoğunluk ve çeşitlilik karşısında bilirkişilik uygulamaları yönünden talebe ne ölçüde cevap verilebildiğini tespit etmek; gelecekte karşılaşılabilecek olası suç yoğunluklarını ortaya koyarak bu kapsamda gerekli değişiklikleri tartışmak ve karşılaşılan sorunlara çözüm önerileri sunabilmektir.

2. GENEL BİLGİLER

2.1. Bilişim Suçları

2.1.1. Bilişim ve Bilişim Sistemi Kavramları

Bilişim, bilginin elektronik ortamda üretilmesi, kaydedilmesi, saklanması, taşınması ve/veya kullanılması ile ilgili cihaz, materyal, işlem ve yöntemleri kapsamaktadır (Öztürk, 2007). Her ne kadar günlük dilde bilgisayar ve bilişim sözcüklerinin birbiri yerinde kullanıldığı görülmekte ise de bilişim kavramı bilgisayar yoluyla bilginin işlenmesi ve saklanması gibi evreleri de içine alan ve bu amaca hizmet eden her tür cihaz ve sistemi içerir bir kavramdır (Yılmaz, 2010).

Bilgisayarlar, günümüz bilişim sistemi içerisinde en yoğun olarak kullanılan cihazlardır. Bilgisayarı programlanabilir aygıtlar ve elektronik hesap makinelerinden ayıran özellik bilgisayarların genel amaçlı kullanılabilme yeteneğidir yani bilişim özelliğine sahip olmalarıdır (Yazıcıoğlu 1997, Yenidünya ve ark. 2003).

Bilişim kavramı içerisinde bilişim ağlarının da incelenmesi gerekecektir. Bilişim ağları ya da bilişim sistem ağları temel olarak bilgisayarların aralarında bağlantı kurmak sureti ile iletişime geçmelerini içeren bir sistemdir. Bilgisayarların birbiri ile iletişim kurmasını sağlayan fiziki ortam ile bu ortamın fonksiyonunu gerçekleştirebilmesini sağlayan donanım ‘ağ’ kavramı ile ifade edilmektedir (Yenidünya ve ark. 2003). Bir ağ, coğrafi olarak küçük bir bölge ile sınırlı ise LAN (Local Area Network); büyük bir bölgeye yayılmış ise WAN (Wide Area Network) olarak adlandırılmaktadır. Bilgisayar ağlarından birisi olan internet ise dünyadaki en yaygın ve kamuya açık bilgisayar ağı olarak karşımıza çıkmaktadır. İnternet günümüz dünyasının en bilinen ve en yaygın olarak kullanılan ağı olma özelliğini taşımaktadır.

Ceza hukuku terminolojimizde kullandığımız "bilişim sistemi" kavramının ise zaman içerisinde bir netlik ve anlam bütünlüğüne ulaştığını söylemek mümkün olacaktır. İlk olarak 765 Sayılı ETCK'nda 11. Bapta 'Bilişim Alanında Suçlar' başlığı altında 525/a ile 525/d maddeleri arasında "bilgileri otomatik olarak işleme tutmuş olan bir sistem"den bahsedildiği; söz konusu babı Yasaya ekleyen 3756 Sayılı yasa değişikliğinin gerekçesinde ise bu tanımın yanında ayraç içerisinde bilgisayar kelimesi kullanıldığı görülmektedir. Daha sonra ilerleyen teknolojiye ve bunun doğurduğu ihtiyaçlara göre bilişim sistemi kavramının bilgisayardan çok daha öteye gittiği kabul edilmiş ve 5237 Sayılı TCK'ndaki kapsayıcı tanımlama ile hangi sistem ve araçların bilişim sistemi sayılabileceği konusunda bir netliğe kavuşulabilmiştir. Bilişim sistemi, 5237 Sayılı TCK'nun 243. maddesinin gerekçesinde belirtildiği gibi; "verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistemler"in tümüne verilen isimdir (Taşkın, 2008). Dolayısıyla bir sistemin bilişim sistemi sayılabilmesi için; verileri alıp gönderebilmesi, otomatik işlemlere tabi tutabilmesi ve manyetik olması, genel amaçlı kullanılabilmesi, çok amaçlı işlem görebilmesi gibi bir takım kriterleri sağlaması gerekecektir (Kurt, 2005).

Bugün bilişim ve iletişim teknolojileri, sahip oldukları kapasite nedeniyle hem dönüşümün ve hem de toplumları dönüştürmenin en etkin ve maliyeti düşük yöntemi olarak görünmektedir. Karşılıklı ilişkiler bütünü olarak görülebilecek toplumların yavaş yavaş bu özelliklerini kaybettikleri ve artık giderek bir ağ (network) toplumu oldukları yönünde görüşler dillenmektedir (Yalçın, 2003). Bilişim dünyasındaki bu hızlı ve büyük gelişmelerin olumsuz bir yönünün, suç ve suçlu profili üzerinde de farklılaşmalara, değişimlere ve çeşitliliğe yol açmaları olduğu söylenebilir. Gerek ülkemizde gerekse

hemen hemen tüm dünya ülkelerinde bu değişimlere paralel düzenlemeler getirilerek bilişim suçlarıyla mücadele yönünde yeni normlar ve yaklaşımlar yaratılmaktadır.

2.1.2. Bilişim Alanındaki Suçlar

Bilişim teknolojilerini ilgilendiren suçlar; bilgisayar bağlantılı suç, bilgisayarla işlenen suç, bilgisayara karşı işlenen suç, bilgisayar suçu, internet suçu, elektronik suç, sanal suç, siber suç, bilişim sistemi aracılığı ile işlenen suç, bilişim alanında işlenen suç gibi onlarca isimle nitelenmiştir. Suç kapsamını en geniş şekilde kavraması nedeniyle "bilişim suçu" terimi son zamanlarda daha çok kabul görmekte ve kullanılmaktadır (Öztük, 2007).

Bilişim suçu ile ilgili Avrupa Birliği Uzmanlar Komisyonu tarafından Mayıs 1983'te Paris Toplantısı'nda yapılan resmi tarife göre, bilişim suçu, "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetkisiz gerçekleştirilen her türlü davranış"tır (Özdemir ve ark., 2013).

Bilişim suçları kavramı ceza hukuku literatürümüze ilk olarak 765 Sayılı ETCK'nda 06.06.1991 yılında 3756 Sayılı Kanun ile yapılan değişiklikle 'bilişim alanında suçlar' başlığı altında girmiştir (Değirmenci, 2005). Halen yürürlükteki 5237 Sayılı TCK'nda aynı başlık altında düzenlenen bilişim suçları ile ilgili hükümlere 243 ila 246. maddeler arasında yer verilmektedir. Klasik suç tiplerinin bilişim alanında işlenen suçlara ilişkin müeyyideleri karşılayamaması karşısında, 765 Sayılı eski TCK'da yer almayan bir kısım düzenlemeler yürürlükteki 5237 Sayılı TCK 'Topluma Karşı Suçlar' başlıklı üçüncü kısmı içerisinde 10. bölümde 'Bilişim Alanında Suçlar' başlığı altında 243 ila 246. maddeleri arasında düzenlenmiştir (https://www.tbmm.gov.tr/kanunlar/k5237.html). Bu kapsamda TCK'nun 243.

maddesinde ‘bilişim sistemine girme’ ; 244. maddesinde ‘sistemi engelleme, bozma, verileri yok etme veya değiştirme’, TCK’nun 245. maddesinde ‘banka veya kredi kartlarının kötüye kullanılması’ suçlarına ilişkin düzenlemeler yer almaktadır. Aynı bap altında, 24.03.2016 Tarih ve 6698 Sayılı Kanunun 30. maddesiyle eklenmiş olan TCK’nun 245/A maddesinde, ‘yasak cihaz ve programlar’, TCK’nun 246. maddesinde ‘tüzel kişiler hakkında güvenlik tedbiri uygulanması’ düzenlemeleri mevcuttur (https://www.tbmm.gov.tr/kanunlar/k5237.html).

Yine bir kısım suçlar açısından, dolandırıcılık ve hırsızlık suçlarında olduğu gibi, suçun bilişim sistemi kullanılarak işlenmesinin bir ‘nitelikli hal’ olarak düzenlendiği görülmektedir. Bu kapsamda, Ayrıca bilişim sistemleri aracılığıyla işlenen nitelikli hırsızlık (m.142) ve nitelikli dolandırıcılık (m.158) eylemleri de bilişim suçları dahilinde değerlendirilmektedir (Yılmaz, 2011).

Bununla beraber, bilişim suçları kavramı içerisinde değerlendirilen ancak çalışmamızda ‘internet alanında suçlar’ alt başlığı altında incelenen bir kısım suçlara da yasal düzenlemelerimizde yer verilmiştir.

2.2. İnternet Aracılığıyla İşlenen Suçlar

2.2.1. İnternet Kavramı ve İnternetin Tarihçesi

Aralarında elektriksel bağlantı olan bağımsız bilgisayar topluluğuna bilgisayar ağı denir (Öner, 2003). Siber Suçlar Konvansiyonu açıklayıcı faaliyet raporundaki tanıma göre; ağ, iki veya daha fazla bilgisayar sisteminin kablolu (örneğin tel), kablosuz (örneğin radyo, kızıl ötesi veya uydu) ya da her ikisi ile birden bağlı olmasıdır (TBMM, 2012).

Bilgisayar ağları kulanım şekillerine göre dört tiptir; iç ağ ya da diğer bir değişle intranet, ekstranet, sanal özel ağ olarak ifade edilen VPN (Virtual Private Network) ve internet (Kessler, 1999). İç ağ; internet protokollerini kullanan, kamu haberleşme sistemlerinden faydalanabilen, güvenli bir şekilde organizasyon bilgilerinin ve işlemlerinin bir kısmını o şirketin çalışanlarıyla paylaşan özel bir bilgisayar ağıdır. Ekstranet; internet protokollerini kullanan, kamu haberleşme sistemlerinden faydalanabilen, güvenli bir şekilde organizasyon bilgilerinin ve işlemlerinin bir kısmını o şirketin çalışanlarıyla birlikte, şirketin tedarikçilerine, satış elemanlarına, çözüm ortaklarına, müşterilerine ya da diğer şirketlere paylaştıran özel bir bilgisayar ağıdır. Sanal özel ağlar ise genellikle bir veya birden fazla şirket ya da organizasyonun iletişim kurmak için internet kullandıkları özel bir iletişim ağıdır (Güngör, 2007). Tüm sayılanlar içinde en kapsamlı bilişim sistem ağı internettir. İnternet dünya genelindeki milyonlarca bilgisayarın birbirine ağlar ile bağlanmasının oluşturduğu küresel bilgisayar ağları sistemini ifade etmektedir (Erkan ve ark., 1999).

İnternette veri alışverişini sağlayan tüm ağlar bir protokole bağlı olmak zorunda olup; bu protokollere Transport Control Protocol / Internet Protocol (TCP/IP) ismi verilmektedir (Kızıltan, 2007). Dünya üzerinde bulunan ağların ve bilgisayarların TCP/IP denilen yöntemle birbirine bağlanmasıyla oluşan, yeryüzündeki en büyük insan ve makine birliğini sağlayan ağ sistemine internet denir (Baron ve ark., 1998).

İnternet teknolojisinin temelleri, Joseph Carl Robnett Licklider isimli bir bilgisayar bilimci tarafından tanımlanan ve ağ iletişimi ile bağlantılandırılabilecek sosyal etkileşimlere dair ilk kavram olan "Galaktik Ağ" kavramı ile atılmıştır (A Brief History Of The Internet, https://www.internetsociety.org/internet/history-internet/brief-history-internet/). Daha sonra bu kavram, Amerika Birleşik Devletleri tarafından kendi

bünyesinde 1958 yılında geliştirdiği ARPA (Advanced Research Project Agency) projesi ile hayata geçirilmiştir. Amerikan hükümeti nükleer bir savaş halinde ya da sosyal bir karışıklık durumunda ülke yöneticilerinin birbirleriyle haberleşmesini güvenli ve kesintisiz bir şekilde gerçekleştirmek için, tek bir merkezden yönetilmeyen ve tek bir ana bilgisayar ünitesinden bağımsız olarak çalışabilen bir bilgisayar ağı kurulması amacıyla harekete geçmiştir. Bu projenin geliştirilmesiyle ortaya çıkan ARPANET sistemi ile paylaşım ağının üniversiteleri de içine alacak şekilde yaygınlaştırılması sağlanmıştır (Gromov, 2012). Ancak sistemin genişlemesi ile iletişim problemleri baş göstermiş, 1983 yılında bu sorunun giderilmesi amacıyla TCP/IP protokolü oluşturulmuştur (A Brief History Of The Internet, https://www.internetsociety.org/internet/history-internet/brief-history). 1989 yılında Cenevre'de bulunan CERN (European Organization for Nuclear Research) merkezinde WEB (world wide web) teknolojisi ortaya çıkmış, 1990 yılında internet sayfaları aktarım protokolü olan HTTP (hyper-text transfer protocol) geliştirilmiştir (Kızıltan, 2007).

1990 Haziran'ında TCP/IP'nin ilk kullanıldığı ağ olan ARPANET'in kullanımdan kaldırılması ile internetin dünya çapında yaygınlaşması hedefi ivme kazanmıştır (İnternet Tarihi, http://www.internetarsivi.metu.edu.tr/tarihce.php).

Ülkemizde ilk olarak TÜBİTAK (Türkiye Bilimsel Ve Teknolojik Araştırma Kurumu) tarafından desteklenen bir proje kapsamında ODTÜ (Orta Doğu Teknik Üniversitesi) Bilgi İşlem Daire Başkanlığınca 12 Nisan 1993 tarihinde ilk internet bağlantısı gerçekleştirilmiş ve kullanıma açılmıştır (Sınar, 2001).

İnternetin temel fonksiyonu bilgisayarlar arası güvenli ve hızlı bir şekilde veri iletişimini sağlamaktır. İnternet üzerinde yararlanılabilecek hizmetler her geçen gün çeşitlenmektedir. İnternet aracılığı ile ses ve görüntü iletimi gerçekleşebilmekte, her çeşit verinin aktarımı yapılabilmektedir.

İnternetten faydalanılabilecek hizmetlerin başında bilgi paylaşımını en yaygın şekilde gerçekleştiren web siteleri uygulaması gelmektedir. Web ismi İngilizce World Wide Web kelimelerinin kısaltılması ile meydana gelir. Web; yazılı, sesli ve görüntülü pek çok farklı nitelikteki verilere erişimi sağlayan çoklu bir hiper ortam sistemidir (Sınar, 2001). Web siteleri web sayfalarından oluşmaktadır. HTML (Hyper Text Mark up Language) adı verilen bir işaretleme dili kullanılarak oluşturulurlar. HTML ile oluşturulan web sayfaları HTTP adı verilen standart bir aktarım protokolü kullanılarak sunuculardan kullanıcılara aktarılır. Web tarayıcıları web sitelerine URL (Uniform Resource Locators) adreslerini kullanarak ulaşır. Her web sitesi bir sunucudan yayınlanır ve her sunucu bir IP (Internet Protocol) numarası ile internete bağlanmak zorundadır. Kullanıcıların her sitenin IP adresini bilmesi beklenemeyeceğinden IP numaralarına karşılık olarak URL adresleri geliştirilmiştir (Yıldız, 2007).

İnternetin yaygın kullanımlarından ve en önemli fonksiyonlarından birisi de elektronik postalardır. Elektronik posta, kısaca e-posta, bilgisayar ağlarında işlev gören, "kağıtsız" dijital bir posta sistemidir (Leong, 1998).

İnternetin bir diğer yaygın kullanım alanı forum ve tartışmaların yapılabildiği haber grupları ve internet kullanıcılarının eş zamanlı olarak birbirleriyle konuşmalarını sağlayan IRC (Internet Relay Chat) sistemidir (Sınar, 2001).

Bilgiye en kolay ve hızlı şekilde ulaşımı sağlayan arama motorları da internetin en önemli fonksiyonlarından biri olarak kabul edilmektedir. Bir arama motoru ya da arama servisi, internette World Wide Web veya bir şirket iç ağındaki bilgisayar sistemleri üzerinde ya da kişisel bilgisayarlarda depolanmış bilgileri bulmaya yardım etmek için tasarlanmış bir programdır. Arama motoru bir kelime ya da deyim olarak verilen arama konusunu içeren veya karşılayan dokümanları liste olarak sunar. Arama motorları çabuk ve etkin hizmet görmek için dizin bilgilerini düzenli olarak günceller. İnternetin bu denli yaygın kullanılmasının arkasındaki en önemli nedenlerden biri arama motorlarıdır (Güngör, 2007). En geniş kapsamlı arama motorları olarak; google.com, bing.com, ask.com, duckduckgo.com sayılabilir.

Son olarak; dosya aktarma protokolü anlamına gelen FTP (File Transfer Protocol) özellikli siteler internetin en önemli fonksiyonlarından biri olarak karşımıza çıkar. FTP, bir bilgisayardan diğerine iki yönlü dosya aktarımı yapılabilmesini sağlayan uygulama protokolüdür (Sınar, 2001).

2.2.2. İnternet'e Özgü Eylemler

İnternete özgü eylemler, sanal ortamın kendine özgü özelliklerinden kaynaklanan ve varolan düzenlemelerle karşılanabilmesi çoğu zaman mümkün olamayan bir takım eylemlerden oluşmaktadır. İnternete özgü eylemler genel olarak interneti de içinde alan bilişim sistemlerinin çeşitli unsurlarına yönelik saldırılar olarak tanımlanabilir.

Diğer bir değişle, internet ortamında ortaya çıkabilecek internet suçları büyük ölçüde bu ortamı sağlayan bilgisayar sistemi ve verilerine hukuka aykırı ve haksız olarak yapılan müdahalelerden ve bu sistemde zararlı içerikli bir takım yayınları

bulundurmaktan ibarettir (Yıldız, 2006). Aynı şekilde, sisteme zararlı içerikli bir takım programlar yollamak da bu kapsamda değerlendirilecektir.

Hack – Hacker – Cracker Kavramları

Sisteme yapılan saldırıların sınıflandırılması konusu tartışılırken, özellikle ve öncelikle "hack", "hacker" ve "cracker" gibi kavramların açıklanması gerekecektir.

"Hack"; bilişim sistemlerinin yapılarında bulunan açık kapı denilen kodlama hatalarının kullanılarak sistemlere sızılmasıdır. Normal şatlar altında erişim izni olmayan sistemlere, o sistemlerin güvenlik önlemlerinin aşılarak girilmesidir. Bu eylemleri yapan kişilere "hacker" yani 'bilgisayar korsanı' denilmektedir (Özdilek, 2002; https://tureng.com/tr/turkce-ingilizce/hacker).

Bilgisayar korsanları, amaçları açısından iki gruba ayrılırlar; siyah ve beyaz hackerlar. Siyah hackerlar, diğer bir ifade ile "cracker"lar yani 'sistem kırıcılar', açığını buldukları bir sistemin içeriğini silebilir ya da değiştirebilirler (https://tureng.com/tr/turkce-ingilizce/cracker). Buldukları sistem açıklarını kullanarak zararlı sonuçlara neden olurlar. Örneğin kredi kartı ile internet üzerinden alışveriş yapan bir kullanıcının kredi kartı numarasını ele geçirerek kartın kullanılması ile zarar verilmesi eyleminin gerçekleştirilmesi bir sistem kırıcı eylemidir (Özdilek, 2002). Diğer yandan beyaz bilgisayar korsanları sadece bilgiye ulaşmak için sistemdeki verilere izinsiz erişirler. Bu grup, günümüzde sistem güvenliğinin sağlanmasında ve geliştirilmesinde önemli rol üstlenmiştir. Firmalar sistem güvenliklerini sağlamak ve test etmek amacıyla beyaz bilgisayar korsanlarına sistemlerine izinsiz erişim için finansman sağlamaktadırlar (Özdilek, 2002).

Sistemlere Yapılan Saldırıların Sınıflandırılması

Bu tanımlamalardan sonra, sisteme zarar veren saldırıların çok çeşitli ve karmaşık olması karşısında belli bir sınıflandırma yapılması gerekecektir. Genel olarak saldırı sınıflandırması süreçsel ve işlemsel olarak ikiye ayrılabilir (Berkay, 2006). İnternette gerçekleştirilen saldırı teknikleri süreçsel olarak dört kategoridir; engelleme, dinleme, değiştirme ve oluşturma (Berkay, 2006). Engelleme niteliğindeki saldırılar sonucunda sistemin bir kaynağı yok edilmekte veya kullanılmaz hale getirilmektedir (https://docplayer.biz.tr/1666203-Dr-i-sogukpinar-g-y-t-e-bil-muh-bol.html). Örnek olarak; donanımın bir kısmının bozulması, iletişim hattının kesilmesi, dosya sisteminin kapatılması gösterilebilir. Dinleme yöntemi ile, izin verilmemiş bir şahıs, bilgisayar ya da programdan ibaret yetkisiz bir tarafça bir kaynağa erişim sağlanmaktadır (Canbek ve ark., 2207). Değiştirme yönteminde, izin verilmemiş bir kaynak üzerinde değişiklik yapılmaktadır. Örnek olarak; bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesajın içeriğinin değiştirilmesi gibi (https://docplayer.biz.tr/1666203-Dr-i-sogukpinar-g-y-t-e-bil-muh-bol.html). Oluşturma ya da diğer bir değişle imalat yönetiminde, izin verilmemiş bir taraf sisteme suni bilgiler eklemektedir. Örneğin; ağ üzerinde sahte mesajlar yollanması ya da bir dosyaya ilave kayıtlar eklenmesi gibi (Canbek ve ark., 2007).

İnternette gerçekleştirilen saldırı teknikleri işlemsel olarak da sınıflandırılabilmektedir. Bilgisayar ya da bilgisayar ağına saldıran kişi, istediği sonuçlara çeşitli adımlardan geçerek ulaşacaktır. Bu adımlar; araçlar, erişim, sonuçlar ve amaçlar olarak sıralanabilir (Canbek ve ark., 2007). Araçlar kategorisi ise kendi içinde bilgi toplama, tarama ve dinleme şeklinde alt kategorilere ayrılmaktadır. (Berkay,

2006). Denilebilir ki, saldırı teknikleri temelde araçlar kategorisinin konusunu belirlemektedir (Yıldız, 2006).

Sistemlere Yapılan Saldırı Teknikleri

Bir bilgisayara ya da bilgisayar ağına yapılabilecek saldırıların çok çeşitli tekniklerle yapılabilmesi mümkündür. Konunun daha iyi değerlendirilebilmesi için bu saldırı tekniklerinin sınıflandırılmasında yarar vardır. Saldırı teknikleri genel olarak dört başlık altında incelenebilir; bilgi toplamak, tarama yapmak, sisteme sızmak ve kalıcılığı sağlamak.

Bilgisayar sistemine hukuka aykırı olarak girmenin ilk adımı sisteme ilişkin bilgi toplamaktır. Bilgi toplama işlemiyle ağ üzerindeki bilgisayar sayısı, kullanılan işletim sistemleri ve güvenlik yazılımları gibi pek çok bilgiye ulaşılabilmektedir. Sisteme girmek için pek çok bilgi toplama yöntemi vardır. İnternette yayınlanan ve öğrenilmesinde hukuka aykırılık unsuru bulunmayan bilgiler üzerinde açık kaynak araştırması yapmak, arama motorlarını kullanarak saldırı öncesi bilgi sahibi olmak bunlardan bazılarıdır. İnternette veri alışverişini sağlayan tüm ağların bağlı olmak zorunda olduğu TCP/IP protokollerine tabi olan ağların birbirleri ile iletişim kurarken kullandıkları IP adreslerinin aynı zamanda irtibat bilgilerinin bulunduğu Whois veri tabanlarından hedef hakkında bilgi almak kullanılan yöntemlerden biri olarak karşımıza çıkmaktadır. Aynı şekilde, DNS (Domain Name System) adreslerinin bulunduğu veri tabanları da bu bilgileri toplamak için kullanılabilir (Tulum, 2006). DNS, internet bağlantılarında rakamların zaman zaman sorun yaratması nedeniyle aynı basamakları, aynı sözcükleri gösteren ve sözcükler bilgisayara girildiğinde doğru adresi bulan işlemlerin yapılmasını sağlayan sisteme verilen isimdir (Bulut, 2001). Yine insan

ilişkileri ve ya insanların dikkatsizlikleri kullanılarak birey ya da şirket hakkında bilgi toplamak olarak adlandırılan sosyal mühendislik yönteminde, örneğin teknik servis ya da destek alınan bir kurumdan arama yapıyormuş gibi davranmak bu kapsamdadır (Hack Teknikleri, http://www.bilmuh.gyte.edu.tr/ispinar/BIL673).

