TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİMDE STANDARDİZASYON, SERTİFİKASYON, AKREDİTASYON VE EN İYİ UYGULAMALAR

Pelin ÖZKAYA

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2021

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİŞİMDE STANDARDİZASYON, SERTİFİKASYON, AKREDİTASYON VE EN İYİ UYGULAMALAR

Pelin ÖZKAYA

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2021

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Adli Bilişimde Standardizasyon, Sertifikasyon, Akreditasyon ve En İyi Uygulamalar" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Pelin ÖZKAYA

Tarih:

İmza:

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Adli Bilimler Anabilim Dalında
Pelin ÖZKAYA tarafından hazırlanan
"Adli Bilişimde Standardizasyon, Sertifikasyon, Akreditasyon ve En İyi Uygulamalar" adlı tez çalışması
aşağıdaki jüri tarafından YÜKSEK LİSANS TEZİ olarak OY BİRLİĞİ ile kabul edilmiştir.

Tez Savunma Tarihi: 15.06.2021

Prof.Dr. Refik SAMET
Ankara Ü. Mühendislik Fakültesi
Jüri Başkanı

Doç.Dr. Çelebi ULUYOL
Gazi Ü. Gazi Eğitim Fakültesi
Üye

Dr.Öğr.Üyesi Yılmaz AR
Ankara Ü. Mühendislik Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof. Dr. Fügen AKTAN
Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

ÖNSÖZ

Adli bilişimde elektronik verilerin delil haline dönüştürülmesi ve mahkemelerde yargılama sürecine hukuka uygunluk çatısı altında dahil edilmesi, bilişim sistemlerinden delil elde etme özelliği bulunan yazılım ve donanımlarla mümkündür. Bu yazılım ve donanımların etkili şekilde kullanılabilmesi ise, uluslararası kurallarla düzenlenmiş bir takım özel prosedürlerle sağlanmaktadır. Prosedürlerin, ilgili eğitimleri almış adli bilişim uzmanlarınca yürütülen aşamalarda ve uluslararası standarda bağlı akredite edilmiş laboratuvarlarda uygulamaya konulması, adli bilişim sürecinin olması gereken şeffaflıkla, tarafsızlıkla ve hukuka uygun şekilde yürütülmesi için elzemdir.

Bugün Adli Bilişim olarak bilinen bilim dalının ortaya çıkışı, bu alanda çalışma yapan uzmanlar ve araştırmacıların başlattığı süreç modelleriyle ortaya çıkmış, bu modeller baz alınarak aşamalar belirlenmiş, bu aşamalara uygun en iyi uygulama rehberleri ve standartlar oluşturulmuştur.

Bu tez çalışmasında, bahsi geçen model çalışmalarının çerçevesi çizilmiş, modeller arasındaki benzerlikler ve farklılıklar gözetilerek öneri bir model sunulmuştur. En iyi adli bilişim uygulamaları, standardizasyon, akreditasyon ve sertifikasyon kuralları ile hukuki düzenlemeler araştırılarak, önerilen modele ve Türkiye'deki duruma uyumu konusunda tavsiyelerde bulunmaya çalışılmıştır.

Bu süreçte desteği, yardımı ve tarafıma olan inancıyla, beraber çalışmaktan onur ve mutluluk duyduğum değerli danışman hocam Prof. Dr. Refik Samet'e en içten teşekkürlerimi sunuyorum. Azimli, kararlı ve güçlü bir birey olarak yetişmemdeki tüm emekleri ve sonsuz motivasyonları için sevgili aileme, enerjisi, hevesi ve merakı tükenmeyen kendime de sonsuz teşekkürler.

SİMGELER VE KISALTMALAR

A2LA	American Association for Laboratory Accreditation
ACEE	AccessData Certified Examiner for Enterprise
ACPO	Association of Chief Police Officers
API	Application Programming Interface
ANAB	ANSI National Accreditation Board