Hedefle ilgili bilgi toplama çalışması yapıldıktan sonraki adım tarama yapmak şeklinde karşımıza çıkacaktır. Taramada, elde edilen bilgiler sisteme girilerek, bu bilgilerden hareketle sistemi tarayarak açık portları, çalışan servisleri, uygulamaları, işletim sistemini ve bunlarla ilgili güvenlik açıklarını bulmak yöntemi kullanılmaktadır. Tarama işlemi, saldırganın hedef aldığı ağın yöneticisinin ağ üzerindeki tüm bilgilerini elde edene kadar devam ettirdiği, hedef ağın tüm bileşenlerini ve bunlara erişim haklarını saptamak amacıyla yapılan bir işlemdir (Yılmaz, 2004).

Üçüncü aşamada, gerekli bilgilerin elde edilmesi ve bu bilgilerin kullanılarak tarama yapılması sonrasında sisteme sızmak amacı güdülmektedir. Sisteme sızmak pek çok değişik yöntemin kullanılmasıyla gerçekleştirilebilir. Sniffing adı verilen yöntemde, ağ trafiğini gizlice almak için sniffer adı verilen programlar kullanılarak bu bilgiler çalınmakta; tüm ağ trafiği gözetlenebilmekte ve önemli bilgilere ulaşılmaktadır. Spoofing adı verilen yöntemde, ağ üzerindeki makinelere kendini başka bir makine gibi tanıtarak ulaşılamayan bilgilere ulaşılabilmektedir. Bu yöntem genelde hedeften ek haklar kazanmak, saldırı ile ilgili olarak işlenen suçlardan başka kurum veya kişilerin sorumlu olmasını sağlamak, kendini gizlemek veya dağınık saldırılar düzenlemek için kullanılan bir yöntemdir (Yılmaz, 2004). Oturum çalmak olarak nitelenen bir başka yöntemde, hem sniffing hem de spoofing teknikleri birlikte kullanılmakta; yetkisi olmayan bir sunucuya girmek isteyen saldırgan bu sunucuya bağlanan birinin

oturumunu çalarak kullanıcının daha önce girdiği kullanıcı ismi ve şifresi ile oturuma devam etmektedir (Yılmaz, 2004).

Şifre saldırıları sisteme sızmak için kullanılan bir diğer yöntemdir. Sisteme sızmak için elde edilmesi gereken şifreler ilk önce varsayılan veya olası muhtemel şifre kombinasyonlarının denenmesi ile elde edilebilir yahut bu şekilde elde edilemediği takdirde çeşitli yöntemlerle şifre kırma yoluna gidilebilir.

Genel olarak şifre kırmak için üç yöntem bulunmaktadır; bunlar, sözlük formatına uygun olarak yazılmış şifrelerin bulunduğu script (kod) dosyalarının kullanılması anlamına gelen sözlük tabanlı şifre kırma yöntemi, şifrelerin tahmini için karakterlerin her türlü kombinasyonunun denenmesiyle ortaya çıkan zorlamayla şifre kırma yöntemi ve bu iki yöntemin birleşmesinden oluşan hibrit yöntem olarak sayılabilecektir (Yılmaz, 2004).

DOS (Denial Of Service) saldırıları da sisteme sızmak için kullanılan tekniklerden biridir. Denial of Service olarak açılımı yapılan DOS saldırıları sayesinde normal kullanıcıların erişimlerini engelleyecek şekilde bilgisayar sistemini ulaşılmaz hale getirilmek için yazılım hataları kullanılmakta ya da sunucu ve ağ kaynakları tüketilmektedir (Yılmaz, 2004). DDos Atakları adı verilen bir başka teknikte, verilen hizmetin aksatılması amacıyla sisteme düzenli ve arka arkaya saldırılar gerçekleştirilmekte, sistem hizmet veremez hale getirilmektedir. Sisteme sızmak için yaygın olarak kullanılan saldırılardan bir diğeri web saldırılarıdır. Bunların temelinde web sitesine izinsiz girmeye çalışmak, sitede kullanılan uygulamalardaki güvenlik açıklarından yararlanarak siteye zarar vermek ya da web sunucusundan şirketin veya organizasyonun ağına sızmak fikri bulunmaktadır. Sisteme sızmak için kullanılan bir

diğer yöntem cookie (çerez) saldırılarıdır. Cookie'ler sunucu tarafın bağlantılarının, bağlantının alıcı tarafındaki bilgiyi hem depolamak hem de düzeltmek için kullanabildiği genel bir mekanizmadır (Sarıhan, 1998). Hedef seçilen web sitelerinin şifreleri kodlanmamış olarak cookie'de saklanmaktadır. Bu yöntemde bir takım yazılımlar sayesinde kurbanın daha önce girdiği ve kullanıcı ismiyle şifresini yazdığı sitenin cookie'si saldırgan tarafından rahatlıkla kullanılmaktadır (Yılmaz, 2004).

Web uygulamalarına yönelik saldırıların en önemlilerinden biri de elektronik posta saldırılarıdır. Elektronik posta adreslerini ele geçirmek için kullanılan çeşitli yöntemler vardır. Bunlardan biri sahte elektronik posta gönderilerek mesajın başka bir kişi ya da kurumdan geldiği düşüncesi yaratılmak suretiyle kullanıcının şifresinin ele geçirilmesidir. Yine, bir kişiye gerçek dışı reklam ve benzeri amaçlarla sürekli olarak elektronik posta mesajları gönderilmesi anlamına gelen spam'ların, elektronik posta adreslerinin gasp edilmesi ya da çocuk pornografisi ve benzeri gayrı ahlaki iletilerin gönderilerek kişilerin taciz edilmesi amacıyla kullanılmaları bir yana; internet ağını tıkayan, sistemi yavaşlatan hatta sunucuları çökerterek işlem yapamaz hale getiren etkileri bulunmaktadır (Yıldız, 2006).

Elektronik posta sistemi kullanılarak gerçekleştirilen bir diğer eylem, elektronik posta mesajlarına virüs veya truva atı gibi programlar ekleyerek karşı tarafın bilgisayarına zarar vermeyi amaçlayan elektronik sabotajdır (Yıldız, 2006). Tüm bu sayılan yöntemlerin kullanılmasıyla sonuç olarak sisteme sızılarak çok çeşitli şekillerde zarar doğurma imkanı bulunmaktadır.

Hedef sisteme sızılması işlemi gerçekleştirildikten sonra, saldırganın amacı sistemde kalıcılığı sağlamak olacaktır. Burada amaç sisteme yeniden sızılmak

istendiğinde daha önce gerçekleştirilen işlemlerin tekrarlanmamasıdır. Arka kapı olarak tabir edilen truva atları, ağ solucanları, bukalemunlar, tavşanlar, mantık bombaları ve virüsler gibi bir takım yazılımların kullanılmasıyla sistemde kalıcı olmak amaçlanmaktadır.

Truva atı yazılımı yasal bir program içerisindeki yasal olmayan talimatlar içeren ya da başka bir iş yapar izlenimini verip kullanıcıdan habersiz işlemler gerçekleştiren bir programdır (Yılmaz, 2004). Truva Atı yazılımı pek çok kullanıcı tarafından edinilmek istenen yararlı bir yazılımın içine yerleştirilmekte; yararlı yazılımlar ücretsiz olarak web sitelerinden indirilerek ya da e-posta yoluyla temin edilerek çalıştırılmaya başlandığında Truva Atı yazılımı da çalışmaya başlamakta; böylelikle işletim sisteminin açıklarından yararlanarak sisteme hakim olmaktadır (Dülger, 2014).

Yine Truva Atı metodunun bir türü olan Mantık Bombaları yıkıcı bilgisayar komutlarını yerine getiren programlar olarak karşımıza çıkar. Yararlı bir yazılım görüntüsünde sisteme giren bu programlar zarar verici sonuçlar ortaya çıkartacak komutlar yerleştirirler. Truva Atı'na benzeyen bir başka yazılım türü olan bukalemunlar güvenilir programlar gibi hareket etmekte fakat gerçekte bir takım hile ve aldatmalar içermektedirler. Uygun bir şekilde programlandığında bukalemunlar, yasaya uygun hazırlanmış yazılımların simülasyonu olan programlar gibi çalışmaktadırlar (Yılmaz, 2004).

Ağ Solucanları ise, iletişim sistemlerinin ve çalışan servislerin güvenlik açıklarını kullanarak kendiliğinden bulaşan; bilgisayar sistemlerinin içerisinde dolaşan, bunu yaparken sistem içerisindeki donanım veya yazılımlara zarar vermesi gerekliliği aranmayan programlardır (Dülger, 2014). Ağ Solucanlarının amacı, bir sistemi

etkiledikten sonra bu etkilediği sistem vasıtasıyla diğer sistemlere de kendisini kopyalamak, bunu yaparken bir takım şifreler ve dokümanlar gibi bilgileri toplamaktır (Dülger, 2014).

Tavşan isimli programlar; içine girdikleri bilişim sisteminde işlemciye devamlı olarak anlamlı olmayan komutlar gönderen, bu yolla normal işleyişi sağlayacak komutların verilmesine engel olmak suretiyle sistemi yavaşlatan programlardır (Dülger, 2018). Bu programlar son derece hızlı bir şekilde çoğalarak, bellekte ve/veya diskte yeteri kadar alan kalmayana dek kolonileşmek, bu yolla ana sistemin kaynaklarını, bilgi işleme gücünü yitirinceye kadar kurutmak amacını güderler (Dülger, 2014).

Sistemde kalıcılığı sağlamak adına kullanılan bir diğer yöntem olan Salam Tekniği daha çok bankacılık alanında kullanılan bir yöntemdir; burada banka hesaplarındaki rakamların virgülden sonraki küsuratlarının fark yaratmayacak kadar küçük bir miktarı fail tarafından belirlenen hesaba aktarılıp orada birikmektedir (Dülger, 2018). Bu işlemin gerçekleştirilmesi için genellikle Truva Atı yazılımının çeşitleri kullanılmaktadır.

Kalıcılığı sağlayan bir diğer yöntem çok küçük programlar olan bilişim virüslerinin kullanılmasıdır. Bilişim virüsleri kendi kendisini çoğaltabilen, bilişim sistemlerine kopyalarını göndermek suretiyle bu sistemleri etkileyebilen yazılımlardır ve çok çeşitli olmakla birlikte, genel özellikleri itibariyle kendilerini başka bir programa ekleyerek yayılırlar (Kızıltan, 2007). Virüsün sistemde kaldığı süre içinde verdiği zarar ise virüsün türüne göre değişiklik göstermektedir. Kimi virüsler sadece sistemi yavaşlatmak gibi zararlar verirken, kimileri hafızadaki tüm verileri yok edici niteliktedir, kimileri ise donanımı kullanılmaz hale getirirler (Akıncı ve ark., 2004).

2.2.3. İnternet Aracılığıyla Gerçekleştirilen Eylemler

İnternet aracılığıyla gerçekleştirilen eylemler, yapısı itibariyle çok hızlı büyüyen, kullanımı ve yayınlanması kolay, her eve, her iş yerine erişebilen, modern dünya insanına birçok farklı şekillerde hizmet veren sanal bir dünya olan internette saniyeler içerisinde vuku bulabilen ve yasalarımızda tanımlanmış birçok suç tipini içerebilen eylemlerdir. Bu suç tipleri yapısı itibariyle bilişim suçu değillerdir; ancak internet içerisinde ve internet aracı kılınarak işlenen suçlardır.

Bilişim suçları doğaları gereği bilişim ağları ve internet üzerinden işlenen suçlar iken, internet vasıtasıyla işlenen suçlar kısmında değinilecek eylemler daha ziyade internetin modern bir yayın ve kitle iletişim aracı olması yönüyle oluşturduğu zeminde gerçekleşme olanağı bulan suçlardır.

Doğal olarak pek çok suç tipinin internet aracılığı ile işlenme olanağı varken, durmaksızın gelişen yeni teknolojiler ile gelecekte internet aracılığıyla işlenebilecek suçlar listesinin daha da uzaması muhtemel görülmektedir. Bunun yanı sıra, internet üzerinden yapılan bir yayının ulusal sınırları aşarak diğer kitle iletişim araçlarına oranla daha geniş kitlelere ulaştığı ve etkileşimli özelliğinden dolayı doğurduğu sonuçların daha etkili olduğu gözlemlenmektedir. Böyle bir gücün kötüye kullanılması durumunda suç içerikli materyallerin aynı hız ve etkiyle dünyaya yayılması gibi son derece ciddi ve tehlikeli bir sonuç ortaya çıkmaktadır (Yıldız, 2006).

Örneğin bireysel nitelikli olan özel hayatın gizliliğini ihlal gibi bir suçun dahi internet aracı kılınarak işlenmesi halinde, gerek özel hayatın gizliliğinin ihlalindeki yoğunluk derecesi anlamında gerekse mağdurun uğrayacağı zararın kapsamı açısından

çok ciddi sonuçlar doğacağı, bu bağlamda internet gibi etkileşimli ve yaygın bir alanın suçta kullanılmasının büyük fark yaratacağı ortadadır.

İnternet aracılığıyla işlenen eylemler çok çeşitli olabileceğinden, ancak örnekleme yolu ile bu kapsamda karşılaşılabilecek bir kısım klasik suç tiplerinden bahsedilebilecektir. İnternet aracılığıyla işlenenebilecek suç tipleri arasında; TCK'nun 84. maddesinde düzenlenen intihara yönlendirme, TCK'nun 106. maddesinde düzenlenen tehdit, TCK'nun 107. maddesinde düzenlenen şantaj, TCK'nun 125. maddesinde düzenlenen hakaret, TCK'nun 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlal, TCK'nun 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal, TCK'nun 112. maddesinde düzenlenen eğitim ve öğrenimin engellenmesi, TCK'nun 123. maddesinde düzenlenen kişinin huzur ve sükununu bozma ve TCK'nun 124. maddesinde düzenlenen haberleşmenin engellenmesi suçları sayılabilecektir.

2.3. Adli Bilişim

Adli bilişim; adli bilimler içerisinde yer alan bir çalışma alanıdır. Temel olarak verilerin kurtarılması esasına dayanan adli bilişim, dijital verilerin içerdiği bilgileri, delil inceleme prosedürlerini göz önünde bulundurarak gerçeği açığa çıkartmak amacıyla dijital delilin kopyalanması, belirlenmesi, çözümlenmesi, yorumlanması ve belgelenmesi sürecidir (Orta, 2015).

Adli bilişim sürecinde kopyalama işlemi, elde edilen delilin kontamine olmaması için orjinal delilin birebir kopyasının oluşturulmasını ifade etmektedir (Brown, 2010).

Belirleme işlemi, olay yerinde bulunan bilişim ile ilintili bulguların tespit edilerek tüm incelemeler yapılana kadar delil olarak kabul edilmesi sürecidir.

Çözümleme, kopya delil üzerinde anahtar aramalar yapılması; yorumlama ise çözümleme ile dijital delil içerisinden elde edilen bulguların olayla ilişkisini araştırma eylemidir (Özen ve ark., 2015).

Son olarak, belgeleme işlemi ile olay konusu ile bulunan veriler arasındaki ilişkiyi açıklayan bir raporun hazırlanması gerçekleştirilmektedir (Say, 2006).

2.3.1. Adli Bilişimin Çalışma Alanları

Veri Kurtarma

Adli bilişim alanında karşımıza en çok çıkan delil tiplerinden olan veri saklama medyaları, özellikle sabit diskler, hareketli parçalara sahip olduğu için çabuk bozulma eğilimi gösterirler, diskin mantıksal veya fiziki zarar görmesi çok doğal bir olaydır (Çakır ve ark., 2013). Ayrıca, laboratuvara gelen bazı deliller kasten zarara uğratılmış da olabilir.

Her ne şekilde olursa olsun veri saklama medyaları içerisindeki bilgiler çoğu zaman tamamen yok olmamaktadır ki; böyle bir medya içindeki bilgilerin incelemeye alınmadan evvel kurtarma işlemine tabi tutulması gerekliliği bulunmaktadır (Güllüce ve ark., 2015).

Veri kurtarma işlemi; veri depolama medyaları üzerindeki silinmiş bilgilerin kurtarılması, bozulmuş veya formatlanmış bölümleme yapısı bilgilerinin tekrar oluşturulması gibi mantıksal olarak zarar görmüş medyalardaki bilgilerin tekrardan yerine getirilmesi işlemidir (Güllüce ve ark., 2015).

Kaza ya da kullanım sonucu veya kasten teknik olarak medyalar üzerinde manyetik olarak kodlanmış 1 ve 0'larla ifade edilen bilgilerin silinmesi sonucu adli inceleme için kullanılan özel yazılımlar bu bilgileri bir yere kadar elde etmemizi sağlayabilmektedirler (Ekizer, 2014).

Fiziksel arızalı disklerden veri kurtarmak için uygulanan en gelişmiş yöntem arızalı parçaların çok dikkatli bir şekilde değiştirilmesi yöntemidir. Bu işlem çoğu zaman 'temiz oda' denen ve tek bir toz zerresinin bile girmediği laboratuvar ortamında yapılmalıdır (Baloğlu, 2013). Aksi halde, havadaki en ufak bir toz zerresi dahi disk yüzeyine zarar verecek ve okunabilir seviyede olan diğer bilgileri de okunamaz hale getirecektir (http://yazilim.soysal.biz/harddisk-dedigimiz-yenilmez-yutulmaz-icat/).

Veri kurtama işlemleri bilgisayarın depolayacağı bilgi miktarını gösteren gigabyte'larca bilgi üzerinde gerçekleştirilmekte; bit bit yapılan bu veri inceleme işlemleri çok zahmetli olsa da, bir suçun araştırılmasında bize çok önemli sonuçlar doğuracağı için bu yönteme başvurulmasında zorunluluk bulunmaktadır (Çakır, 2014).

Veri İmha Etme

Adli bilişimin çalışma alanlarından biri de veri imha etme olarak karşımıza çıkmaktadır (Ekizer, 2014). Veri imha etme sürecinde; veriler, gerekli görülen güvenlik seviyesine bağlı olarak çeşitli biçimlerde silinmektedir.

Saklanmasına gerek kalmayan verilerin standart silme komutları kullanılarak silinmesi yeterli değildir; bu verilerin güvenli ve kalıcı bir biçimde imha edilmesi gereklidir (https://www.emt.com.tr/tr/cozumler/guvenli-veri-imha-cozumleri-15).

Wipe (Dosyaları Kalıcı Olarak Silme) adı verilen yöntemle, güvenli veri silme donanımları tarafından işlem sonrası test ve raporlama özelliği ile tüm sektörler üzerindeki veriler bit seviyesinde anlamsız veriler ile yer değiştirilmektedir (Poonia, 2014).

Degaussing ya da Degauss İşlemi (Manyetik İzleri Bozma) yöntemi ile, harddisk, floppy disk, manyetik kaset, LTO (Linear Tape Tecnology) , DLT (Distributed Ledger Teknology) gibi manyetik depolama yapan medyalar üzerindeki veriler yüksek bir manyetik alan ile bozularak ulaşılmaz hale getirilmektedir (https://www.emt.com.tr/tr/cozumler/guvenli-veri-imha-cozumleri-15).

Degauss cihazları manyetik depolama sürücülerindeki verilerin imhası için kullanılmalıdır (https://en.wikipedia.org/wiki/Degaussing). Veri imha etmede kullanılan bir başka yöntem, sürücülerin fiziksel olarak parçalanarak imha edilmesi yöntemidir (Sağlık Bakanlığı, 2018).

Veri Saklama

Adli bilişim laboratuvarları için veri depolama birimleri olmazsa olmaz bir gereksinimdir (http://www.dijitaldeliller.com/veridepolama.html). Öyle ki adli bilişim laboratuvarlarının temelde, "inceleme", "depolama" ve "sunum" olmak üzere üç parçadan oluştuğunu söylemek mümkündür (Craiger ve ark., 2008).

Bir adli bilişim laboratuvarında depolama çözümü aslında tam olarak neler yapıldığına, iş yüküne, personel sayısına ve çalışma prosedürlerine bağlı olarak değişebilecektir (http://www.dijitaldeliller.com/veridepolama.html).

Depolama çözümleri genel olarak 3'e ayrılmaktadır; doğrudan bağlı depolama alanı DAS (Direct Attached Storage) ; ağ üzerinden bağlı depolama alanı NAS (Network Attached Storage) ve depolama alanı ağı SAN (Storage Area Network) (https://www.batuhandemirdal.com.tr/veri-depolama-sistemleri-das-nas-san/).

DAS yönteminde, depolama cihazları host bilgisayarın bir parçasıdır, diğer bir değişle bilgisayarın hard diski gibidir veya bir sunucuya bağlıdır. Bu yöntemde depolama alanına erişilebilmesi için sunucuya da erişebilmek gerekmektedir; dolayısıyla, sunucular bozulursa kullanıcı depolama alanına ulaşamaz (http://www.dijitaldeliller.com/veridepolama.html).

NAS yönteminde, depolama çözümleri hard disklerden ve yönetim yazılımından oluşur; ki bunlar tamamıyla dosyaları ağ üzerinde hizmete açmak üzere adanmıştır (http://www.dijitaldeliller.com/veridepolama.html). Sunucuya bağlı DAS sistemlerdeki gibi arıza veya yavaşlamalardan etkilenmez. Sistemi kapatmadan arızalı diski değiştirme imkanı verir. Tüm işletim sistemlerine dosya paylaştırabilir. Bu özellikleriyle DAS sistemine göre daha avantajlıdır.

SAN yönteminde, lokal ağdan bağımsız olarak depolama alanı ile sunucular arasında çalışan yüksek performanslı bir depolama ağı kullanılır (http://www.dijitaldeliller.com/veridepolama.html). İleri düzey bir sistemdir ve yönetimi komplekstir. Dosya düzeyinde paylaşım imkanı sağlayan DAS ve NAS sistemlerinden farklı olarak, SAN büyük data bloklarını taşıma imkanı sunar (https://www.batuhandemirdal.com.tr/veri-depolama-sistemleri-das-nas-san/). Veri tabanı, görüntü işleme gibi uygulamalar için önemlidir (http://www.dijitaldeliller.com/veridepolama.html).

Şifreleme

Adli bilişimin en önemli çalışma sahası şifreleme ve şifre kırma alanlarını içermektedir. Şifreleme yöntemi; şifre bilimi anlamına gelen kriptoloji sahası içinde değerlendirilmelidir. Şifrelemenin temel amacı ileti güvenliğini sağlamaktır. Şifreleme, düz metinden oluşan bir iletinin içeriğini uygun anahtar bilgisi elde olmadan okunamayacak hale getirme işlemidir (Güven, 2007).

Şifrelemenin amacı, temel olarak, iletinin istenmeyen şahıslar tarafından okunmasını engellemektir (http://members.tripod.com/enoter_hukuk/kriptoloji.htm). Şifreleme, fiziksel dünyada sahip olduğumuz güvenli ortamı elektronik dünyaya taşımamızı sağlar. Bilgi güvenliği söz konusu olduğunda, veri şifreleme teknolojisi gizlilik ve bütünlük sağlamak açısından çok büyük bir başarı elde etmiştir (Balogun ve ark., 2013).

Özellikle internet alanında önem arz eden şifreleme ile güvenli web sayfaları ve güvenli elektronik iletim sağlanabilmektedir. Örneğin; bir web sayfasının güvenli olabilmesi için, bilginin tutulduğu ve bilgiyi isteyen makineler arasındaki iletişimin şifreli olması gerekmektedir. Böylelikle; kullanıcılar güvenli olarak e-posta iletisi gönderebilir veya elektronik ticaret (örneğin kredi kartı ile alışveriş) yapabilirler. Şifreleme yalnızca internet üzerinde değil, telefonlarda, televizyonlarda, kısacası günlük hayatın pek çok alanında kullanılmaktadır.

Adli bilişim çalışmalarında, gerek internet ortamında gerekse telefonlar, kredi kartları, ATM kartları gibi bilişim cihazları ile ilintili olarak sıklıkla karşımıza çıkan şifreleme işlemi önemli ölçüde yer almaktadır.

Şifre Çözme

Şifreleme gibi şifre çözme işlemi de adli bilişimin çalışma alanı içinde sıklıkla kullandığı bir yöntem olarak karşımıza çıkar. Kriptoloji bilimi içerisinde yer alan şifre çözme, şifrelemenin tam tersi yani şifreli metnin düz metne çevrilmesi işlemidir (Güven, 2007).

Adli bilişim alanına giren delil incelemeleri ve analizleri, delilin içerdiği verilere ya da doğrudan delilin içeriğine ulaşılamadığı hallerde genel geçer şifre çözme yöntemlerine başvurularak gerçekleştirilebilmektedir. Genel olarak şifre kırmak için kullanılan üç yöntem vardır; sözlük tabanlı yöntem, zorlama yöntemi ve hibrit yöntemi (Yıldız, 2006). Sözlük tabanlı şifre kırma yönteminin esası sözlük formatına uygun olarak yazılmış şifrelerin bir dosyaya saklanmasına dayanmaktadır (Yıldız, 2006).

Birçok kullanıcının şifrelerini sözlüklerde bulunan kelimelerden seçmesi nedeniyle bu yöntem işe yaramaktadır. Şifreleri sırayla denemeye yarayan bir takım yazılımlar kullanılarak şifreler tek tek denenmekte ve doğru şifreye ulaşılmaya çalışılmaktadır. Zorlamayla şifre kırma yönteminde, şifrelerin tahmini için karakterlerin her tür kombinasyonu denenmektedir. Genellikle alfanümerik karakterler (az ve 09) ile başlanır ve özel karakterlerle (@,!,?,$,vs) devam edilir (https://www.turkhackteam.org/web-server-guvenligi/547059-sifre-kirma-yontem-ve-mantigi.html). Bu yöntemde mesela aa ile başlanır ve ab,ac … diye devam edilerek denemeler yapılmaktadır (https://docplayer.biz.tr/2668892-Sifrelemenin-temel-elemanlari.html).

Hibrit yöntemi, yukarıda anlatılan iki yöntemin birleşmesinden oluşmaktadır. Sözlük tabanlı şifre kırma yöntemi hızlı ama etkisiz, zorlamayla şifre kırma tekniği ise

yavaş ama etkilidir. Hibrit yöntemde, sözlükteki şifrelere zorlama tekniğiyle yeni karakterler eklenmekte ve şifre kırılmaya çalışılmaktadır (https://docplayer.biz.tr/2668892-Sifrelemenin-temel-elemanlari.html). Mesela listedeki bir şifre "adam" ise, zorlama tekniği bu kelimeye "adam01" gibi eklemeler yapar (https://docplayer.biz.tr/2668892-Sifrelemenin-temel-elemanlari.html).

Gizlenmiş Dosya Bulma

Adli bilişimin çalışma alanlarından biri de; incelenecek delil içerisinde bir şekilde gizlenmiş yahut silinmiş olan, dolayısıyla ilk etapta elde edilemeyen verilere ulaşılabilmesi amacıyla gizlenmiş dosyaların bulunması yöntemidir. Varlığı bilinen bir dosyanın, şüpheli bilgisayar üzerinde aranarak ortaya çıkarılması işlemi klasik yöntemlerle arama yapılarak yahut silinmiş dosyaların geri getirilmesi ile gerçekleştirilebilir.

Gizli dosyalar işletim sistemi kullanıcı ara yüzünde doğrudan görülemeyen dosyalardır; daha açık bir ifade ile gizli özelliği açık olan, dosyaları keşfederken ya da listelerken kullanıcıların göremeyeceği dosyalardır (https://www.techopedia.com/definition/1837/hidden-file). Gizli dosyaların gösterimi için "DIR/AH" komutu kullanılabilir (Henkoğlu, 2011).

Bilinen tüm dosyalar başlık bölümü içine yerleştirilmiş bir imzaya sahiptirler. Dosya imzaları harici ya da dahili olabilir (The National Archives, 2012). Harici imzalar dosya adı uzantılarıdır ve dosya formatına dair ipucu verirler. Uzantı, dosya adının sonunda, dosya adından son noktayla ayrılmış bir dizi karakterlerdir (Naqvi, 2015).

Dahili imzalar, belirli dosya formatlarında yaygın olarak kullanılan bayt dizileridir ki hangi formatta kodlanmış ise o formattaki dijital nesneleri tanımak için kullanılabilir (The National Archives, 2012).

Dosya imzaları kullanılmak suretiyle, dosyanın uzantısı değiştirilmiş dahi olsa dosyanın gerçek kimliğine ulaşmak ve ilgili programları bularak dosyanın içeriğine erişmek mümkündür.

Dosya imzaları, şüpheli dosyayı ortaya çıkartmak için kullanılan en önemli ipucu olarak karşımıza çıkar. Varlığı bilinen bir dosyanın, şüpheli bilgisayar üzerinde aranarak ortaya çıkarılması işlemi klasik yöntemlerle gerçekleştirilebilir.

Gizli dosyalar, dosyanın disk üzerinde gizlenebileceği özel alanlar kullanılarak ya da dosya üzerinde değişiklikler yapılarak örneğin dosya uzantısı silinerek oluşturulabilir. Fakat dosya üzerinde yapılan bu değişiklikler ile dosyanın kimliği; diğer bir değişle imzası değiştirilemeyeceğinden, dosya imzalarının incelenmesi yöntemi ile sonuca ulaşılabilmektedir (Henkoğlu, 2011).

2.3.2. Adli Bilişimin Safhaları

Elektronik delillerin klasik delillerden farklı özellikler taşıması, delillere ulaşma konusunda bazı farklılıklar ortaya çıkarmaktadır (Sansar, 2017). Örneğin, bir cinayet vakasında, olay mahallinde bulunan tabanca, kuvvetle muhtemeldir ki suça ilişkin bir delildir; muhafaza altına alınarak, gerekli incelemelerin yapılması için götürülür, oysa ki dijital delillerde durum bundan çok farklıdır. Öncelikle, muhafaza altına alınan bir elektronik aygıt içerisinde suça ilişkin delil bulunup bulunmadığı belli değildir (Tan, 2009).

Örneğin; suç mahallinde bulunan bir bilgisayarın suçta kullanılıp kullanılmadığı veyahut suça ilişkin bir delil ihtiva edip etmediği belli değildir. Şüphesiz ki, tabanca örneğinde de suça ilişkin kesin bir belirginlik yoktur. Ancak ortamda bulunan bilgisayar yahut bir başka elektronik aygıt konusunda bu belirsizlik çok daha fazladır (Tan, 2009).

Muhafaza altına alınarak incelemeye başlanmış bir klasik delil, çeşitli analizlerden sonra çözülür ve nitelendirilir. Ancak elektronik delillerde bu işlem o kadar basit ve kolay olmamaktadır. Adli bilişimde delilin incelenmesi, nitelendirilmesi ve analizi klasik delillere kıyasla daha karmaşık, çok daha teknik ve oldukça pahalı bir işlemdir (Tan, 2009).

Dijital delilleri incelerken de genel adli ilkeler geçerlidir, ancak farklı dava ve medya türleri farklı inceleme metotları gerektirir (National Instutite Of Justice Special Report, 2016).

Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder ve uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar (Tan, 2009). İşte bu prosedürlere adli bilişim safhaları denilmektedir. Adli bilişim safhaları, bazı görüşlere göre dört tane olarak sayılırken (Artuner, 2015); bazı görüşler, bu aşamaların beş adet olduğu yönündedir (Orta, 2015).

Kimi kaynaklar ise, adli bilişim safhaları içine, henüz delillere ulaşılmamış olunan hazırlık aşamasını da ekleyerek ayrı bir başlık halinde incelemektedir (Özbek, 2013). Ancak çalışmamız kapsamında adli bilişim safhaları; toplama (collection), inceleme (examination), çözümleme (analysis) ve raporlama (reporting) olarak dört bölüm halinde incelenecektir (Kateeb ve ark., 2005).

Toplama

Toplama, delillerin elde edilmesidir. Öncelikle, delillerin toplanmaya başlanılabilmesi için elverişli yasal durumun mevcut olması gerekir ki bu da ancak usulüne uygun olarak verilmiş bir arama kararı veyahut CMK m. 116 gereğince şüphe üzerine arama ile mümkündür (Tan, 2009). Yasal prosedürün eksiksiz olarak yerine getirilmesi, delillerin hukuka uygunluğu noktasında önem taşımaktadır. Toplama aşamasında olay yeri öne çıkmaktadır. İçerisinde delilerin bulunduğu mekân, olay yeridir. Adli yaşam döngüsünün en önemli aşamalarından biri olan delilerin toplanması sürecinin ne kadar sağlıklı ilerlediği, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır (John, 2012).

Toplama aşaması, klasik suçlarda olduğu gibi kolluğun olay mahalline intikaliyle başlar. Yine klasik suçlarda olduğu gibi olay mahallinin güvenliğinin sağlanması, yetkisiz kişilerin olay yerinden çıkarılması gibi uygulamaların derhal yerine getirilmesi çok önemlidir. Olay yerinde bulunan elektronik aygıtların durumlarının sağlıklı bir biçimde korunabilmesi ancak bu sayede sağlanabilir (Tan, 2009).

Olay yerine yetkisiz kişilerin girmemesi temin edildikten sonra, mümkünse bir adli bilişim uzmanının olay yerine getirilerek, delil toplama işinin ona bırakılması gerekir. Esasen elektronik delilerin, klasik delillerden farklı yapısı bunu zorunlu kılmaktadır. Ancak bir adli bilişim uzmanı, delil kaybı yaratmaksızın -ya da mümkün olan minimum kayıpla- dijital delilleri toplayabilecektir. Delilerin incelenmesinden alınacak sonucun kalitesi ve sonuçların güvenilirliği bu sürecin doğru işlemesiyle doğrudan bağlantılıdır (Beckett ve ark, 2007).

Ancak olay yerinde dijital delillerden farklı olarak klasik suç delillerinin yer alması kuvvetle muhtemeldir. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare (mouse) üzerinde bulunabilecek parmak izleri, mahalde bulunan şüpheliye ait giysiler, eşyalar vb. unsurlar da birer delildir. Bu aşamada kriminalistik inceleme ihmal edilmemelidir. Fakat bu, hassasiyet gerektiren potansiyel dijital delillere zarar vermeden yapılmalıdır. Örneğin bir CD üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar nedeniyle CD'nin içerisindeki bilgilerin kaybını doğurabilecektir. Bu nedenle kriminal veri toplama ile adli bilişim verileri toplama arasında makul bir denge tutturulmalıdır (Özen ve ark., 2015).

Öncelikle olay yeri fotoğraflanmalı, ortamda bulunan bilgisayar, yazıcı ve diğer donanım aygıtlarının konumları belirtilecek şekilde notlar ve krokiler hazırlanmalıdır. Özetle, bu aşamaya kadar uygulanan yöntemler açısından, kriminalistik ile adli bilişim yöntemlerinin bir arada yürütüldüğünü söylemek mümkündür (Ekizer, 2014). Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir (Karagülmez, 2011).

Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilmelidir; olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır (Tan, 2009).

Bilgisayarın açılması halinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacak, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta

bilgisayar kapatılmamalıdır (Dülger ve ark., 2014). Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir (Brown, 2010). Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare oynatılarak görüntünün gelmesi sağlanmalıdır (Dülger ve ark., 2014).

Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Ancak kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak arkadaki güç kablosu çekilmelidir (Dülger ve ark., 2014). Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir ki kanıtların bütünlüğünü korumak kabul edilebilirliğini sağlamak için şarttır (Saleem, 2015). Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adli bilişim uzmanlarınca ve laboratuvar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir.

Bilgisayarların muhafaza altına alınarak incelenmek üzere laboratuvarlara götürülmesi aşaması oldukça dikkat ve özen gerektirmektedir. Donanım araçlarının hassas yapısı gereği, dikkatlice paketlenmesi ve yine aynı dikkatle taşınması şarttır. Sarsıntı, elektrik akımları, elektromanyetik ortamlar, aşırı sıcak ya da sıvı maddelerle temas gibi haller bu aygıtların işlevini yitirmesine neden olacaktır ki bu da potansiyel delillerin kaybıdır. Ayrıca paketlemenin, statik elektrikten ve manyetik alanlardan etkilenmeyecek biçimde yapılması gerekmektedir (Ekizer, 2014).

Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılacaktır. Orijinal dijital kanıt asla değiştirilmemeli ve adli bilişim uzmanları orijinal kanıtların resmi, diğer bir ifade ile klonu üzerinde çalışmalıdır (Mehta, 2017).

Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Bu nedenle aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adli bilişimde yapılan birebir kopyalama işlemine imaj (forensic image) denilmektedir (Özbek, 2013). Bu kopyalama, sistemdeki tüm verilerin buna özel yazılımlar kullanmak suretiyle ve düşük seviye bit bazında başka bir ortamda bir örneğinin yani 'imajının' ya da 'görüntüsünün' oluşturulması suretiyle yapılır. Düşük seviye bit bazında kopyalama yapılmasının önemi; daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere ulaşma olanağını vermesidir (Ekizer, 2014).

İmaj alma işleminde dikkat edilmesi gereken önemli bir başka husus da, kopyaların alınacağı sistemin örneğin bilgisayarın doğrudan çalıştırılmaması gerektiğidir. Bilgisayarın açılması, işletim sisteminin çalışmasına bağlı olarak yeni veriler işlerken önceki verilerin kaybı sonucunu doğurabilecektir. Bu nedenle bilgisayarın diski sökülüp yazma korumalı bulunmayan bir başka sistem içerisine yerleştirilmeli ve imaj alma işlemi bu biçimde gerçekleştirilmelidir. Hangi donanım aygıtı ve hangi modeli için ne tür bir yazılım kullanılacağı, hangi prosedürlerin izleneceği iyi bilinmelidir çünkü her donanım türü için farklı bir yöntem izlenmesi gerekecektir. Bu nedenle adli bilişim uzmanının, delil kaybını mümkün olan minimum düzeye indirmek için gerekli olan bilgiye sahip olması çok önemlidir (Çakır ve ark., 2013).

İnceleme

Toplama safhasının imaj alma işlemi ile sona ermesinden sonra inceleme aşaması başlar. İmajın alınmasından sonra artık işin teknik yönü geride kalmıştır ve elimizde birtakım bulgular vardır. Bunların bazıları görünmekte, bazıları henüz görünmemektedir. İnceleme ile tüm bu bulgular üzerinde çeşitli işlemler yapılarak olası suç unsurları ortaya konacaktır. Yani inceleme safhası özetle, imajı alınmış verilerin gözle görünür biçime getirilme sürecidir **(**Akcan, 2008).

İnceleme aşaması sonucunda her türlü veri ortaya konmuş olacaktır. Örneğin; fotoğraflar, grafik dosyaları, videolar, word ve excel gibi çeşitli yazı dokümanları, chat ve MSN benzeri ortamlar içerisinde geçen konuşma kayıtları, e-postalar, ziyaret edilmiş ve sık kullanılan web siteleri, sıkıştırılmış dosya ve klasörler, şifreli dizinler, silinmiş dosya ve klasörler, dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları ilk başta akla gelen ve en sık rastlanan hususlar olarak sayılabilir (Tan, 2009).

Bu aşamada birtakım yazılımlar kullanılmaktadır. Bu yazılımlara, ülkemizde de kolluk tarafından kullanılan EnCase ve FTK (Forensic Toolkit) örnek olarak verilebilir (Fei, 2007).

Çözümleme

Sistemden imajı alınmış verilerin gözle görünür hale getirilmesinden sonra analiz aşamasına geçilecektir. Elde edilen verilerin hangilerinin ne ölçüde adli makamlara sunulmak üzere raporlanacağı belirlenir (Sansar, 2017).

Bu safhanın bir tür ayıklama aşaması olduğunu söylemek yanlış olmayacaktır. Tüm ilgisiz dosyalar bu değerlendirme aşamasında elenecek, raporlama aşamasına

geçirilmeyecektir. Ancak işe yarayabileceği düşünülen bulgular, elde ediliş metotlarını ayrıntılarıyla anlatan tutanaklarla teslim edilecektir (Tan, 2009).

Raporlama

Dijital deliller toplanmış, inceleme ve analiz aşamalarından geçmiş ve artık adli bilişimin son safhası olan raporlamaya gelinmiştir. Bundan sonra yapılacak olan, hangi bulguların o soruşturma açısından kullanılabilir olduğunun belirlenerek adli makamlara sunulmasıdır (https://www.ekizer.net/adli-bilisim-computer-forensics/).

Bu yönüyle raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Ancak burada akla bu hukuki değerlendirmeyi kimin yapacağı sorusu gelir ki bu artık adli bilişim uzmanı değil, kolluk olacaktır. Adli bilişim uzmanlarının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği ve o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilecek ve adli makamlara sunulacaktır (Tan, 2009).

Bu sunum ile birlikte ayrıca ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin açıklamaları içerir teknik bilgiler verilecek ve adli bilişimin hangi metotlarının kullanıldığı anlaşılır bir dille belirtilecektir (Ukşal, 2015).

Bu suretle açıklayıcı bir rapor hazırlanacaktır (Ekizer, 2014).

Hazırlanacak bu raporda; olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme esnasında kullanılan yazılım ve donanımlar hakkında bilgiler, inceleme sırasında kullanılan metotlar ve araştırma sonunda ele geçen bulgular yer almalıdır(Akcan, 2008).

2.3.3. Mevzuatımızda Adli Bilişim

Yürürlükteki mevzuatımız açısından adli bilişimi ilgilendiren ilgili hükümler; CMK m. 134 ile Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi ve Suç Eşyası Yönetmeliği 8. maddesidir.

5271 Sayılı CMK'nun 134. maddesi, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma hükümlerini düzenlemektedir. Bilgisayarlarda ve bilişim sistemlerinde yapılacak arama, kopyalama ve elkoyma gibi işlemler, esasen bir koruma tedbiri hükmündedir. Kanun koyucu bu hükmü kanunda, Arama ve Elkoyma bölüm başlığı altında, 'Koruma Tedbirleri' kısmında düzenlemiştir. Maddenin ilk fıkrası, yapılacak arama, kopyalama ve elkoyma işlemlerindeki yasal prosedürü düzenlemektedir. Buna göre, yürütülmekte olan bir soruşturma esnasında şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütükleri üzerinde arama, kopyalama ve çözümleme gibi esasen adli bilişimi ilgilendiren işlemler yapılabilecektir; karar verecek makam ise, cumhuriyet savcısının talebi üzerine hakim olacaktır (Dülger, 2018).

Adli ve Önleme Aramaları Yönetmeliği 17. maddesi ise; bilişim suçlarına ait deliller üzerinde yapılacak arama ve elkoyma işlemlerinde uygulanacak usulleri içermektedir. Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti ilgiliye verilir. Yönetmelik, kanundaki düzenlemeden farklı bir husus olarak, bu tedbirin konusu olan araçlar kapsamında bilgisayar ve programları ile

kütüklerine ilaveten bilgisayar ağları, uzak bilgisayar kütükleri ve çıkarılabilir donanımlardan bahsetmektedir. Bu da yerinde bir düzenlemedir (Tan, 2009).

Suç Eşyası Yönetmeliği 8. maddenin 3. fıkrasında; bilişim suçları ile ilgili elde edilecek delillerin korunmasına ilişkin düzenlemeler getirmiştir. Elektronik delillerin hassas yapısının yönetmelik tarafından ortaya konulduğu bu düzenleme, adli bilişim alanında elde edilen delillerin bozulmasını önleme amaçlı olarak nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilmelerine dair hükümler içermektedir (http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf).

Bu hükümlerin yanı sıra, CMK'nın diğer hükümleri de doğal olarak adli bilişim uygulamalarıyla delil etme açısından yürürlük alanı bulacaktır. Özellikle delillerin yasallığı gibi başlıklar, CMK'daki düzenlemelere tâbi olacaktır (Tan, 2009).

2.4. Bilirkişilik Uygulamaları ve Adli Tıp Kurumu

Bilirkişi, sahip bulunduğu teknik veya özel bilgisini kullanarak, mahkemeyi maddi mesele ile ilgili bir delil hakkında aydınlatmakla görevlidir. Hâkim veya soruşturma safhasında savcının uygun göreceği kişi veya kurumlar bilirkişi olarak görevlendirilmektedir. 5271 sayılı Ceza Muhakemesi Kanunu (CMK) ve Ceza Muhakemesi Kanununa göre İl Adlî Yargı Adalet Komisyonlarınca Bilirkişi Listelerinin Düzenlenmesi Hakkında Yönetmelik, 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu (HUMK) ile bilirkişilik müessesesini yasal bir zemine oturtmuştur.

CMK'nun 63. maddesi, bilirkişi atanması ile ilgili koşulları düzenlemektedir. Buna göre; "(1)Çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hallerde

bilirkişinin oy ve görüşünün alınmasına re'sen, Cumhuriyet savcısının, katılanın, vekilinin, şüphelinin veya sanığın, müdafinin veya kanunî temsilcinin istemi üzerine karar verilebilir. (Değişik cümle: 3/11/2016-6754/42 md.) Ancak, genel bilgi veya tecrübeyle ya da hâkimlik mesleğinin gerektirdiği hukukî bilgiyle çözümlenmesi mümkün olan konularda bilirkişiye başvurulamaz. (Ek cümle: 3/11/2016-6754/42 md.) Hukuk öğrenimi görmüş kişiler, hukuk alanı dışında ayrı bir uzmanlığa sahip olduğunu belgelendirmedikçe, bilirkişi olarak görevlendirilemez (http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf)." denilmektedir.

CMK'nun 66. maddesi ile, atama kararı ve incelemelerin yürütülmesindeki usul düzenlemektedir. Buna göre, "(1)Bilirkişi incelemesi yaptırılmasına ilişkin kararda, cevaplandırılması uzmanlığı, özel veya teknik bilgiyi gerektiren sorularla inceleme konusu ve görevin yerine getirileceği süre belirtilir." Aynı maddenin son fıkrasında ise, "Bilirkişiye inceleyeceği şeyler mühür altında verilmeden önce bunların listesi ve sayımı yapılır. Bu hususlar bir tutanakla belirlenir. Bilirkişi, mühürlerin açılmasını ve yeniden konulmasını yine tutanakla belirtmek ve bir liste düzenlemekle yükümlüdür (http://ww w.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf)" düzenlemesi getirilmiştir.

CMK, m.67 'Bilirkişi raporu, uzman mütalaası' başlığını taşımaktadır. Bu madde düzenlemesine göre; "(1)İncelemeleri sona erdiğinde bilirkişi yaptığı işlemleri ve vardığı sonuçları açıklayan bir raporu, kendisinden istenen incelemeleri yaptığını ayrıca belirterek, imzalayıp ilgili mercie verir veya gönderir. Mühür altındaki şeyler de ilgili mercie verilir veya gönderilir ve bu husus bir tutanağa bağlanır. (2) Birden çok atanmış bilirkişiler değişik görüşleri yansıtmışlarsa veya bunların ortak sonuçlar üzerinde ayrık görüşleri varsa, bu durumu gerekçeleri ile birlikte rapora yazarlar. (3) (Değişik: 3/11/2016-6754/45 md.) Bilirkişi, raporunda ve sözlü açıklamaları sırasında çözümü

uzmanlığı, özel veya teknik bilgiyi gerektiren hususlar dışında açıklama yapamaz; hâkim tarafından yapılması gereken hukukî nitelendirme ve değerlendirmelerde bulunamaz." denilmektedir. Ayrıca aynı maddenin son fıkrasında, "Cumhuriyet savcısı, katılan, vekili, şüpheli veya sanık, müdafii veya kanunî temsilcisi yargılama konusu olayla ilgili olarak veya bilirkişi raporunun hazırlanmasında değerlendirilmek üzere ya da bilirkişi raporu hakkında, uzmanından bilimsel mütalâa alabilirler (http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf)." düzenlemesi getirilmektedir.

Adli bilirkişilik alanında verilen hizmetler; genel itibariyle olay yeri incelemesinin gerçekleştirilmesi, delillerin toplanması ve laboratuvar incelemeleri ile delillerin analizinin yapılarak sonuç çıkartılması olarak karşımıza çıkmaktadır. Bu noktada en önemli problem, bahse konu hizmetleri yerine getirebilecek adli bilişim uzmanı sayısının yetersizliği ve buna karşın bilişim suçlarının her geçen gün yaygınlaşarak çoğalmasıdır. Adli bilişim, çok yeni bir disiplin olmamasına karşın, ülkemiz için yeni diye nitelendirilebilecek bir kavramdır.

Ülkemizde, bilişim teknolojileri ile ilgili bilirkişilik görevlerinin icrasına yönelik, hukuk sistemimizde yetkilendirilmiş bir adli bilişim uzmanlık alanı henüz mevcut değildir. Bu yönüyle adli bilişim alanındaki bilirkişilik faaliyeti, standart ve yetkin bir eğitime sahip olunmadan, uzmanların asli görevlerinin ifasına katkı sağlamak maksadıyla yürüttükleri ilave bir faaliyet olarak görülmektedir. Bu eksiklikten dolayı, bilişim cihazlarındaki potansiyel yasal delillerin elde edilmesi ve değerlendirilmesi konusunda üniversiteler ve bazı ticari kuruluşlara bilirkişi olarak başvurulmaktadır. Belirtmek gerekir ki, adli bilişim uzmanı, bilgisayar teknolojilerinden anlamanın, bilgisayar mühendisi ya da bilgisayar bilimcisi gibi ünvanlara sahip olmanın ötesinde

ayrı bir uzmanlık dalıdır. Adli bilişim uzmanı, bilişim sistemleri konusunda ileri derecede bilgi sahibi kimsedir (Dülger, 2017).

Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur (Tan, 2009). Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür. Bu sertifika programlarından en çok kabul edilenleri; EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) olarak sayılabilir (Ekizer, 2014).

Son zamanlarda, ülkemizde de adli bilişim uzmanı yetiştirilmesi açısından çeşitli üniversitelerde lisans ve lisansüstü programları oluşturulmaktadır. Ancak resmi bir kurum olarak adli bilişim konusuna eğilmek gerekmektedir ki bu konuda hali hazırda kolluk içerisinde oluşturulmuş birimler ve ATK hizmet vermekte ise de, uzman sayısının yeterli olduğu söylenemeyecektir (Tan, 2009).

Emniyet Genel Müdürlüğü (EGM) 1998 yılında adli bilişim ve ileri teknoloji suçları ile mücadele alanında faaliyetlerine başlamıştır (Alaca, 2008). Ancak özellikle personel konusunda yeterli yatırımın yapılmaması nedeniyle bugün az sayıdaki yetkin personeli ile bu görevleri ifa etmeye çalışmaktadır. Halen ATK ve Jandarma Genel Komutanlığında (JGK) benzer işlevlere sahip yapılanmalar mevcut olup benzer sorunlar bu kurumlarda da yaşanmaktadır (Taşçı ve ark., 2015). Kısacası sorun personelin yetkinliğinde değil sayısal yetersizliktedir.

Adli bilişim alanında verilen hizmetlerin en önemlisi belki de delillerin toplanması sürecidir ki, ülkemizde delillere elkoyma sürecinde işlemler yapılırken

nelere dikkat edileceği hususu ile ilgili standartlar ve sorumluluklar henüz herhangi bir mevzuatta net olarak belirtilmemiştir. Sonuç olarak uygulamada birçok delil, daha en başta geri dönülmeyecek şekilde kaybolabilmektedir. Son zamanlarda mevcut problemlerin çözümü için kolluk kuvvetlerinde çeşitli çalışmalar yapılmaktadır. Örneğin, kolluk kuvvetleri çalışmada standartlaşma sağlamak için kendi akış şemalarını oluşturmaktadırlar (Taşçı ve ark., 2015).

EGM'nde, bilişim suçlarıyla ilgili delil tespitleri ve soruşturma, İstanbul, Ankara ve İzmir'de Siber Suçlarla Mücadele Şube Müdürlükleri tarafından yürütülmektedir. JGK'nda ise; uluslararası standartlara yakın bir laboratuvar, Kriminal Daire Başkanlığı bünyesinde Bilişim Teknolojileri İnceleme Şube Müdürlüğü adı altında açılmış, 15 Eylül 2007 tarihinden itibaren aktif olarak, cep telefonu, sabit disk, SIM kart, multimedya kart ve çeşitli veri kartlarını inceleme konularında hizmet vermektedir. Ayrıca birimde görevli bilişim uzmanları tarafından, Olay Yeri İnceleme Timlerine, bilişim suçlarında olay yeri incelenmesi, delillere el konulması ve muhafazası konusunda eğitim verilmektedir (Çiçek, 2008).

ATK, Adalet Bakanlığı'nın bağlı kuruluşu olarak çalışmakta olan Türkiye'nin en eski ve en önemli resmi bilirkişilik kurumudur. ATK'nun kuruluş tarihi 1 Mart 1913'tür. ATK, adli tıp ve adli bilimler alanında hem eğitim hem de hizmet anlamında çok önemli bir yere sahiptir (İnce ve ark., 2012).

ATK resmi internet sitesinde 'Kuruluş' başlığı altında "Adli Tıp Kurumu, 19.02.2003 tarih, 4810 Sayılı Kanun'la değişik, 14.04.1982 tarih ve 2659 sayılı Kanun'la ilgili olarak adalet işlerinde bilirkişilik görevi yapmak, adlî tıp uzmanlığı ve yan dal uzmanlığı programları ile görev alanına giren konularda diğer adlî bilimler alanlarında

sempozyum, konferans ve benzeri etkinlikler düzenlemek ve bunlara ilişkin eğitim programları uygulamak üzere Adalet Bakanlığına bağlı Adli Tıp Kurumu kurulmuştur. Adalet Bakanlığınca Kuruma bağlı olarak Adlî Tıp Kurumu grup başkanlıkları veya şube müdürlükleri kurulabilir. Adlî Tıp Kurumu grup başkanlıkları bünyesinde bir veya daha çok adlî tıp ihtisas dairesi bulunur." açıklaması getirilmiştir (https://www.atk.gov.tr/adli-tip-kurumu-baskanligi.html).

Adalet Teşkilatı içinde adli bilişim konusunda resmi bilirkişilik yapmak üzere ATK bünyesinde ilk oluşturulan birim, 2004 yılında kurulan ATK FİD Başkanlığı Bilişim ve Teknoloji Suçları Şubesi'dir (Koç ve ark., 2009).

15 Temmuz 2016 tarihindeki darbe girişimi sonrası savcılık ve mahkemelerde adli bilişimle ilgili resmi bilirkişilik talebinin çok fazla artması nedeniyle, FİD bünyesinde bulunan Bilişim ve Teknoloji Suçları ile Ses ve Görüntü İnceleme Şubesi, 15.08.2016 Tarih ve 674 Sayılı KHK ile düzenlenen ve 10.11.2016 Tarih ve 6758 Sayılı Kanun ile yeni kurulan ABİD bünyesine alınmış olup; bu tarih itibariyle adli bilirkişilik faaliyetine devam etmektedir.

25.11.2016 Tarih ve 29899 Sayılı Resmi Gazetede yayınlanan Adli Tıp Kurumu Kanunu Uygulama Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik ile yürürlüğe giren Adli Tıp Kurumu Kanunu Uygulama Yönetmeliğinin 14/A. maddesi ABİD'nin çalışma alanı ve yapılanması konusunda düzenlemeler getirmektedir. Buna göre;

"Adli Bilişim İhtisas Dairesi

Madde 14/A –(Ek:RG-25/11/2016-29899)Adli Bilişim İhtisas Dairesi'nde uzman ya da mühendis bir başkan, yeteri kadar uzman, mühendis, tekniker ve yardımcı personel bulunur. Adli Bilişim İhtisas Dairesi aşağıdaki birim ve şubelerden oluşur:

a) Veri inceleme şubesi,

b) Mobil cihazlar inceleme şubesi,

c) Kriptoloji ve elektronik cihazlar inceleme şubesi,

d) Ses ve görüntü inceleme şubesi,

e) ARGE şubesi,

f) İş Tasnifi ve önceliği bürosu.

Her şubede uzman ya da mühendis bir şube müdürü ile yeteri kadar personel bulunur.

İş Tasnifi ve Önceliği Bürosu'nda yeteri kadar uzman, mühendis ile tekniker görev yapar.

Adli Bilişim İhtisas Dairesi'nin görevleri ve çalışma usulleri şunlardır:

a) Mahkemeler, hâkimlikler, Cumhuriyet Savcılıkları tarafından gönderilen bilişim suçları, ses ve görüntü analizi ile ilgili konularda gerekli incelemeleri yaparak sonucu bir raporla mahalline bildirir.

b) Bilişim alanı ile ilgili teknik personel yetiştirilmesi ve yeterliliklerinin sınanması hususlarında faaliyet gösterir.

c) Bilişim alanı ile ilgili her türlü yazılım ve donanım geliştirilmesi hususlarında projeler yürütür.

d) İlgili şubelerde ekipler halinde çalışılır. Her bir ekibin liderinin uzman ya da mühendis olması esastır.

e) Gönderilen deliller Adli Tıp Kurumu Emanet Birimi'nden İş Tasnifi ve Önceliği Bürosu'nca teslim alınır. Söz konusu büro tarafından delil üzerinde yapılacak incelemenin türü, gönderen makam yazısında belirtilen hususlar da gözetilerek hangi şube ya da şubeler tarafından inceleneceği, önceliğin hangi şubeye verileceği, delilin bu Yönetmeliğin 20 nci maddesi kapsamınca önceliği bulunup bulunmadığı belirlenir ve buna göre ilgili şubeye tasnifi ve teslimi yapılır.

f) Adli Bilişim İhtisas Dairesi, faaliyet alanlarına yönelik diğer hususlarda bu Yönetmeliğin ilgili hükümlerine tabidir (http://www.yayin.adalet.gov.tr/dosyalar/pdf/atkm_2017.pdf)."

ABİD bünyesinde birçok birim ve şube barındırmakta; elektronik ve dijital deliller üzerinde inceleme yaparak Cumhuriyet savcılıkları ve mahkemelere rapor hazırlamaktadır. Olay yerinde bulunabilecek bilgisayar kasaları, sabit diskler, harici sabit diskler, modemler, disketler, CD, DVD, flash diskler, elektronik devreler ve benzeri her türlü bilişim delillerinin incelemesi ve raporlandırılması yapılabilmektedir.

Adli bilişim alanında resmi bilirkişilik hizmetini bünyesinde bulunan Veri İnceleme Şubesi, Mobil Cihazlar İnceleme Şubesi, Kriptoloji ve Elektronik Cihazlar İnceleme Şubesi ile Ses ve Görüntü İnceleme Şubesi aracılığıyla gerçekleştiren ABİD'nin görevleri, ATK resmi internet sitesinde " Mahkemeler ile hakimlikler ve

savcılıklar tarafından talep edilen bilişim ile ilgili konularda gerekli incelemeleri yapmak; veri toplama, inceleme, depolama veya aktarma işlevi gören bilişim sistemleri ile her türlü sayısal ve elektronik materyal üzerinde inceleme, araştrma ve analizleri yapmak, sonuçlarını bir raporla tespit etmek." olarak belirtilmektedir (https://www.atk.gov.tr/adli-tip-kurumu-baskanligi.html).

ABİD adli bilirkişilik hizmetinin yanı sıra, bilişim alanı ile ilgili teknik personel yani adli bilişim uzmanı yetiştirilmesi ve bu personelin yetkinliklerinin sınanması; bilişim alanı ile ilgili her türlü yazılım ve donanım geliştirilmesi hususlarında da görevlendirilmiştir (http://www.yayin.adalet.gov.tr/dosyalar/pdf/atkm_2017.pdf).

Bilişim suçları ile ilgili adli vakaların artışı ve özellikle 15 Temmuz 2016 darbe girişimi sonrası ortaya çıkan resmi bilirkişilik talebinin çok fazla artması nedeniyle bilirkişilik hizmetini yürüten ve tüm ülke çapında hizmet veren bir birim olan ATK FİD Bilişim ve Teknoloji Suçları Şubesi'nin eski mevzuatın değiştirilmesi suretiyle FİD çatısı altından çıkarılıp, ABİD haline getirilmesi, yargılama sürecinin hızlı ve etkin sonuçlandırılması açısından son derece yerinde bir düzenleme olmuştur.

ABİD'nin bilişim ve internet suçlarının daha fazla işlendiği İstanbul ve Ankara'da olmak üzere iki büyük ilde faaliyet vermesi; hizmet talep edilen dosyaların çok daha hızlı ve etkin bir şekilde sonuçlandırılmasını ve dijital incelemelerin süratle yapılmasını sağlamaktadır. Bununla berbaber, ABİD'nin, adli bilişim bilirkişilik hizmet türlerine göre ayrı birim ve şubeler halinde yapılandırılmasının da, resmi bilirkişilik hizmetinin sunulmasına uzmanlaşma, etkinlik ve süratlilik kattığı değerlendirilmektedir.

3. YÖNTEM VE GEREÇLER

Çalışmamız, Adli Tıp Kurumu (ATK) bünyesinde adli bilişim alanında 10 yıllık süreç içerisinde bilirkişilik hizmeti verilen dosyaları kapsayan iki ayaklı bir inceleme içermektedir. Çalışmamızın ilk ayağında; ATK Fizik İhtisas Dairesi (FİD) Bilişim ve Teknoloji Suçları Şubesinde 2009, 2010 ve 2011 yılları içinde bilirkişilik hizmeti verilen toplam 81 dosya taranmıştır. Çalışmamızın ikinci ayağında; 2012 – 2016 yılları arasında FİD Bilişim ve Teknoloji Suçları Şubesi'ne gelen 337 adet ve 2017-2018 yılları içerisinde Adli Bilişim İhtisas Dairesi (ABİD)'e gelen 2.458 adet dosya sadece sayısal verileri dahil edilerek istatistiki olarak incelenmiştir. Sonuç olarak, bilirkişilik hizmeti verilen 81 dosyadan veriler tarama usülü toplanmış, Adli Bilişim İhtisias Dairesine gelen 2.458 adet dosyadan da sayısal veriler derlenmiştir. Bunun sonucunda verilerin betimsel istatistiği ve grafiksel gösterimleri hazırlanmıştır (Demir, 2017).

Çalışmamız kapsamına; çalışmamızı doğrudan bilişim ve internet suçları ile sınırlandırabilmek amacıyla 2009-2016 dönemi içinde FİD bünyesindeki Ses ve Görüntü İnceleme Şubesi'ne ve yine 2017-2018 yılları içerisinde ABİD bünyesindeki Ses ve Görüntü İnceleme Şubesi'ne gelen dosyalar dahil edilmemiştir.

Çalışmamızın amacı; bilişim suçlarının yıllara ve türlerine göre dağılım oranları, dosyalara verilen hizmet türü, dosyaların geldiği yer ve dosyanın gönderildiği merci, sanık ve mağdur cinsiyeti, incelenen materyal tipleri, verilen hizmete göre ekspertiz sayısı, gözlemlenen suç tipleri ve suç tiplerinin teknik bilgi gerektirip gerektirmediği, ihlal edilen haklar ve zarar tipleri, hizmet verilen ekspertiz sayısı ve gelen dosyalar için hizmet verilememe nedenleri yönünden değerlendirmeler yapılarak, adli bilişim alanındaki bilirkişilik hizmetleri yönünden gerek mevzuatta ve gerekse uygulamada

eksiklikler barındıran, iyileştirilmesi gereken hususlara işaret etmektir. Ayrıca 15 Temmuz 2016 darbe girişimi sonrası adli bilişimle ilgili resmi bilirkişilik talebiyle gelen adli dosyalarda artış olduğunu düşündüğümüzden, çalışmamıza 2012 - 2018 yılları arasındaki dosya sayılarını içerir istatistiki veriler dahil edilmiş ve dosya artışının tespit edilmesi amaçlanmıştır.

Bu çalışmamızda yöntem olarak istatistiksel araştırmaya başvurulmuştur. Araştırma modelleri; verilerin toplanması ve çözümleme yapılabilmesi için koşulların çalışma amacına uygun olarak oluşturulması ile ortaya çıkmaktadır (Karasar, 2005).

İstatistik, çok sayıda dış etkene bağlı nesne, varlık ya da olayların sayısal dökümü yapılabilen özelliklerini incelemeye yarayan bir teknik ya da yöntem kümesidir. İstatistiksel araştırmanın amacı; raslantıyı göz önünde tutarak olayları belirleyen genel yasaları, genel eğilimi ortaya çıkartmak, ana nedenleri aramak, olaylara arasındaki ilişkileri ve bağlantıları bulmak, böylece türlü yönetim, bilim ve teknik dallarında yapılacak kestirimlere, öngörülere, alınacak kararlara ve girişilecek eylemlere yardımcı olmaktır (Aydın, 2016).

Çalışmamızda ATK FİD Bilişim ve Teknoloji Suçları Şubesi'ne bilirkişilik hizmeti almak üzere adli kurumlar ve kolluk tarafından gönderilmiş olan dosyalar içerisindeki veriler anlamlandırılarak bir sınıflandırmaya tabi tutulmuştur. Her bir veri kendi sınıflandırması içinde kayıt altına alınmıştır. Bu aşamadan sonra istatistiksel sonuçlara ulaşabilmek için elde edilen veriler analiz edilmiş; verilerin kendi aralarında karşılaştırmaya tabi tutulmasıyla anlamlı sonuçlar elde edilmeye çalışılmıştır.

2009 -2011 yılları arasında kalan dönemde ATK FİD'ne gelen dosyalar açısından, suçu oluşturan eylemin teknik bilgi gerektirip gerektirmemesi bağlamında suçun günlük

yaşama yayılmasında gözlenen yoğunluk ve bilişim teknolojilerinin kullanımının yıllara göre gösterdiği artış tespit edilmek istenmiştir.

Yine aynı dönemde ATK FİD'ne gelen dosyalar yönünden suçun verdiği zararın türleri ve yıllara göre artış gösterip göstermediği ayrı bir başlık altında değerlendirilmiştir.

Bunun gibi, 2009 -2011 yılları arasında kalan dönemde ATK FİD'ne gelen dosyalara verilen hizmetin ekspertiz sayısı oranında incelenmesi ve ekspertiz materyallerinin tespiti ile, suçun toplum içindeki yaygınlığı ve özellikle bilişim suçları dışında kalan diğer suçların işlenmesi sırasında bilişim sistemlerinin kullanım oranları, ayrıca dosya gönderen merci ve dosyanın geldiği yer incelemesi ile suçların ülke içerisindeki dağılımı ve suç kastının yoğunluğu gibi noktalarda sonuçlar sunulmuştur.

Aynı dönemde ATK FİD'ne gönderilen dosyalar ile ilgili hizmet verilebilme oranı ve hizmet verilemediği yahut eksik hizmet verilebildiği durumlarda sorunun neden kaynaklandığı çalışmamızın inceleme alanında olan hususlardan biridir. Böylelikle, bilirkişilik sistemi içerisinde yaşanan sorunlar tespit edilmiş ve çözüm önerileri sunulmuştur.

ATK FİD'ne 2009, 2010, 2011 yılları arasında gelen dosyalara ait elde edilen istatistiklere, aynı birime adli bilirkişilik hizmeti talebiyle 2012 – 2016 yılları arasında gönderilen dosyalara ait sayısal veriler ile ATK bünyesinde 2017 yılı itibariyle hizmete başlayan Adli Bilişim İhtisas Dairesi'ne 2017 -2018 yılları içerisinde gelen adli bilişimle ilgili dijital delil ve adli bilirkişilik dosyalarına ait sayısal veriler de çalışmamız verilerine eklenmiştir.

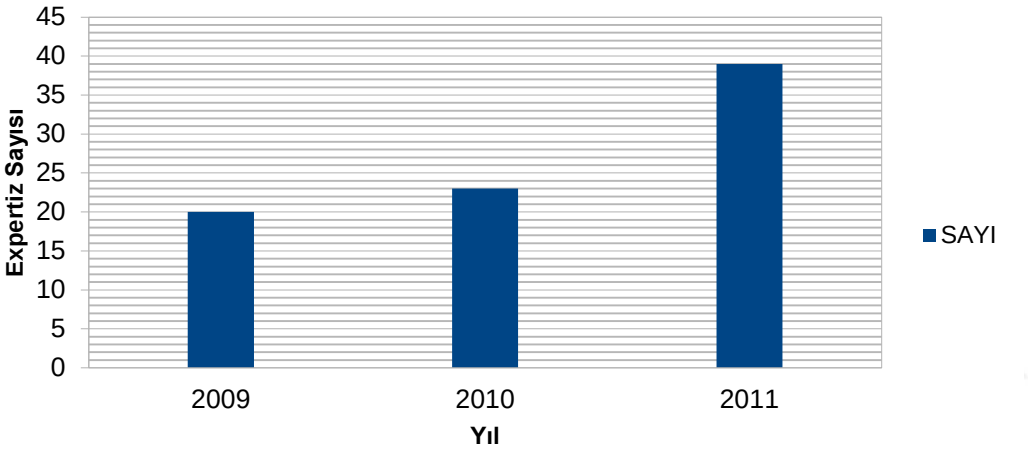
Yaptığımız değerlendirmede, genel olarak inceleme kapsamına giren 2009- 2018 yıllarını kapsayan 10 yıllık bir bir süreç içerisinde bilişim suçlarının, internet aracılığıyla işlenen suçların ve suçta delil olarak bilişim araçlarının ve internetin kullanılmasının gösterdiği artış ile bununla bağlantılı olarak ATK bünyesinde adli bilişim alanında resmi bilirkişilik hizmeti talep edilen dosya sayılarındaki artış ortaya konulmuştur.

4. BULGULAR

Çalışmamız kapsamında 2009 - 2010 - 2011 yılları arasında yapılan dosya taramalarımız istatistiki olarak grafikler ile gösterilmiştir.

Ayrıca 2012-2016 yılları arasında Adli Tıp Kurumu Fizik İhtisas Dairesi Bilişim ve Teknoloji Suçları Şubesi'ne ve 2017 ile 2018 yılları içerisinde Adli Bilişim İhtisas Dairesi'ne gelen dosyaların toplam sayıları da tez çalışmamıza dahil edilerek grafikler halinde sunulmuştur.

2009 – 2011 yılları arasında gelen dosya sayısı



Şekil 1: 2009 – 2011 yılları arasında gelen dosya sayısı

Yukarıdaki şekilde de görüleceği üzere, ATK FİD Bilişim ve Teknoloji Suçları Şubesi 'ne gönderilen dosya sayısı; 2009 yılında 20, 2010 yılında 22 ve 2011 yılında 39 adettir.

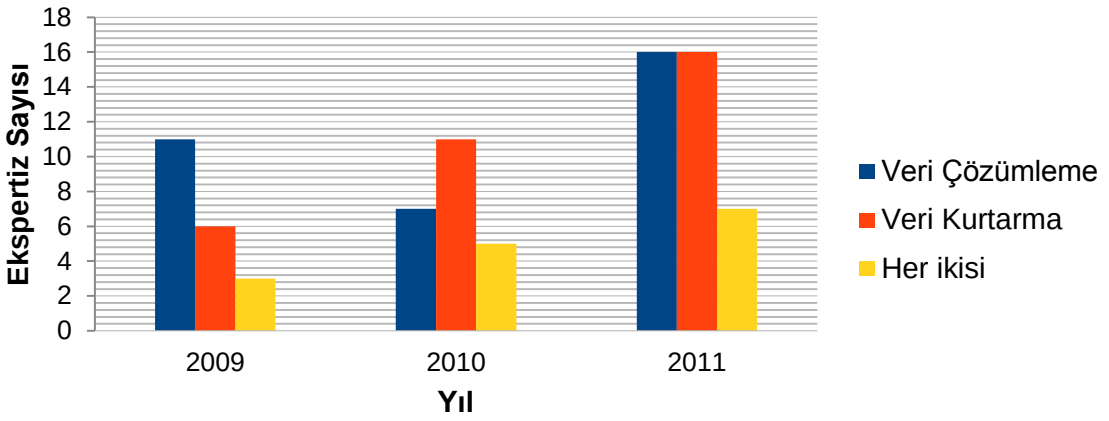
Buna göre, gönderilen dosya sayısında, 2010 yılında %15'lik bir artış yaşanmış, ardından 2011 yılında 2010 yılına göre %69'luk bir artış daha gerçekleşmiştir.

Genel bir değerlendirme ile, 2009 ile 2010 yılları arasındaki fark çok dikkat çekici değilken, 2011 yılında ATK FİD'ne gönderilen dosya sayısında neredeyse iki katı oranında ani ve ciddi bir artış görüldüğü açıktır.

Dolayısıyla elde edilen bulgulardan açıklıkla anlaşılacağı üzere, gönderilen dosya sayıları önceki yıllara oranla önemli miktarda artmaktadır.

Özellikle inceleme kapsamımıza giren 2011 yılı içerisindeki artış ciddi bir suç yoğunluğunu ortaya koymaktadır.

Hizmet türlerine göre ekspertiz sayısı



Şekil 2: Hizmet Türlerine göre ekspertiz sayısı

Yukarıdaki şekilde de görüleceği üzere, ATK FİD Bilişim ve Teknoloji Suçları Şubesi tarafından 2009 yılında 11 adet veri çözümleme, 6 adet veri kurtarma işlemi gerçekleştirilmiş, 3 adet dosyada ise her iki işleme de ihtiyaç duyulmuştur.

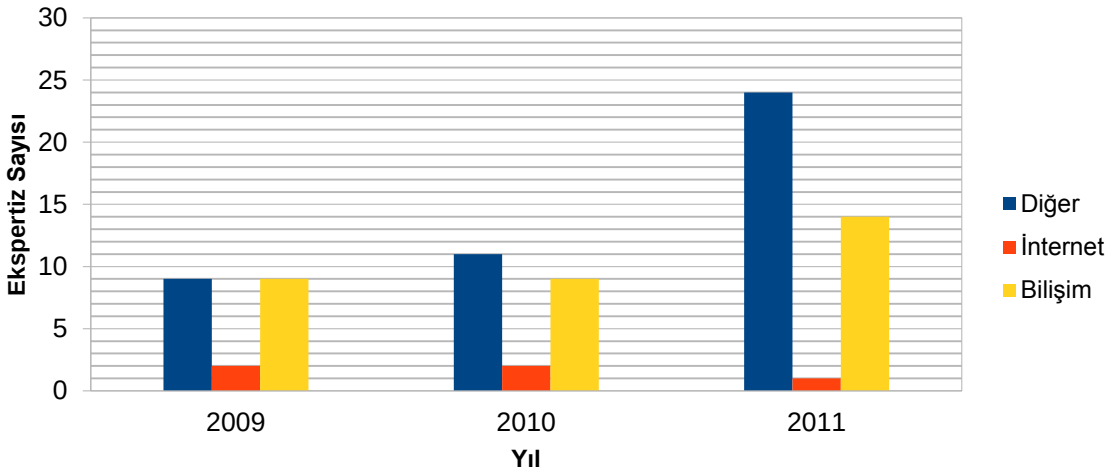
2010 yılında 7 adet veri çözümleme, 11 adet veri kurtarma ve 5 adet her iki hizmete de başvurulduğu görülmektedir.

2011 yılında ise, 16 adet veri çözümleme, 16 adet veri kurtarma hizmeti verilmiş; 7 adet dosyada her iki hizmete de başvurulmuştur.

Bulgulara göre, 2010 yılında verilen veri çözümleme hizmeti azalma göstermiş gibi görünse de, onun yerini veri kurtarma hizmetinin aldığı ve genel olarak oransal bir artış olduğu ortadadır.

Özellikle 2011 yılında veri çözümleme hizmetinin %77'lik bir artış gösterdiği, yine veri kurtarma hizmetinin %45 oranında arttığı; her iki hizmetin verildiği yani verilen hizmet kapsamında hem veri çözümleme hem de veri kurtarma işlemlerinin yapıldığı ekspertiz sayısının ise % 40'lık bir artış gösterdiği görülmektedir.

Suç türlerine göre ekspertiz sayısı



Şekil 3: Suç türlerine göre ekspertiz sayısı

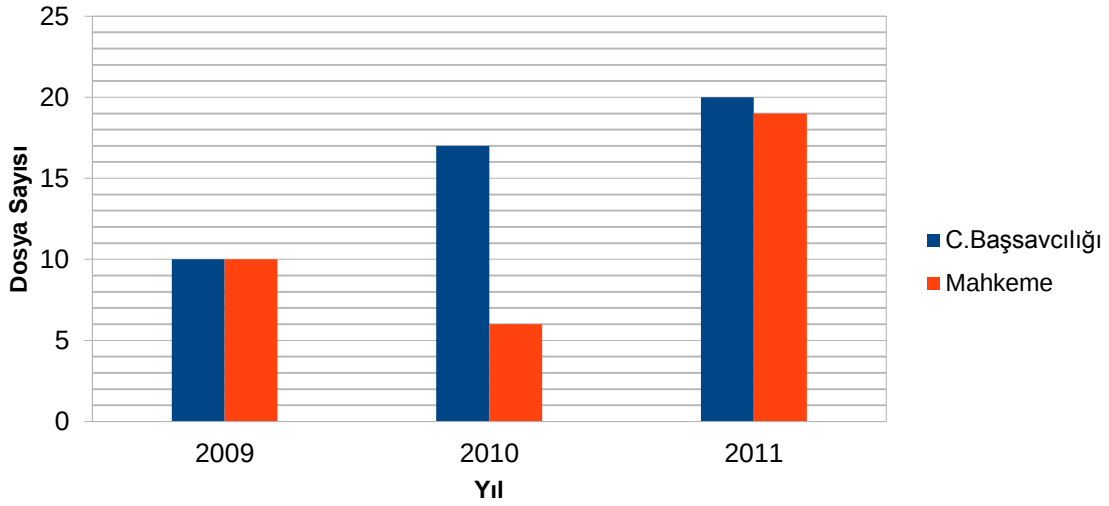
Şekil 3'te görüleceği üzere, ATK FİD tarafından 2009 yılında bilişim alanında 9 adet ve internet aracılığıyla işlenen suçları içerir 2 adet dosyaya hizmet verilmiş; bu kategoriler dışında kalan ve suçun işlenişi sırasında bilişim sistemleri kullanılan yahut suçun çözümlenmesinde bilişim materyallerine delil olarak başvurulan suçları içerir 9 adet dosya incelenmiştir.

2010 yılında bilişim suçları ve internet aracılığıyla işlenen suçlara ilişkin gönderilen dosya sayıları aynı kalırken, diğer suçlar ile ilgili dosyalar 11'e yükselmiş, böylece ekspertiz sayısında %22'lik bir artış olmuştur.

2011 yılında, bilişim alanında işlenen suçlara ilişkin dosyalar %55 oranında ciddi bir artış göstermiş, buna karşılık internet aracılığıyla işlenen suçlarda %50'lik bir düşüş olmuştur.

Tarafımızca buradaki düşüş çok anlamlı bulunmamaktadır, zira 2010 yılı itibariyle ATK FİD'ne gelen internet aracılığı ile işlenen suç dosyası 2 adet iken 2011 yılında 1'e düşmüştür; ülkemizde internetin yeni bir alan olduğu düşünülürse buradaki 1 dosyalık oynama karşılığına denk gelen oran çok anlamlı kabul edilemeyecektir.

Dosya gönderen merci



Şekil 4: Dosya gönderen merci

Yukarıdaki şekilde de görüleceği üzere, ATK FİD Bilişim ve Teknoloji Suçları Şubesi'ne Türkiye kapsamında her ilin Cumhuriyet Başsavcılıkları ve Ceza Mahkemeleri tarafından dosya gönderilmektedir.

2009 yılında Cumhuriyet Başsavcılığından gelen dosya sayısı 10 adet olup, çeşitli mahkemelerce yollanan dosya sayısına eşittir.

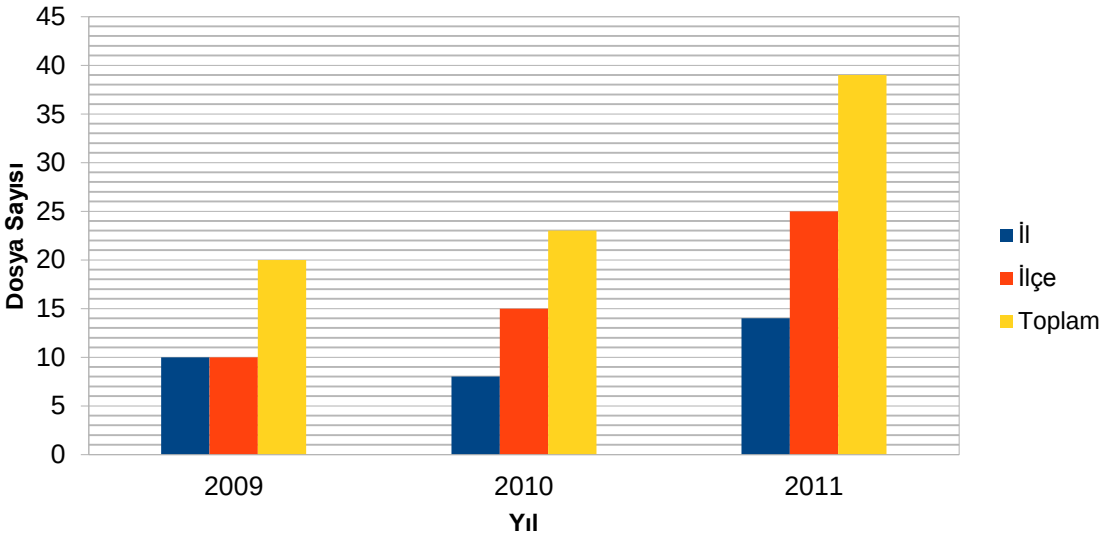
2010 yılında Cumhuriyet Başsavcılığından gelen dosya sayısı 17, çeşitli mahkemelerce yollanan dosya sayısı 6 adettir.

2011 yılı içerisinde ise, Cumhuriyet Başsavcılığından gelen dosya sayısı 20 adede, çeşitli mahkemelerce yollanan dosya sayısı 19 adede çıkmıştır.

Her ne kadar 2010 yılı içerisinde mahkemelerce gönderilen dosya sayısında belli bir düşüş gözlenmekteyse de, genel olarak gönderilen toplam dosya sayısında artış olduğu, dolayısıyla Cumhuriyet Başsavcılıklarınca gönderilen dosyalardaki artışın bir denge yarattığı söylenebilecektir.

2011 yılında ise hem Cumhuriyet Başsavcılıklarından hem de mahkemelerden gelen dosya sayılarının belli bir oranda arttığı görülmektedir.

Dosyanın geldiği yer



Şekil 5: Dosyanın geldiği yer

Şekil 5'te görüleceği üzere, ATK FİD'ne Türkiye kapsamında il ve ilçelerden gönderilen dosya sayıları yıllar içerisinde genel itibariyle artış göstermiştir.

2009 yılında ilden gelen dosya sayısı ile ilçeden gelen dosya sayısı birbirine eşittir.

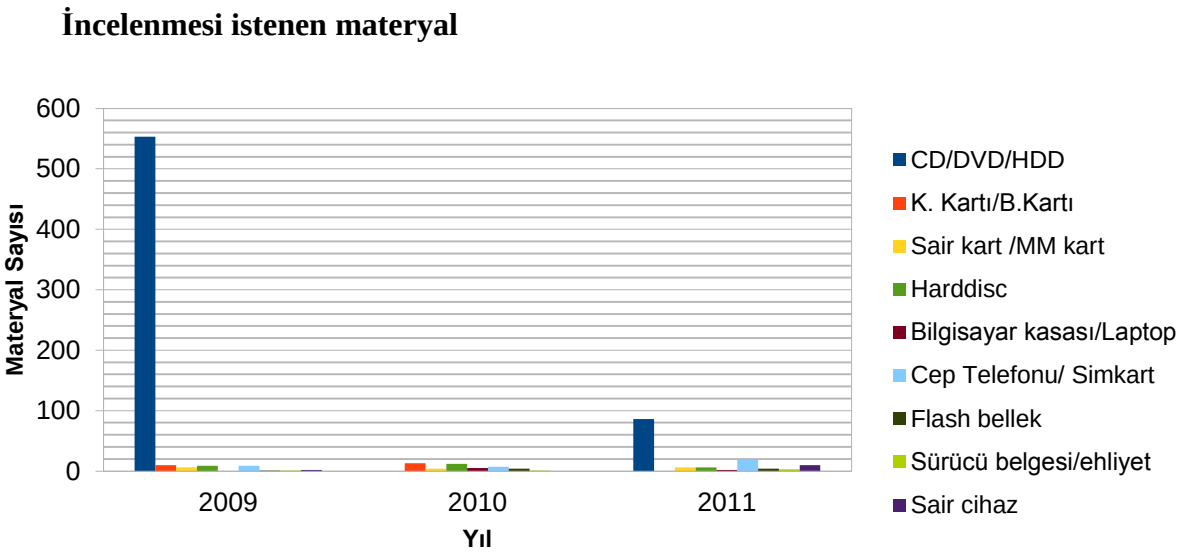
2010 yılında ilden gönderilen dosya sayısında düşüş görülmekteyse de, dikkat çekici olarak ilçelerden gelen dosya sayıları 10'dan 15'e yükselerek, yarı oranında artmıştır.

Yine 2011 yılı içerisinde hem ilden hem de ilçeden gelen dosya sayılarında artış olduğu görülmektedir.

2010 yılında ilden gönderilen dosya sayısı 8 iken 2011 yılında bu sayının 14'e çıktığı görülmektedir.

Ancak, 2011 yılında özellikle ilçeden gönderilen dosya sayıları 15'ten 25'e yükselerek bu defa %66 oranında bir artış yaşanmıştır.

Burada özellikle dikkat çekici olan nokta, yıllar içerisinde ilçeden gönderilen dosya sayılarındaki ciddi yükselişlerdir.



Şekil 6: İncelenmesi istenen materyal

Şekil 6'da görüleceği üzere, ATK FİD'ne çok çeşitli bilişim materyalleri gönderilmektedir. Çalışmamızda yakın materyaller gruplandırılarak bir değerlendirme yapılması amaçlanmıştır.

Genel itibariyle CD/DVD/HDD şeklinde gruplanan disk materyalleri 2009 ve 2011 yılları içerisinde en fazla sayıda ekspertiz hizmeti verilen grup olmuştur. 2009 yılında ATK FİD'ne incelenmek üzere 553 adet, 2011 yılında 86 adet CD/DVD/HDD materyalinin göderildiği anlaşılmaktadır. 2010 yılında ise bu gruba dahil bir materyalin incelenmediği anlaşılmaktadır.

En fazla hizmet talep edilen bu grubu, cep telefonları izlemektedir. ATK FİD'ne incelenmek üzere 2009 yılında 9 adet, 2010 yılında 7 adet ve 2011 yılında 19 adet cep telefonu ve sim kart gönderilmiştir.

Üçüncü sırada hard disc incelemeleri gelmektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 9 adet, 2010 yılında 12 adet ve 2011 yılında 6 adet hard disc gönderilmiştir.

Kredi kartları ve bankamatik kartları bu grubu takip etmektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 10 adet, 2010 yılında 13 adet banka ve kredi kartı gönderilmiştir. 2011 yılında ise bu gruba dahil bir materyalin incelenmediği anlaşılmaktadır.

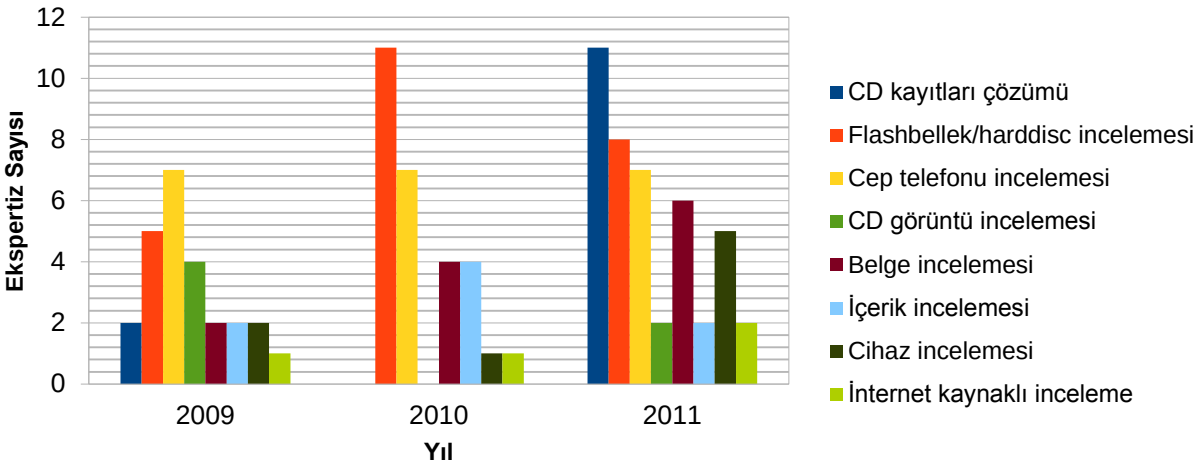
Sair cihazlar beşinci sırada yer almaktadır. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 2 adet, 2011 yılında 10 adet sair cihaz gönderilmiştir. 2010 yılında ise bu gruba dahil bir materyalin incelenmediği anlaşılmaktadır.

Flash bellekler, sair cihazları izleyen kategori olarak tespit edilmiştir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 1 adet, 2010 yılında 4 ve 2011 yılında 4 adet flash bellek gönderilmiştir.

Bir sonraki kategori bilgisayar kasaları ve laptoplar olarak gözlenmektedir. ATK FİD'ne incelenmek üzere 2010 yılında 5 adet, 2011 yılında 2 adet bilgisayar kasası ve laptop gönderilmiştir. 2009 yılında ise bu gruba dahil bir materyalin incelenmediği anlaşılmaktadır.

Son sırada yer alan kategori sürücü belgeleridir. ATK FİD'ne incelenmek üzere 2009 yılında 1 adet, 2010 yılında 1 adet ve 2011 yılında 3 adet sürücü belgesi gönderilmiş vesürücü belgeleri en az sayıda gönderilen materyal olarak tespit edilmiştir. gönderilmiştir.

Verilen hizmete göre ekspertiz sayısı



Şekil 7: Verilen hizmete göre ekspertiz sayısı

Yukarıdaki şekilde görüleceği gibi, ATK FİD'nde çok çeşitli bilirkişilik hizmetleri verilmektedir. Çalışmamızda nitelik itibariyle benzer hizmetler gruplandırılarak bir değerlendirme yapılması amaçlanmıştır.

Genel itibariyle en fazla bilirkişilik talep edilen ekspertiz grupları arasından, 'flashbellek/harddisk incelemeleri' şeklinde gruplanan bilirkişilik hizmeti en fazla talep edilen grup olmuştur. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 5 adet, 2010 yılında 11 adet, 2011 yılında ise 8 adet flashbellek/harddisk incelemesi talebi gelmiştir.

Bunu grubu, cep telefonu incelemeleri izlemektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 7 adet, 2010 yılında 7 adet, 2011 yılında 7 adet cep telefonu incelemesi talebi gelmiştir.

Üçüncü sırada CD kayıt çözümlemeleri gelmektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 2 adet, 2011 yılında 11 adet CD kayıt çözümlemesi talebi geldiği görülmektedir. 2010 yılında ise bu gruba dahil bir inceleme talebi gelmediği anlaşılmaktadır.

Dördüncü sıradaki ekspertiz grubu belge incelemeleridir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 2 adet, 2010 yılında 4 adet, 2011 yılında 6 adet belge incelemesi talebi gelmiştir.

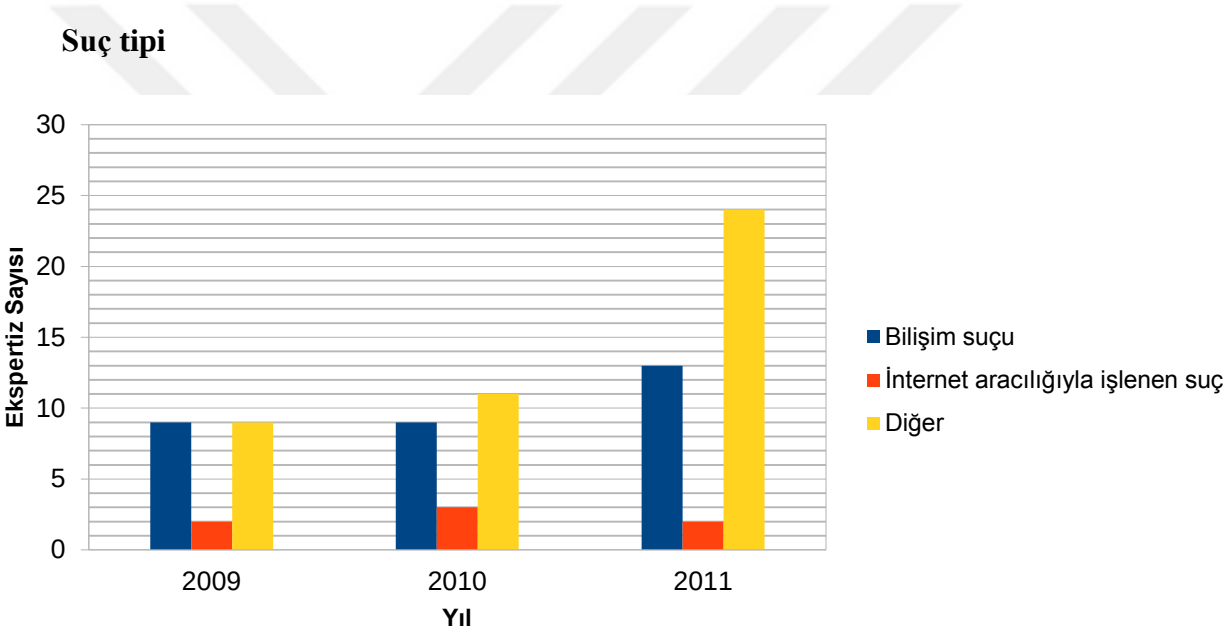
Bu grubu içerik ve cihaz incelemeleri takip etmektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 2 adet içerik ve 2 adet cihaz incelemesi, 2010 yılında 4 adet içerik ve 1 adet cihaz incelemesi ve 2011 yılında 2 adet içerik ve 5 adet cihaz incelemesi talebi gelmiştir.

Altıncı sıradaki ekspertiz grubu CD görüntü kaydı incelemeleridir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 4 adet, 2011 yılında 2 adet CD kayıt

çözümlemesi talebi geldiği görülmektedir. 2010 yılında ise bu gruba dahil bir inceleme talebi gelmediği anlaşılmaktadır.

Son sırada yer alan kategori olarak internet kaynaklı incelemeler izlemektedir. Buna göre; ATK FİD'ne incelenmek üzere 2009 yılında 1 adet, 2010 yılında 1 adet, 2011 yılında 2 adet belge incelemesi talebi gelmiştir.

Görüleceği üzere, buradaki sıralama bir önceki şekilde yer verilen 'incelenmesi istenen materyal' kategorisi ile belli bir uyum içerisinde ilerlemektedir.



Şekil 8: Suç tipi

ATK FİD'ne bilirkişilik hizmeti talebiyle gönderilen dosyalardaki suç tiplerine göre yapılacak değerlendirme çalışmamızın en önemli bölümünü oluşturmaktadır.

Burada yapılan gruplama, çalışmanın sistematiği ile örtüşecek şekilde; bilişim alanında suçlar, internet aracılığıyla işlenen suçlar ve bu gruplar içerisine girmemekle birlikte suçun işlenmesinde bilişim sistemlerinin yahut internetin kullanıldığı, bir diğer

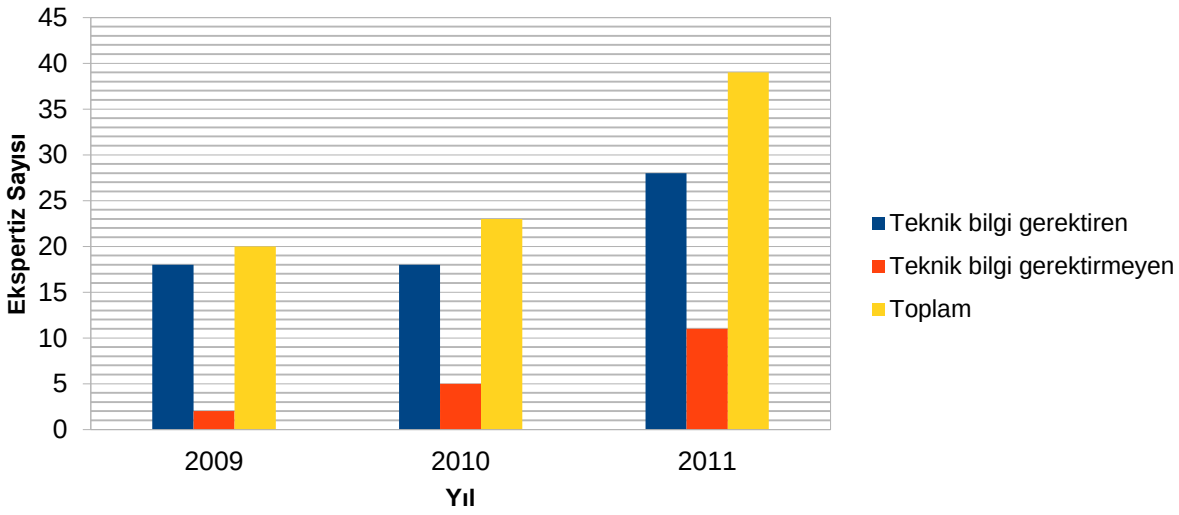
değişle bir şekilde delil olarak bilişim ve/veya internet materyallerine başvurulan sair suçlar olarak husule getirilmiştir.

Şekildeki grafikde de görüleceği üzere, bilişim alanında suçlarla ilgili ekspertiz talebi gerek 2009 gerekse 2010 yılında 9 adettir; ancak 2011 yılı itibariyle bu sayı 13'e yükselmekte ve %44 oranında artmaktadır.

İnternet aracılıyla işlenen suçlar ise, aynı yoğunluk ve düzenli artışı göstermemektedir. Buna göre, FİD'ne 2009 yılında bu içerikte 2 adet; 2010 yılında 3 adet; yine 2011 yılında 2 adet talep gelmiştir.

Bu gruplar dışında kalan ve suçun işlenmesinde bilişim sistemlerinin yahut internetin kullanıldığı, bir diğer değişle bir şekilde delil olarak bilişim ve/veya internet materyallerine başvurulan sair suçlar 2009 yılında 9 adet talep olurken, 2010 yılında bu sayı 11'e çıkmış ve %22'lik bir artış ortaya çıkmıştır. 2011 yılında ise bu sayı 24'e çıkmış ve %84'lük çok ciddi bir artış göstermiştir.

Teknik bilgi gerekli olup olmadığı yönünden suç tipi



Şekil 9: Teknik bilgi gerekli olup olmadığı yönünden suç tipi

ATK FİD'ne bilirkişilik hizmeti talebiyle gönderilen dosyalardaki suç tiplerine göre yapılan değerlendirmede; suç işlenme yaygınlığı ve çeşitliliği ortaya konulmuştur.

Bununla birlikte, bilişim alanında ve internet aracılığıyla işlenen suçların toplumun her kesiminde yaygınlaştığını tespit etmek, ancak suçların teknik bilgi gerektiren bir düzeyde daha fazla işlenebildiğini ortaya koymakla mümkündür.

Bu anlamda e-posta aracılığıyla bir başkasına tehdit içerir e-mail göndermek vb. eylemler 'teknik bilgi gerektirmeyen suçlar' kategorisinde yer alırken, bir banka veya kredi kartının sahte olarak düzenlenmesi gibi suçun icra edilebilmesi için bilişim araçlarının kullanımı alanında belli bir düzeyde teknik bilgi kullanılan eylemler 'teknik bilgi gerektiren suçlar' kategorisinde değerlendirilmiştir.

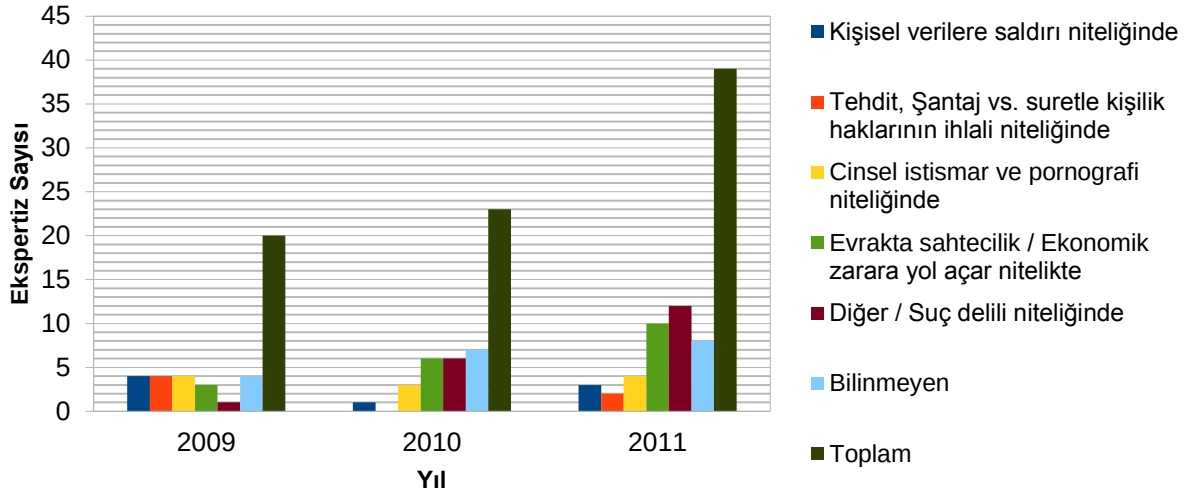
Teknik bilgi gerektirmeyen bilişim ve internet suçları 2009 yılında 2 adet, 2010 yılında 5 adet ve 2011 yılında 11 adet olarak kaydedilmiş ve her yıl belli bir düzeyde artış sergilemiştir.

Teknik bilgi gerektiren bilişim ve internet suçları, 2009 ve 2010 yıllarında 18 adet olarak aynı sayıda gözlenmiştir.

Ancak 2011 yılında birden bire teknik bilgi gerektiren suçlarda ciddi bir artış yaşandığı ve 2011 yılı içinde ATK FİD tarafından teknik bilgi gerektiren 28 adet dosyaya bilirkişilik hizmeti verildiği görülmektedir.

Dolayısıyla 2011 yılı itibariyle ciddi bir artış ortaya çıkmış ve %55'lik bir artış gözlemlenmiştir.

İhlal edilen haklar ve zarar nevi



Şekil 10: İhlal edilen haklar ve zarar nevi

ATK FİD'ne bilirkişilik hizmeti talebiyle gönderilen dosyalardaki suç tiplerine göre yapılan değerlendirme sonrasında, bu suçların doğurduğu zarar ve bu suçlarla ihlal edilen hak nevilerinin tespiti önem arz etmektedir.

ATK FİD'nde tutulan dosya örneklerinin sınırlı dosya bilgisi içermesi nedeniyle, değerlendirme içerisine bilinmeyen dosyalar da eklenmiştir.

Ayrıca aynı hakkı ihlal eden yahut aynı neviden zarar doğuran suçlar kategorize edilme yoluna gidilmiştir.

Buna göre; kişisel verilere saldırı niteliğinde olan, cinsel istismar ve pornografi niteliğinde olan ve ekonomik zarara yol açan suçlar ayrı ayrı gruplar olarak değerlendirmeye alınmıştır.

2009 yılında kişisel verilere zarar niteliğinde 4 adet dosyanın gönderildiği, 2010 yılında bu sayının 1'e düştüğü ve 2011 yılında 3 adet dosyanın kaydedildiği görülmektedir.

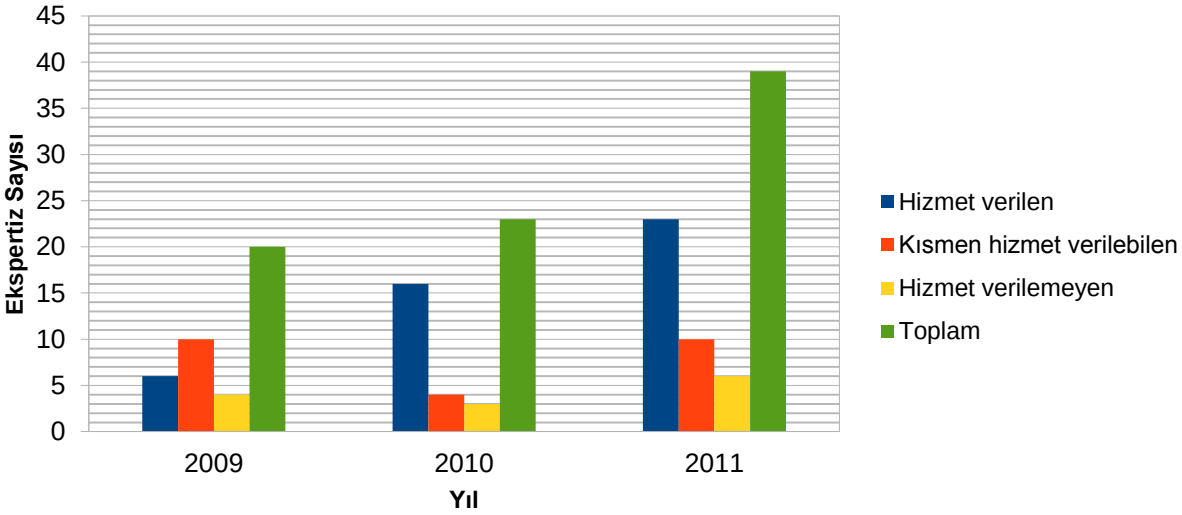
Kişilik haklarının ihlali niteliğinde zarar doğuran suçlara ilişkin olarak 2009 yılında 4 adet ve 2011 yılında 2 adet dosya gönderildiği; 2010 yılında ise kişilik haklarının ihalil niteliğinde zarar doğuran suçlara ilişkin hiç dosya kaydedilmediği görülmektedir.

Cinsel istismar ve pornografi niteliğinde zarara yol açan suçları içerir 2009 yuılında 4, 2010 yılında 3 ve 2011 yılında 4 adet dosyanın göndeirlmiş bulunduğu anlaşılmaktadır.

Ekonomik zarara yol açan suçlar ise 2009 yılında 3 adet, 2010 yılında 6 adet ve 2011 yılında 10 adet olarak kaydedilmiştir.

Dosya kapsamından zarar nevi tespit edilemediği için bilinmeyen olarak kategorize edilen grupta ise; 2009 yılında 4 dosyanın kaydedildiği, 2010 yılında 7 ve 2011 yılında 8 dosya kaydedildiği görülmektedir.

Hizmet verilip verilmediğine göre ekspertiz sayısı



Şekil 11: Hizmet verilip verilmediğine göre ekspertiz sayısı

ATK FİD tarafından 2009, 2010 ve 2011 yılları içerisinde bilirkişilik hizmeti sağlamak amacıyla incelenen her dosyada hizmet verme imkanı doğmadığı görülmektedir.

Dolayısıyla, bu anlamda bir ayrım yapmak ve talep edilen adli bilirkişilik hizmetinin karşılanıp karşılanmadığı noktasında anlamlı bir sonuç elde edebilmek amaçlanmış; bilirkişilik hizmeti verilen, verilemeyen ve kısmen hizmet verilebilen dosyalar gruplandırılarak incelenmiştir.

Buna göre, 2009 yılında ATK FİD'ne gelen 20 dosyadan sadece 6'sına hizmet verilebilmiş, 10 adet dosyaya kısmen hizmet verilebilirken, 4 adet dosyaya hiç hizmet verilememiştir.

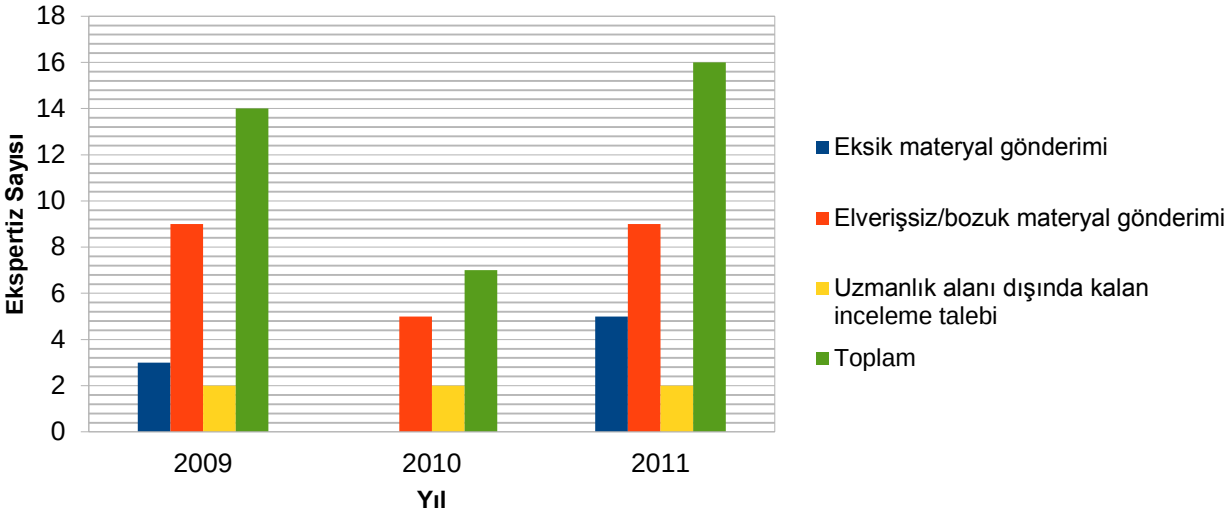
Yine, 2010 yılında ATK FİD'ne gelen 23 dosyadan bu defa 16'sına hizmet verilebilmiş, 4 adet dosyaya kısmen hizmet verilebilirken, yalnızca 3 adet dosyaya hiç hizmet verilememiştir.

2011 yılında, ATK FİD'ne gelen 39 dosyadan 23'üne hizmet verilebildiği, 10 dosyaya kısmen hizmet verilebilirken, 6 dosyaya talep olunan hizmetin verilemediği anlaşılmaktadır.

İlerleyen yıllar içerisinde, ATK FİD tarafından bilirkişilik hizmeti verilebilen dosya sayısı giderek artmaktadır. 2010 yılında bu artışın % 84 oranında olduğu görülmektedir.

2011 yılında ise bilirkişilik hizmeti talebiyle gönderilen dosyalara ATK FİD tarafından hizmet verilebilme oranında % 60'lık bir artış yaşandığı gözlemlenmektedir.

Gelen dosyalar için hizmet verilememe nedeni



Şekil 12: Gelen dosyalar için hizmet verilememe nedeni

ATK FİD'ne gönderilen dosyaların bir kısmına, bir takım sebeplerden dolayı talep edilen bilirkişilik hizmetinin verilemediği görülmüştür.

Yukarıdaki şekilde ortaya çıkan sonuçlar; ATK FİD tarafından hizmet verilememe nedenlerinin irdelenmesi, eksikliklerin tespit edilebilmesi ve çözüm üretilebilmesi anlamında büyük öneme sahiptir.

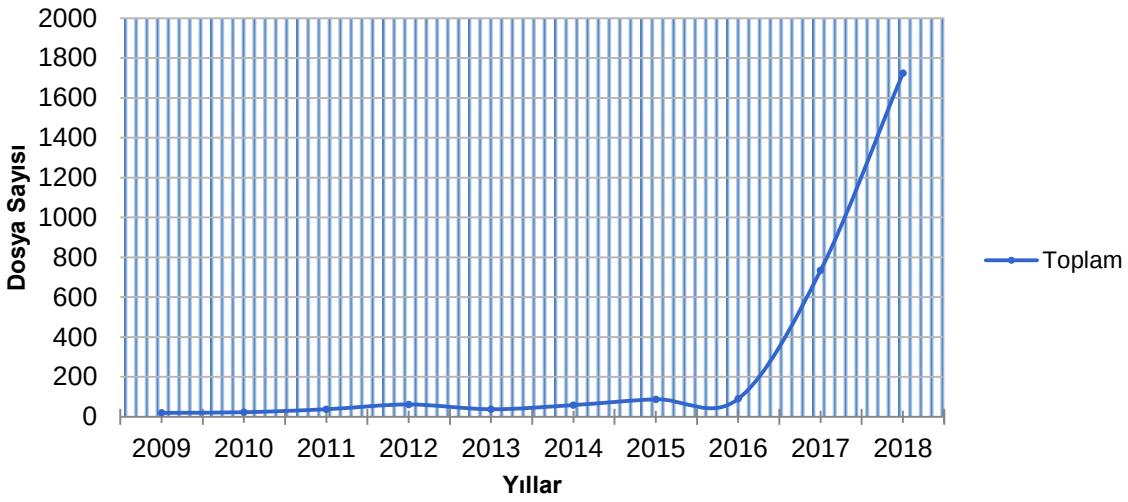
Bu amaçla yapılan incelemede, ATK FİD tarafından dosyanın geri gönderilmesinde gösterilen nedenler kategoriler halinde toplanarak, eksik materyal gönderimi, elverişsiz ve/veya bozuk materyal gönderimi ve uzmanlık alanı dışında kalan inceleme talebi şeklinde gruplandırmalara ulaşılmıştır.

2009 yılında hiç veya kısmen hizmet verilemeyen 14 dosyanın 3'ünde eksik materyal gönderildiği, 9'unda elverişsiz/bozuk materyal gönderildiği, 2 dosyada ise uzmanlık alanı dışında inceleme talep olunduğu görülmektedir.

2010 yılında gönderilen dosyalara bakıldığında; hiç veya kısmen hizmet verilemeyen 7 dosyanın 5'inde elverişsiz/bozuk materyal gönderildiği, 2 dosyada ise uzmanlık alanı dışında inceleme talep olunduğu, buna karşın eksik materyal gönderimi yapılmadığı anlaşılmaktadır.

2011 yılına bakıldığında, hiç veya kısmen hizmet verilemeyen 16 dosyanın 5'inde eksik materyal gönderildiği, 9'unda elverişsiz/bozuk materyal gönderildiği, 2 dosyada ise uzmanlık alanı dışında inceleme talep olunduğu görülmektedir.

2009 -2018 yılları arasında gelen toplam dosya sayısı



Şekil 13: 2009 – 2018 yılları arasında gelen toplam dosya sayısı

ATK bünyesinde FİD tarafından 2009 - 2011 yılları arasında adli bilişim alanında bilirkişilik hizmeti verilen dosyalara ek olarak, 2012 - 2016 yılları arasında FİD ve 2017 - 2018 yılları arasında ABİD tarafından hizmet verilen dosya sayıları çalışmamızın istatistiki verilerine dahil edilmiştir.

Söz konusu verilerin tablo olarak bir arada gösterilmesi, yıllar içerisinde adli bilişim alanında bilirkişilik hizmeti almak amacıyla Adli Tıp Kurumu'na gönderilen dosya sayılarındaki artışı net olarak ortaya koyacaktır:

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
FİD Bilişim ve Teknoloji Sb.	20	23	39	62	38	59	88	90	-	-
ABİD Veri İnc.	-	-	-	-	-	-	-	-	598	867
ABİD Kriptoloji ve Elek.Cihazlar	-	-	-	-	-	-	-	-	45	158
ABİD Mobil Cihazlar	-	-	-	-	-	-	-	-	91	679
Toplam	20	23	39	62	38	59	88	90	734	1724

Tablo 1: 2009 – 2018 yılları arasında gelen toplam dosya sayısının tablo olarak gösterimi.

Buna göre; ATK'na adli bilişim alanında resmi bilirkişilik talebiyle; 2009 yılında 20; 2010 yılında 23; 2011 yılında 39; 2012 yılında 62; 2013 yılında 38; 2014 yılında 59; 2015 yılında 88; 2016 yılında 90; 2017 yılında 734 ve 2018 yılında 1724 dosya gelmiştir.

ATK FİD'ne 2009 – 2016 yılları arasında gönderilen dosyaların yıllar içerisinde istikrarlı ve dengeli bir artış gösterdiği görülmektedir.

Buna göre; 2010 yılında 2009 yılına oranla %15; 2011 yılında 2010 yılına oranla % 65.22; 2012 yılında 2011'e oranla % 63.16'lık bir artış olmuştur.

Bu noktada, 2013 yılında gönderilen dosya sayısının bir önceki yıla göre %38'lik bir düşüş yaşadığı görülmekteyse de, 2014 itibariyle dosya sayısının yeniden istikrarlı bir artışa geçmesi ve %55,26 'lık bir artış göstermesi karşısında bu veri anlamlı bulunmamıştır.

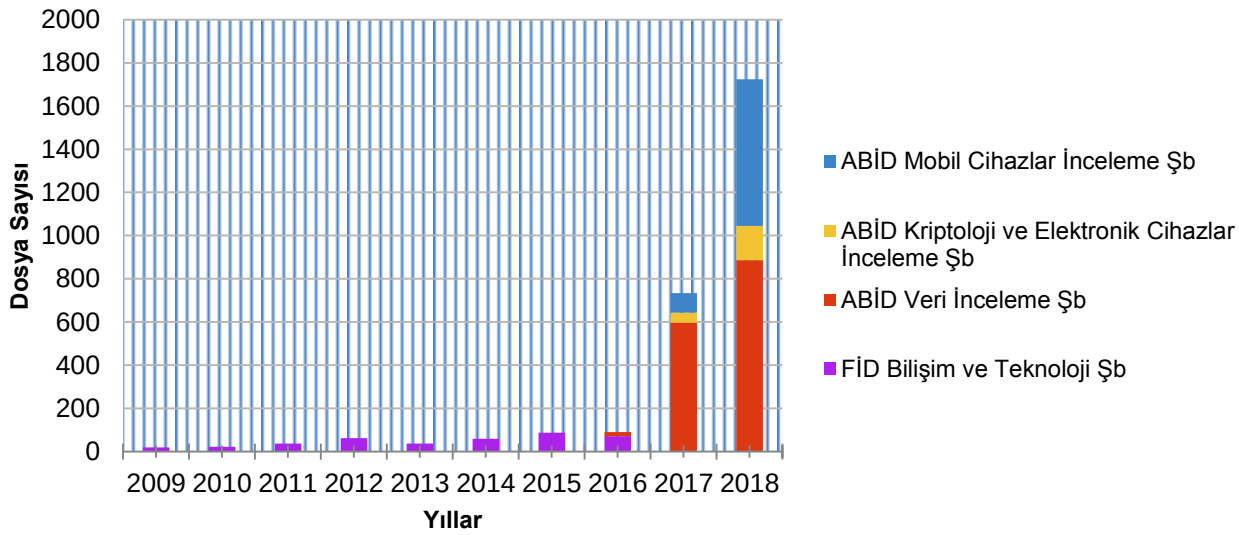
2013 yılında dosya sayısındaki bu düşüşün EGM Siber Suçlarla Mücadele Şube Müdürlükleri ve JGK Bilişim Teknolojileri İnceleme Şube Müdürlüğüne daha fazla dosya gönderilmesi nedeniyle ortaya çıktığı kanaatindeyiz.

2015 yılında gönderilen dosya sayısı 2014 yılına oranla % 49.15'lik bir artış göstermiştir. 2016 yılında 2015 yılına oranla % 2.27'lik bir artış yaşanmıştır.

15 Temmuz 2016 darbe girişimi sonrası 25.11.2016 tarhinde yeni kurulan ATK ABİD'nin adli bilişim konusunda resmi bilirkişilik hizmetine başladığı 2017 yılında ise % 715.56'lık bir artış gözlenmektedir.

2018 yılında da ATK ABİD'ne gönderilen adli bilişim ile ilgili bilirkişilik dosya sayısı hızla artmaya devam etmiş ve bu defa % 134.88'lik bir artış görülmüştür.

2009 -2018 yılları arasında şubelere göre dosya dağılımı



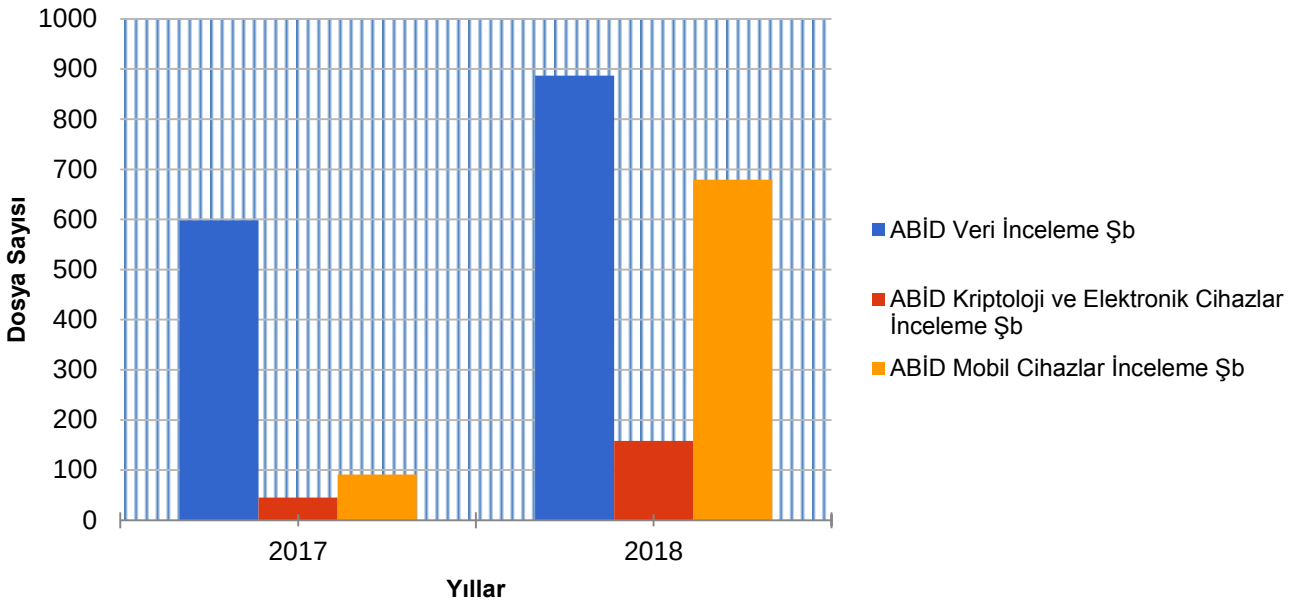
Şekil 14: 2009 – 2018 yılları arasında şubelere göre dosya dağılımı

ATK FİD Bilişim ve Teknoloji Suçları Şube Müdürlüğü'ne 2009 – 2016 yılları arasında gönderilen dosyaların, 2013 yılı hariç, 2016 yılının sonuna kadar dengeli bir artış gösterdiği görülmektedir.

2017 yılından itibaren yeni kurulan ATK ABİD hizmete başlamış ve bünyesinde bulunan adli bilişim alanında bilirkişilik hizmeti veren Mobil Cihazlar İnceleme, Kriptoloji ve Elektronik Cihazlar ve Veri İnceleme Şube Müdürlüklerine gelen tüm dosya oranlarında olağanüstü bir artış yaşanmıştır.

2017 ve 2018 yıllarına ait verilere göre; ATK ABİD'ne gelen dosyalarda olağanüstü oranlarda artış görülmüştür.

2017 - 2018 yılları arasında ABİD şubelerine göre dosya dağılımı



Şekil 15: 2017 – 2018 yılları arasında ABİD şubelerine göre dosya dağılımı

ATK ABİD'ne 2017 ve 2018 yılları içinde gönderilen dosyaların hangi şubeler arasında dağıldığının tespitinin yapılması, adli bilirkişilik talep edilen hizmet türlerinin belirlenebilmesini de sağlayacaktır.

Buna göre; 2017 yılı içerisinde ABİD Veri İnceleme Şube Müdürlüğü'ne 598; Mobil Cihaz İncelemeleri Şube Müdürlüğü'ne 91 ve Kriptoloji ve Elektronik Cihazlar Şube Müdürlüğü'ne 45 adet dosya gelmiştir. Bu verilere göre, en fazla talep olunan adli bilirkişilik hizmetinin veri inceleme alanında ortaya çıktığı görülmektedir. Bunu sırasıyla mobil cihazlar alanındaki incelemeler ile kriptoloji ve elektronik cihaz incelemeleri izlemektedir.

2018 yılı içerisinde ABİD Veri İnceleme Şube Müdürlüğü'ne 887; Mobil Cihaz İncelemeleri Şube Müdürlüğü'ne 679 ve Kriptoloji ve Elektronik Cihazlar Şube Müdürlüğü'ne 158 adet dosya gelmiştir. 2018 yılı içerisinde en fazla talep olunan adli bilirkişilik hizmetinin yine veri inceleme olduğu, bunu mobil cihazlar alanındaki incelemeler ile kriptoloji ve elektronik cihaz incelemelerin izlediği görülmektedir.

2018 yılında veri incelemesi konusundaki adli bilirkişilik hizmeti taleplerinde 2017 yılına oranla % 48.33'lük bir artış gerçekleşmiştir. Mobil cihaz incelemeleri alanında talep olunan adli bilirkişilik hizmeti yönünden bu artış % 646.15 olarak tespit edilmektedir. Kriptoloji ve elektronik cihaz incelemeleri yönünden % 251.11'lik bir artış gözlenmektedir.

Adli bilirkişilik talep edilen hizmet türlerine dair sıralamaların, doküman incelemesi yapılan 2009-2011 yılları bulguları ile tutarlılık göstermesi dikkat çekicidir.

Buna göre;, 2009 – 2011 yılları arasında FİD'ne gönderilen dosyaların 'incelenmesi istenen materyal' ve 'verilen hizmete göre ekspertiz sayısı' açısından analizinde elde edilen sonuçlar, ABİD'ne gönderilen dosyalara verilen hizmet türüne göre oluşturulmuş şubeler arasındaki dağılım ile örtüşmektedir.

Şöyle ki, ‘incelenmesi istenen materyal’ açısından yapılan analizlerde; 2009 – 2011 yılları içerisinde en fazla sayıda ekspertiz hizmeti verilen materyal türünün ‘disk materyalleri’ ve bunları takiben ‘cep telefonları’ olduğu ortaya konulmuştur.

ATK ABİD'ne 2017 ve 2018 yılları içinde gönderilen dosyaların sayısal analizinde de; en fazla dosyanın Veri İnceleme Şube Müdürlüğü’ne, bunu takiben Mobil Cihaz İncelemeleri Şube Müdürlüğü’ne gönderildiği görülmektedir. Böylece veri incelemesi yapılan ‘disc materyalleri’ ve mobil incelemeye konu olan ‘cep telefonları’ her iki analizde de ilk iki sırada yer almıştır.

Yine, ‘verilen hizmete göre ekspertiz sayısı’ açısından yapılan analizlerde; 2009 – 2011 yılları içerisinde en fazla sayıda ‘flashbellek/harddisk incelemeleri’ şeklinde gruplanan bilirkişilik hizmetinin verildiği ve bunu takiben ‘cep telefonu incelemeleri’nin ikinci sırada en fazla verilen hizmet türü olduğu görülmektedir.

ATK ABİD'ne 2017 ve 2018 yılları içinde gönderilen dosyaların sayısal analizinde de; en fazla dosyanın Veri İnceleme Şube Müdürlüğü’ne, bunu takiben Mobil Cihaz İncelemeleri Şube Müdürlüğü’ne gönderildiği görülmektedir.

Dolayısıyla veri incelemesi türü altında değerlendirilecek ‘flashbellek/harddisk incelemeleri’ ve mobil inceleme türü altında değerlendirilecek ‘cep telefonu incelemeleri’ her iki analizde de ilk iki sırada yer almaktadır. Bu veriler, incelenen 10 yıllık süreç içinde en fazla talep olunan adli bilişim bilirkişilik hizmetlerinin ‘veri incelemeleri’ ve ‘mobil cihaz incelemeleri’ olduğunu göstermektedir.

5. TARTIŞMA VE SONUÇ

Çalışmamızda; ATK FİD'ne 2009, 2010 ve 2011 yılları içerisinde bilirkişilik hizmeti almak amacıyla yollanan adli bilişimle ilgili dosyalar incelenmiş; böylece ülkemizde internet ve bilişim suçlarının nispeten yeni yaygınlaşmaya başladığı belli bir döneme ışık tutulmaya çalışılmıştır. Dolayısıyla öncelikle henüz bilişim sistemlerinin ve internetin bizim için yeni sayılabileceği bu üç yıllık zaman diliminde, insanoğlunun deneyimlediği her yeni olgu gibi bilişim çağının da kendi kriminal çerçevesini ne denli hızlı ve etkin bir şekilde oluşturmaya başladığı gözlemlenmiştir.

2009, 2010 ve 2011 yıllarını içine alan ilk üç yıllık sürecin incelemesine ek olarak; 2012 – 2016 yılları arasında FİD Bilişim ve Teknoloji Suçları Şubesi'ne ve 15 Temmuz 2016 darbe girişimi sonrası 2017-2018 yılları içerisinde ATK ABİD'ne gelen adli bilişimle ilgili dijital delil ve adli bilirkişilik dosyalarında artış olup olmadığı istatistiki olarak incelenmiş ve 10 yıllık süreç içerisinde resmi bilirkişilik hizmetlerinde gözlenen artış ortaya konulmuştur.

Genel itibariyle tüm grafiklerden ortaya çıkan sonuç; ATK'ya gönderilen adli bilişim dosya sayısının ve dolayısıyla bilirkişilik hizmeti talebinin devamlı bir artış içerisinde olduğudur. Buna göre gönderilen dosya sayısı yıllara göre artış göstermiş; 2010 yılından 2011 yılına geçilirken neredeyse iki katı oranında bir artış tespit edilmiştir. Yine dikkat çekici bir nokta, bilişim araçlarının ve internetin, işlenen çok çeşitli suç tiplerinde, gerek suçun maddi unsurları içerisinde gerekse delil mahiyetinde kendini gün be gün daha çok göstermesidir. Öyle ki, suç tipi bilişim alanının dışında kalmakla beraber, işlenişi sırasında bilişim sistemleri yahut internet kullanılan ya da delilleri içerisinde bilişim ve/ veya internet materyalleri bulunan suçlara ilişkin ilerleyen

yıllar boyunca gözlemlenen düzenli artış açık bir biçimde grafiklere yansımıştır. Bu kategorideki suçlar yıllar içerisinde istikrarlı ve hızlı bir yükseliş göstermiştir.

Bilişim suçlarının ve internet aracılığıyla işlenen suçların artış göstermesinin ve suç faillerinin eylemlerini gerçekleştirirken daha fazla internete ve bilişim araçlarına başvurmalarının doğal bir sonucu olarak, ATK tarafından verilen adli bilişim alanındaki resmi bilirkişilik hizmetlerinde de ilerleyen yıllar içerisinde ciddi oranda artış gözlemlendiği görülmüştür. İlerleyen yıllarda adli bilişim alanında talep olunan bilirkişilik hizmetleri, en fazla veri ve mobil cihaz incelemeleri alanında gözlemlenmek suretiyle, sürekli olarak artmaya devam etmiş ve en yoğun resmi bilirkişilik talebi, 15 Temmuz 2016 darbe girişiminin de etkisiyle adli bilişim alanında resmi bilirkişilik talebiyle ATK ABİD'ne çok fazla sayıda dosya gönderilmesi nedeniyle 2017 ve 2018 yıllarında yaşanmıştır.

2009- 2011 yılları içerisinde, dosyaların illerden ilçelere yayılan bir yoğunlukla ve toplumun her kesiminde bilişim teknolojilerinin kullanımının yaygınlaştığı görülmektedir. Öyle ki, adli bilişim incelemeleri artık yalnızca yer itibariyle yetki alanları büyük illerle sınırlı adli merciler tarafından talep edilmemektedir; tüm ülke çapına yayılarak ilçe bazında da adli bilişim bilirkişilik hizmetlerinin olanaklarından yararlanma ihtiyacı ortaya çıkmıştır.

Daha da önemlisi, bu ihtiyaç ilerleyen yıllar içerisinde artmaya devam edecektir. Elde edilen bu sonuç; adli bilişimin gün geçtikçe daha fazla ve daha yaygın olarak başvurulan bir ihtisas alanı ve ülke çapında savcılık ile mahkemelerin tüm yetki alanlarını kapsayacak biçimde her noktaya ulaştırılması gereken bir bilirkişilik hizmeti haline geldiğini göstermektedir.

Hem teknik bilgi gerektiren hem de gerektirmeyen suçlarda artış olduğu, ancak yıllar içerisinde teknik bilgi gerektirmeyen suçlara oranla teknik bilgi gerektiren suçların artışının daha fazla olduğu anlaşılmaktadır. Görüldüğü üzere, nasıl ki bilişim araçlarının günlük kullanım şekli toplumun gelişiminin artması ile daha bilinçli ve daha teknik bir düzeye erişmekteyse, bu bilginin kötü niyetli olarak suç eylemlerinde kullanılması da aynı şekilde daha karmaşık bir görünüm kazanabilmektedir. Diğer bir değişle, toplumun her kesiminden bireyin bilişim araçlarına ve internete karşı daha farkında ve yetkin bir yaklaşım sergilemesi, yani bu araçları kullanma yeteneğinin kriminolojik anlamda gelişmesi, bu alanda işlenen suçları da karmaşıklaştırmaktadır. Bu durum bilirkişilik hizmeti veren kişi, kurum ve kuruluşların etkinliğini sorgulatacak, zamanla yeni beklentiler yaratacak bir düzeye erişilmekte olduğunu göstermektedir. Dolayısıyla adli bilişim alanında bilirkişilik hizmeti veren kurum ve kuruluşlar bazında gözlenen bu değişime ayak uydurulabilmesi adına; talebe cevap verebilecek teknik düzeyde yetkin ve yeterli sayıda uzman yetiştirilmesi ile adli bilirkişilik hizmeti veren kurum ve kuruluşların güncel teknolojiler ile donatılarak kapasitesinin arttırılması gerekmektedir.

Bilişim ve internet suçları ile hemen her nevi hakkın ihlalinin mümkün hale geldiği; fakat en fazla adli bilişim ile ilgili bilirkişilik hizmetinin ekonomik zarara yol açan suçlar açısından talep edildiği sonucuna varılmıştır. Bu noktada, bilişim ve internet suçlarına karşı alınacak önlemlerdeki önem sırasının, doğan zararın nevi ve yoğunluğu dikkate alınarak tespit edilmesi gerekecektir.

Suçun artışına paralel olarak bilirkişilik hizmeti veren kurumların inceleme alanlarının genişlendiği ve incelenmek üzere gönderilen materyallerin çeşitlendiği tespit edilmiştir. Çalışmamız bulgularından elde edilen sonuç, hemen herkesin kullanımında

bulunan cep telefonları gibi yaygın olarak rastlanan bazı bilişim materyalleri sıralamada üstlerde yer alırken, diğer yandan bilişim suçuna konu olması, örneğin üzerinde değişiklik yapılması ya da başkaca herhangi bir suretle suça konu edilmesi daha fazla teknik bilgi ve uzmanlık gerektiren kredi kartları ve bankamatik kartları gibi bazı materyallerin ise, kullanımı yaygın olsa dahi daha alt sıralarda yer aldığı yönündedir. Bununla birlikte gönderilen materyal çeşitliliği istikrarlı olarak artmaktadır. Örneğin; sair cihazlar kategorisi açısından, yıllar içerisinde oransal olarak büyük bir artış yaşanmıştır.

Dolayısıyla, yıllar içerisinde gönderilen bilişim materyallerinin çeşitlenmesi ve artmasının bir sonucu olarak, adli bilişim alanında çalışan uzmanların yetkinliğinin ve gerek adli bilişim uzmanlarınca gerekse adli bilirkişilik hizmeti veren kurumlar tarafından verilebilen hizmetlerin çeşitliliğinin talebi karşılar düzeye getirilmesi gerekmektedir.

İncelenen materyallere ilişkin değerlendirmeyle benzeştiği üzere, genel olarak yıllar içerisinde adli bilişim bilirkişilik hizmeti talebinin arttığı ve yine verilen ekspertiz hizmetine dair inceleme alanlarının çeşitlendiği görülmektedir. Bunun yanısıra, cep telefonu ve CD gibi yaygın olarak kullanılan bazı bilişim materyallerine dair incelemeleri ve buna dayalı bilirkişilik hizmetleri alanında daha yoğun bir taleple karşılaşıldığı, bununla beraber internet kaynaklı incelemelerin son sırada yer aldığı çalışmamızdan elde edilen bir başka sonuçtur.

Bu noktada, her ne kadar internet kullanımı gün be gün artmakta ve toplumun geneline yayılmaktaysa da, internet üzerinden gerçekleştirilen suçların henüz önemli bir yoğunluğa ulaşmadığı sonucu dile getirilebilecektir. Sonuç olarak, bilirkişilik hizmeti

veren tüm kurum ve kuruluşların yıllar içerisinde hızlı bir biçimde yaygınlaşan talep oranında hizmetlerini etkili ve yeni bir yelpazede sunabilmesi ihtiyacı doğmaktadır.

Çalışmamızda elde edilen bulgular, ilerleyen zaman içinde hizmet verilebilme oranlarında belli bir artışın yaşandığını ortaya koymaktadır. Buna göre; gerek adli kolluk tarafından delillerin doğru şekilde toplanmaya başlandığı, gerekse adli bilişim konusunda yetkin bilirkişilik hizmeti veren kurumların (EGM Siber Suçlarla Mücadele Birimi, ATK, teknik üniversiteler vb.) ciddi bir gelişim gösterdikleri sonucuna varılmaktadır.

Bununla beraber, hizmet verilebilme oranlarında gözelenen iyileşmeye rağmen; adli bilişim konusunda bilirkişilik hizmetinin her zaman etkin bir şekilde verilememekte olduğu da çalışmamız bulgularından elde edilen sonuçlardan biridir. Adli mercilerden gönderilen her dosya, delil zincirinin gerektirdiği koşullar yerine getirilerek yahut bilinçli adli kolluk personeli tarafından gönderilmemektedir. Dijital delillerin toplanması ve delil zincirinin korunması alanında çalışan nitelikli uzman ve teknik personelin sayısının azlığının bu sonucu ortaya çıkardığı görülmektedir.

Elde edilen bulgular, bilirkişilik hizmeti verme noktasında gelişimimizi sürdürebilmek adına bir taraftan bilirkişi sayısını arttırırken diğer yandan özellikle en önemli hizmet verilememe nedeni olarak ortaya çıkan elverişsiz/bozuk materyal gönderiminin önüne geçebilmek için delile el koyma sürecinde standartların belirlenmesi ile delil toplanması ve delil zincirinin korunarak nakledilmesi alanlarında çalışan teknik personelin eğitimi ve bilinçlendirilmesi gerektiğini ortaya koymuştur.

Tespit edilen bulgulara göre, ATK FİD'ne hem Cumhuriyet Başsavcılıkları hem de mahkemelerce gönderilen dosya sayılarında yıllar içerisinde ciddi bir artış

gerçekleşmiştir. Dolayısıyla adli bilişim; ceza hukuku sistemimiz içinde daha sıklıkla başvurulan ve talep yoğunluğu günden güne artan bir ihtisas alanı haline geldiğinden, verilen bilirkişilik hizmetlerine adli makamlar tarafından zaman içerisinde daha fazla ihtiyaç duyulacaktır. Bu ihtiyacın etkin bir biçimde karşılanabilmesi; bilişim ve internet suçlarına dair soruşturma ve kovuşturma işlemlerini yürüten ve ilk etapta bilirkişilik hizmeti veren kurumlara dosya gönderen Cumhuriyet Başsavcılıkları ve mahkemelerin uzmanlıklarının arttırılması ile kuşkusuz daha mümkün hale gelecektir.

Bilişim suçlarının soruşturma aşamasında görev alan ve Cumhuriyet Başsavcılıkları bünyesinde bulunan Bilişim Suçları Soruşturma Büroları; bünyesinde sadece bilişim suçlarına yönelik çalışan savcıların görevlendirilmesiyle soruşturma aşaması sırasında belli bir uzmanlaşmayı mümkün kılmaktadır (http://www.istanbulanadolu.adalet.gov.tr/rehber/savcilik-sorusturma.php). Bu bürolar; bilişim suçları, internet aracılığıyla gerçekleştirilen suçlar, 5070 Elektronik İmza Kanunu 16 ve 17. maddelerince düzenlenen cezai hükümler, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'daki suçlar, bilişim sistemlerinin kullanılması suretiyle işlenen nitelikli hırsızlık ve dolandırıcılık gibi bilişim alanındaki bir kısım suçların soruşturulması görevini yürütmektedir (http://www.ankara.adalet.gov.tr/sayfalar/yonerge/yonerge.pdf).

Bilişim suçları soruşturma büroları ile koordineli çalışacak, bilişim suçları ve internet aracılığıyla işlenen suçlar alanında uzmanlık eğitimine (yüksek lisans, doktora, sertifika vb.) sahip hakimlerin görevlendirileceği 'bilişim hakimlikleri'nin oluşturulması ve özellikle bilişim suçlarının ve internet aracılığıyla işlenen suçların yüksek oranda gözlendiği nüfusu yüksek büyükşehirlerden başlamak üzere ihtisas mahkemesi olarak

işlev görecek ‘bilişim mahkemeleri’nin kurulması ile kovuşturma aşamasında da uzmanlaşma sağlanacaktır. Bilişim mahkemeleri; hem suçla mücadelede hızlı ve etkin çözümler sunacak hem de bilirkişilik hizmetlerinin etkin kullanımı, yetkin hakimlikler ve mahkemeler eliyle sağlanacaktır. Bu mahkemelerinin hayata geçirilmesiyle daha etkin bir yargılama süreci ortaya çıkacağı gibi, bilişim delillerinin toplanması esas ve yöntemlerine dair eğitim almış bilinçli hakim ve mahkemeler elinde yürütülen kovuşturma sürecinde, bilirkişilik hizmeti veren kurumlara önnek olarak ‘uzmanlık alanı dışında materyal gönderilmesi’ gibi bir kısım uygulamaların da önemli ölçüde azalacağı öngörülmektedir.

Bilişim ve internet alanına ilişkin suçlara dair verilecek bilirkişilik hizmetlerinde uzmanlaşma son derece önemlidir. Bilişim suçlarına yönelik çalışan kolluğun bu konuda uzmanlaşmış olan savcılıklar ve hakimlikler ile koordinasyon içinde çalışması yanında, teknik konularda gerek nitelik ve gerekse nicelik olarak yeterli adli bilişim uzmanlarınca sürecin desteklenmesi son derece sağlıklı sonuçlar ortaya çıkartabilecektir (Özen ve ark., 2015).

Çalışmamız kapsamında elde edilen bulgular, ülkemizde adli bilişim uzmanlığını da kapsayacak şekilde adli bilirkişilik mevzuatı ve uygulamalarıyla ilgili bir takım eksikliklere işaret etmektedir. Bilişim teknolojileri ile ilgili bilirkişilik görevlerinin icrasına yönelik hukuk sistemimizce tanımlanmış ayrı bir “adli bilişim uzmanı” statüsü olan bilirkişi bulunmadığından, adli bilirkişilik hizmetleri daha çok bilgisayar ve elektronik mühendisliği ya da bilgisayar programcılığı mezunları tarafından sonradan adli bilişim konusunda üniversitelerde (Hacettepe, Gazi, Üsküdar vb.) yüksek lisans veya doktora eğitimi ile ya da özel kurslardan bilişim eğitim sertifikası alınarak veya adli bilişim konusunda uzmanlaşmış bilirkişinin yanında usta - çırak usulü ile

yürütülmektedir. Bunun dışında zaman zaman bilirkişi olarak üniversitelere ve bazı ticari kuruluşlara da başvurulmaktadır. Oysa adli bilişim uzmanlığı, standart ve yetkin bir eğitime sahip olunması gereken, tamamen teknik bilgi gerektiren ve bilişim sistemleri konusunda ileri derecede bilgi sahibi olmayı içeren bir meslektir (Dülger, 2017).

Adli bilişim konusunda çalışan ve eğitim almış personelin sayısının yetersizliği yukarıda sayılan çözüm yollarına başvurmayı gerektirmiştir. Söz konusu eksikliği tamamlamak için, "adli bilişim uzmanlığı" statüsünü yasayla belirlemek ve bu statüde çalışacak uzman yetiştirmek üzere adli bilişim uzmanlığı alanında daha fazla sertifika programı açmak, üniversitelerdeki lisans ve lisansüstü programlarının sayısını arttırarak, bu alanda ihtisas yapmaya teşvik edici eğitim politikaları geliştirmemiz gerekmektedir.

Adli bilişim ile ilgili olarak, EGM bünyesinde Siber Suçlarla Mücadele Şube Müdürlükleri ve JGK Kriminal Daire Başkanlığı bünyesinde Bilişim Teknolojileri İnceleme Şube Müdürlüğü ile ATK ABİD ve üniversitelerin mühendislik fakültelerinin bilgisayar ve elektronik mühendisliği bölümleri tarafından resmi bilirkişilik hizmeti verilmektedir. ABİD'nin ATK içerisinde ayrı bir ihtisas dairesi olarak kurulması, kendi adli bilişim uzman personelini eğitmesi ve yetkinliğini denetlemesi, yine kurulan AR-GE Şubesinde yazılım ve programlar geliştirmesi hızlı ve etkin adli bilirkişilik hizmeti verilmesine ve adli bilişim alanında dünyadaki gelişmelerin güncel olarak takibine imkan sağlanmaktadır.

Bununla birlikte, resmi bilirkişilik kurumlarında (EGM, JGK, ATK ve üniversiteler vb.) adli bilişim alanında çalışan uzman personel sayısının azlığı nedeniyle

bilirkişilik ihtiyacına cevap verilmesinde geç kalınması hızla yaygınlaşan bilişim ve internet suçları ile mücadeleyi sekteye uğratabilecektir.

Bilirkişilik hizmeti veren resmi bilirkişilik kurumlarının kendi aralarında bir koordinasyon ve iletişim içinde olması hızlı ve etkin yargılama süreçleri için gereklidir. Bilirkişilerin bilirkişilik sistemi hakkındaki görüşlerinin değerlendirilmesine yönelik olarak 2015 yılında yapılan bir anket çalışmasında ortaya çıkan sonuçlar son derece aydınlatıcıdır. Söz konusu çalışmada, iş yükünün fazlalığı ile ilgili soruya tamamı bilirkişilerden oluşan katılımcıların %40'ının "iş yükünün çok fazla olduğu" yönünde cevap verdiği, "başka kurumlarla koordinasyon lazım mı?" sorusuna % 87'sinin "evet" şeklinde ve "kurumlar arasında koordinasyon var mı?" sorusuna %98'inin "hayır" şeklinde cevap verdiği göz önünde bulundurulmalıdır (Akgün, 2015).

Bu noktada, dağınık illerde hizmet vermekte olan resmi bilirkişilik kurumlarının kendi şubeleri arasında ilgili birimler bazında bir yardımlaşma içinde olunması ve koordinasyon oluşturabilmesinin, bu kurumlar üzerindeki iş yükünü önemli ölçüde azaltacağı ve yıllar içerisinde ciddi oranda artan bilirkişilik hizmeti taleplerine cevap verme sürecini hızlandıracağı kanaatine varılmaktadır.

Çalışmamız adli bilişim alanında en fazla yaşanılan sıkıntılardan birinin, delilin doğru şekilde toplanmamış ve/veya bilirkişiye ulaştırılmamış olması nedeniyle hizmet vermekte sorunlar yaşanması olduğunu göstermektedir (Çiçek, 2008). Bunun önüne geçebilmek için, delile elkoyma sürecinde yapılacak işlemler ile ilgili olarak gerçekleştirilecek prosedürlerin ve özellikle delilin toplanmasından delil zincirini bozmadan delilin nakledilmesine kadar her bir evrede uygulanacak standartların açık bir

suretle mevzuat içerisinde düzenlenmesi ve bu konuda çalışan personelin bir takım eğitimlere tabi tutulması sağlanmalıdır (Taşçı ve ark., 2015).

Çalışmamız kapsamında, Adli Tıp Kurumu tarafından 2009 - 2018 yılları arasında bilirkişilik hizmeti verilen dosyaların incelenmesinden elde edilen sonuç; bu suçların çarpıcı bir biçimde arttığını göstermekte, bununla da kalmayarak bu suçlar teknik bilgi gerektirmesine bakılmaksızın yaygınlaşmakta ve toplumun her kesimine yayılmaktadır. Bilgisayarlar ve akıllı cep telefonları ile bunlar aracılığıyla hemen herkes tarafından yoğun olarak kullanılmaya başlanan sosyal medyanın bilişim ve internet suçlarının artışındaki rolü yadsınamayacaktır. Artık bilişim sistemleri her nevi suçta gerek amaç ve gerekse araç olarak karşımıza çıkabilmekte, sanal dünya hemen her suçun gerçekleştirilebilmesi imkanını sağlamaktadır.

Gözlemlenen bu değişime ayak uydurulabilmesi adına; kamuoyunun suçun artışı ve gerek bilişim gerekse internet suçlarıyla mücadelede alınabilecek bireysel önlemler konusunda bilgilendirilmesi, adli bilişim alanında bilirkişilik hizmeti veren kurum ve kuruluşlar bazında talebe cevap verebilecek teknik düzeyde yetkin ve yeterli sayıda uzman yetiştirilmesi ile adli bilirkişilik hizmeti veren kurum ve kuruluşların güncel teknolojiler ile donatılarak kapasitesinin arttırılması, bu kurumların gerekli eğitim ve altyapı çalışmaları ile adli bilişim alanında uzmanlaşması sağlanan soruşturma ve kovuşturma birimleriyle uyum içerisinde çalışabildiği bir ortamın hayata geçirilmesi gerekmektedir.

Bu çalışmanın ortaya çıkardığı bir diğer sonuca göre; bilişim ve internet alanındaki suçlar arttıkça verilecek bilirkişilik hizmetlerinde de bu bulguyu destekleyecek şekilde oransal bir artış yaşanacaktır.

Dolayısıyla, ülke genelinde bilişim suçlarının hızlı artışı nedeniyle artan adli bilişim bilirkişilik hizmeti talebinin hızlı ve etkin bir şekilde ve de konusunda yetkin ve sayıca yeterli adli bilişim uzman personel ile karşılanabilmesi için; gerekli bölgesel altyapının oluşturulması ve adli bilişim alanında bilirkişilik hizmeti veren resmi bilirkişilik kurumlarının gerektiğinde birbirleri arasında ve gerektiğinde de kendi bünyeleri içinde bulunan şubeleri arasında koordinasyonunu sağlayarak adli bilirkişilik hizmetinin yerinde verilmesi ihtiyaç ve zorunluluğu bulunmaktadır.

Sonuç itibariyle; bilişim ve internet alanındaki suçlarla mücadele açısından sergilenecek çabaların hem mevzuat ve hem de insan kaynakları yönü bulunmakta olup; her iki alanda yürütülecek çalışmalarla, ihtiyaç ve zorunlulukların gözetilmesi ve mevcut eksikliklerin hızla kapatılması suretiyle suçla mücadelede önemli adımlar atılabilecektir. Bilişim ve internet suçluluğu alanlarında etkili önlem ve uygulamalar geliştirmekte elde edeceğimiz başarının, ülkemizi adli bilişim alanında donanımlı bir konuma getirmeye; ayrıca sahip olduğumuz genç ve dinamik iş gücünü geleceğin önemli bir iş kolu olacak adli bilişim teknolojileri alanına yönlendirerek, bu alanda çok sayıda genç insanımıza adli bilişim konusunda yetkinlik kazandırmak suretiyle dünyada avantajlı bir yer edinmeye yarayacağı inancındayız.

6. KAYNAKLAR

1. Adli Tıp Kurumu. (2012) Rapor Düzenlemede Adli Tıp Kurumu İhtisas Kurul Ve Dairelerinin İstediği Belge Ve Materyaller [PDF Belgesi]. Alıntı: http://www.atk.gov.tr/belgevemateryaller.pdf(Son Erişim 2.12.2018**)**

2. Adli Tıp Kurumu İdari Yapı, İhtisas Daireleri http://www.atk.gov.tr/adli-tip-ihtisas-daireleri.html (Son Erişim 2.12.2018)

3. Akcan S. (2008) Adli Bilişim, CMK md. 134 ve Düşündürdükleri [Blog Yazısı] Alıntı: http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html

4. Akgün Ç. (2015) Bilirkişilerin Bilirkişilik Sistemi Hakkındaki Görüşlerinin Değerlendirilmesi. Yüksek Lisans Tezi. İstanbul Üni. Adli Bilimler Enstitüsü, İstanbul.

5. Akıncı H, Alıç AE, Er C. (2004) Türk Ceza Kanunu ve Bilişim Suçları. İnternet ve Hukuk Der: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004

6. Alaca B. (2008) Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi(Antropolojik ve Hukuk Boyutları İle). Yüksek Lisans Tezi. Ankara Üni. Sosyal Bilimler Enstitüsü, Ankara.

7. Artuner H. (2015) Adli Bilişim Alanında Dijital Delil, Delil Karartma ve Delil Toplama. T.C. Hacettepe Üni. Fen Bilimleri Enstitüsü, Ankara.

8. Aydın H. (2016) İstatistik. Alıntı: https://docplayer.biz.tr/374170-Istatistik-istatistik-nedir-istatistiksel-arastirmanin-amaci.html

9. Balogun A. M., Zhu S. Y. (2003) Privacy Impacts Of Data Encryption On The Efficiency Of Digital Forensics Technology. International Journal Of Advanced Computer Science And Applications, Sayı: 2013/5.

10. Baloğlu İ. (2013) Veri Kurtarma Teknolojisi. Alıntı: https://www.difose.com.tr/ver-kurtarma-teknolojisi/

11. Baron B, Ellsworth H, Savetz M. (1998) Internet Unleashed. Çev. Nezihe Bahar, Devrim Türkmen, Sistem Yayıncılık, İstanbul.

12. Beckett J., Slay J. (2007) Digital Forensics: Validation and Verification in a Dynamic Work Environment. Proceedings of the 40th Hawaii International Conference on System Sciences [PDF Belgesi]. Alıntı:https://www.researchgate.net/publication/221177767_Digital_Forensics_Validation_and_Verification_in_a_Dynamic_Work_Environment (Son Erişim 3.12.2018)

13. Berkay A. (2006) Hack Teknikleri [PDF Belgesi]. Alıntı: https://tr.scribd.com/document/49570099/Ahmet-Berkay-Hack-Teknikleri (Son Erişim 2.12.2018)

14. Berrin A. (2016) Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 24- 2.

15. Brown, C.L.T. (2010) Computer Forensics and Evidence Dynamics, in Computer Evidence, Collection and Preservation, Course Technology pp.1-69.

16. Bulut, E. (2001) Elektronik Ticaret ve Elektronik İmza. Mevzuat Dergisi, 4- 48.

17. Canbek G., Sağıroğlu Ş. (2007) Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri:Bir İnceleme.Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23(1-2)1-12.

18. Castells, M. (2013) Ağ Toplumunun Yükselişi. Çev. E. Kılıç, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

19. Casey, E. (2011) Digital Forensics, In : Digital Evidence and Computer Crime: Forensic Science Computer and Internet, Elsevier Inc.

20. Craiger P., Burke P., Marberry C., Pollitt M. (2008). A Virtual Digital Forensics Laboratory, In Advances in Digital Forensics IV.Springer-Verlag New York Inc.

21. Çakır H, Kılıç MS. (2013) Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. Polis Bilimleri Dergisi, Sayı: 2013/3.

22. Çakır H, Kılıç MS. (2014) Adli Bilişim ve Elektronik Deliller. Seçkin Yayıncılık, Ankara.

23. Çiçek İ. (2008) Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları. Yüksek Lisans Tezi. Haliç Üni. Fen Bilimleri Ens.

24. Demir İ. (2017) SPSS Uygulamaları Temel İstatistik Eğitimi, Sürekli Eğitim Merkezi Kurs Notları.

25. Dönmez A. (2001) Bilgisayarcı Matematikçiler. Doğuş Üniversitesi Dergisi, Sayı: 2001/4.

26. Dülger M.V.(2014) Bilişim Suçları ve İnternet İletişim Hukuku. Seçkin Yayıncılık, Ankara

27. Dülger M. V., Modoğlu G. (2014) Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi : Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi.Avrupa Birliği-Avrupa Konseyi Ortak Programı, Ankara.

28. Dülger M. V. (2017) Adli Bilişim ve Ülkemizde Uygulaması. H+ Dergi, 1: 20-26.

29. Dülger M. V. (2018) Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri. Alıntı: http://dulger.av.tr/2018/07/09/bilisim-sistemleri-uzerinde-arama-kopyalama-ve-el-koyma-tedbiri/(Son Erişim 30.04.2019)

30. Ekizer AH. (2014) Adli Bilişim (Computer Forensics). Alıntı: https://www.ekizer.net/adli-bilisim-computer-forensics/ (Son Erişim 18.10.2018)

31. Erkan B, Söngür M. (1999) Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü. Taş Yayınevi, Ankara Hacettepe.

32. Gromov G. (2012) History of Internet and World Wide Web - Roads and Crossroads of the Internet History. Alıntı: http://netvalley.com/intval1.html(Son Erişim 30.04.2019)

33. Güllüce Y. Z., Benzer R. (2015) Adli Bilişimde Hard Disk Arızaları Ve Arızalı DisklerdenVeri Kurtarma Yöntemleri. International Journal Of Human Science. 2015/1.

34. Güngör N. M. (2007) Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları. Yüksek Lisans Tezi. İstanbul Üni Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İstanbul.

35. Güven M.(2010) İnternette Güvenlik ve Hacker. 2.Basım, Seçkin Yayıncılık, Ankara.

36. Henkoğlu T. (2011) Adli Bilişim. İstanbul. Pusula Yayıncılık, İstanbul.

37. İnce, H. Gündoğmuş Ü. N., Yazıcı Y. A., Çağdır S., Aliustaoğlu S. (2012) Türkiye'de Adli Tıp Uygulamalarında Adli Tıp Kurumunun Yeri. Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi 2012- Cilt 9/2.

38. John, J.L. (2012) Digital Forensics and Preservation, Digital Preservation Coalition, Great Britain. Doi: http://dx.doi.org/10.7207/twr12-03 pp.10

39. Karagülmez A. (2011) Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri. Seçkin Yayıncılık, Ankara.

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

40. Kateeb B., Altimus T. (2005) Computer Forensics. Alıntı: www.sis.pitt.edu/jjoshi/TELCOM2813/Spring2005/FinaleKateebAltimus.ppt (Son Erişim 2.12.2018)

42. Kessler G. C. (1999) The Internet, Intranets, Extranets and VPNs. ICA Network Technology Instıtute. Alıntı:http://www.webtorials.com/main/vici/presentn/kess-vpn/kessvpn.pdf(Son Erişim 03.12.2018)

43. Kızıltan MB. (2007) 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları. Yüksek Lisans Tezi. İstanbul Üni. Sosyal Bilimler Enstitüsü, İstanbul.

44. Koç S. , Biçer Ü. (2009) Adli Tıbbın Tarihsel Gelişimi, Türkiye'deki Yapılanması ve Sorunları. Alıntı: http://www.klinikgelisim.org.tr/eskisayi/klinik_2009_22/01.pdf (Son Erişim 06.05.2019)

45. Kur L. (2005) Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Seçkin Yayınevi, Ankara.

46. Koca M. (2003) İnternetle İlgili Ceza Hukuku Sorunları ve Bu Sorunlara İlişkin Çözüm Önerileri. Alıntı: http://www.bilisimsurasi.org.tr/dosyalar/96.doc (Son Erişim 30.04.2019)

47. Leong G. (1998) Computer Child Pornography: The Liability of Distributors? Criminal Law Review. Special Edition: Crime, Criminal Justice and the Internet:19-29.

48. Mehta S. (2017) Cyber Forensics and Admissibility of Digital Evidence. Alıntı: https://www.semanticscholar.org/paper/Cyber-Forensics-and-Admissibility-of-Digital-Cyber-Mehta/f6b402c3f1cae59a5dad9e31a810ca058164bd11(Son Erişim 2.12.2018**)**

49. National Instutite Of Justice Special Report.(2016)Forensic Examination Of Digital Evidence. Alıntı:https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx(Son Erişim 2.12.2018**)**

50. Naqvi S. (2015) The Signature Analysis. Alıntı: https://www.bcu.ac.uk/computing-engineering-and-the-built-environment/research/centre-for-cyber-security/consolidate/dissemination

51. Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı. (2005) İnternet Tarihi. Alıntı: http://www.internetarsivi.metu.edu.tr/tarihce.php

52. Orta M. (2015) Bilişim Suçları Ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması. Yetkin Yayınları, İstanbul.

53. Öner D. (2004) Bilgisayar Ağları. 2. baskı, Papatya Bilim, İstanbul.

54. Özbek M. (2013) Adli Bilişimde Delillerin Toplanması ve İncelenmesi. Yüksek Lisans Tezi. İstanbul Bilgi Üni. Sosyal Bilimler Enstitüsü, İstanbul.

55. Özbek VÖ. (2002) İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları. Dokuz Eylül Üni. Hukuk Fakültesi Dergisi, 4(1): 101-158.

56. Özdemir, S., Kalkan, Ö.K., Türkoğlu, A., Varol, M. ve Tokdemir, M. (2013) Elazığ'da Üniversite ve Lisede Öğrenim Gören Bilgisayar Bölümü Öğrencilerinin Adli Bilişim Suçlarına Yaklaşımları. NWSA-Medical Sciences, 1B0036, 8, (3), 16-25.

57. Özdilek AO. (2002) İnternet ve Hukuk. Papatya Yayıncılık, İstanbul.

58. Özen M, Özocak G. (2015) Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). Ankara Barosu Dergisi, Sayı:2015/1.

59. Öztürk Mİ. (2007) Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri. Yüksek Lisans Tezi. Ankara Üni. Sağlık Bilimleri Enstitüsü, Ankara.

60. Poonia A. S. (2014) Data Wiping and Anti Forensic Techniques. Compusoft, An International Journal Of Advanced Computer Technology, Sayı: 2014/12.

61. Sağlık Bakanlığı. (2018) Bilgi Güvenliği Politikaları Kılavuzu [PDF Belgesi]. Alıntı: https://dosyamerkez.saglik.gov.tr/Eklenti/25755,bilgi-guvenligi-politikalari-kilavuzu-ekler-haricpdf.pdf(Son Erişim 2.12.2018**)**

62. Saleem S. (2015) Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of DigitalForensics

63. Sansar M. (2017) Bilişim Suçlarının Tespiti ve Dijital Delillerin İncelenmesi. Alıntı: http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf(Son Erişim 30.04.2019)

64. Sarıhan TD. (1998) Herkes İçin İnternet. Desnet Yayınları, İstanbul.

65. Say K. (2006) Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi. Yüksek Lisans Tezi. Ankara Üni. Sağlık Bilimleri Enstitüsü, Ankara.

66. Sınar H. (2001) İnternet ve Ceza Hukuku. Beta Yayınları, İstanbul.

67. Singhal, G., Tandan, S. R., & Miri, R. (2013, May). IAA (Internet access account) based security modal for detection and prevention of cyber crime. International Journal of Engineering Research & Technology, 2(5), 67-70.

68. Soğukpınar İ. Veri ve Ağ Güvenliği Ders Notları. Alıntı: https://docplayer.biz.tr/1666203-Dr-i-sogukpinar-g-y-t-e-bil-muh-bol.html

69. Şenel Ö. D. (2015) Türk Ceza Hukuku Reformu Bağlamında Bilirkişilik. Doktora Tezi. İstanbul Üni.Adli Tıp Enstitüsü, İstanbul.

70. Şenyay L. Bilgisayara Giriş. Alıntı: http://kisi.deu.edu.tr//levent.senyay/bilgisayarprogramlama/1_%20Bilg%20prog%20giri%c5%9f.pdf(Son Erişim 19.10.2018)

71. Tan A. (2009). Adli Bilişim (Computer Forensic) [Blog yazısı]. Alıntı: https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ (Son Erişim 18.10.2018)

72. Taşçı U, Can A. (2015) Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997/2014. Fırat Üniversitesi Sosyal Bilimler Dergisi, 25(2): 229-248.

73. Taşkın ŞC. (2008) Bilişim Suçları. Beta Yayıncılık, Bursa

74. TBMM. (2012) Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu

(1/676) [PDF Belgesi]. Alıntı: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf

75. Tulum İ. (2006) Bilişim Suçları ile Mücadele. Yüksek Lisans Tezi. Süleyman Demirel Üni. Sosyal Bilimler Enstitüsü, Isparta.

76. Ukşal M. (2015) Mobile Forensics. Yüksek Lisans Tezi. İstanbul Bilgi Üni. Sosyal Bilimler Enstitüsü, İstanbul.

77. Ünver Y. (2001) Türk Ceza Kanununun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi. İstanbul Hukuk Fakültesi Mecmuası, 59(1-2).

78. Yalçın C. (2003) Sosyolojik Bir Bakış Açısıyla İnternet. C.Ü. Sosyal Bilimler Dergisi, 27:1, 77-89.

79. Yazıcıoğlu Y. (2009) Yeni Türk Ceza Kanunu. Oniki Levha Yayınları, İstanbul.

80. Yazıcıoğlu, RY. (1997) Bilgisayar Suçları, Alfa Yayınevi, İstanbul 1997

81. Yenidünya AC, Değirmenci O. (2003) Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları. Legal Yayıncılık, İstanbul.

82. Yıldız S. (2006) Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi. Nobel Akademik Yayıncılık, Ankara

83. Yılmaz D. (2004) Hacking: Bilişim Korsanlığı ve Korunma Yöntemleri. Hayat Yayınları, İstanbul.

84. Yılmaz S. (2010) Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu. Türkiye Barolar Birliği Dergisi 2010(87).

85. Yılmaz S. (2011) 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. Türkiye Barolar Birliği Dergisi 2011(12).

86. https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (Son Erişim 19.10.2018)

87. https://docplayer.biz.tr/2668892-Sifrelemenin-temel-elemanlari.html (Son Erişim 21.10.2018)

88. http://www.dijitaldeliller.com/veridepolama.html (Son Erişim 19.10.2018)

89. https://en.wikipedia.org/wiki/Degaussing(Son Erişim 02.12.2018)

90. https://www.techopedia.com/definition/1837/hidden-file (Son Erişim 02.12.2018)

91. http://www.yayin.adalet.gov.tr/dosyalar/pdf/atkm_2017.pdf (Son Erişim 09.05.2019)

92. https://www.emt.com.tr/tr/cozumler/guvenli-veri-imha-cozumleri-15(Son Erişim 30.04.2019)

93. http://www.dijitaldeliller.com/veridepolama.html(Son Erişim 30.04.2019)

94. https://www.batuhandemirdal.com.tr/veri-depolama-sistemleri-das-nas-san/(Son Erişim 30.04.2019)

95. http://members.tripod.com/enoter_hukuk/kriptoloji.htm (Son Erişim 01.05.2019)

96. https://tureng.com/tr/turkce-ingilizce/hacker (Son Erişim 06.05.2019)

97. https://tureng.com/tr/turkce-ingilizce/cracker (Son Erişim 06.05.2019)

98. http://www.istanbulanadolu.adalet.gov.tr/rehber/savcilik-sorusturma.php (Son Erişim 14.05.2019)

99. http://yazilim.soysal.biz/harddisk-dedigimiz-yenilmez-yutulmaz-icat/ (Son Erişim 14.05.2019)

100. http://www.ankara.adalet.gov.tr/sayfalar/yonerge/yonerge.pdf (Son Erişim 14.05.2019)

101. https://www.atk.gov.tr/adli-tip-kurumu-baskanligi.html (Son Erişim 14.05.2019)

102. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf (Son Erişim 30.04.2019)

ÖZGEÇMiŞ

I. Bireysel Bilgiler

Adı : Nazlı Nur

Soyadı : AKYOL ÇINAR

Doğum Yeri ve Tarihi : İstanbul 23 Ağustos 1980

Uyruğu : T.C.

Medeni Durumu : Evli

İletişim Adresi ve

Telefonu : Acıbadem Mah. Hukukçular Sitesi J Blok No:24
Kadıköy/İSTANBUL
Tel : 0 216 330 48 66
Cep : 0 532 476 48 87

II. Eğitimi

1. Lisans : 1999 - 2005 : Marmara Üniversitesi, Hukuk

2. Lise : 1994 - 1995 : İzmit Lisesi, 1996-1998 Atılım Lisesi

4. ilköğretim : 1986 Ulugazi İlkokulu, 1991 Kocaeli Koleji, Eskişehir
Ortaokulu

III. Unvanları : Avukat

IV. Mesleki Deneyimi : 08.12 2004 ile 23.12.2005 Avukatlık Stajı, 06.11.2006 tarihi itibariyle fiili olarak ceza hukuku alanında avukatlık.

V. Eğitim ve Seminerler

- Staj bitirme tezi, ‘Ceza Muhakemesi Hukukunda Çocuk Yargılaması’
- 11/2005 Borçlar Kanunu Tasarısının Değerlendirilmesi Sempozyumu, İstanbul Barosu, İstanbul Üniversitesi
- 09/2005 Hukuk İngilizcesi, Staj Eğitim Merkezi.
- 07/2005 Çocuk ve Genç Adalet Sistemi Sempozyumu, İstanbul Barosu, Bahçeşehir Üniversitesi
- 06/2005 CMK Meslek İçi Eğitim Semineri, İstanbul Barosu CMK Uygulama Servisi
- 05/2005 TCK ve CMK’ daki Yeni Gelişmeler Meslek İçi Eğitim Semineri, Marmara Üniversitesi
- 12/2005 Bahçeşehir Üniversitesi ve İstanbul Barosu'nca düzenlenen Ceza Muhakemesi Kanunu ve 6 Aylık Uygulanmasının Değerlendirilmesi Sempozyumu, Bahçeşehir Üniversitesi
- 06/2008 Kadın Hakları Meslek İçi Eğitim Semineri, İstanbul Barosu Kadın Hakları Merkezi
- 06/2008 Avrupa İnsan Hakları Sözleşmesi Meslek İçi Eğitimi, İstanbul Barosu
- 10/2011 Bilişim Hukuku İleri Eğitim Programı, Türkiye Barolar Birliği ve Türkiye Avukatları Sosyal Yardımlaşma ve Dayanışma Vakfı

V. Diğer Bilgiler : İstanbul Barosu İnsan Hakları Komisyonu ile Çocuk Hakları Merkezi üyelikleri bulunmaktadır.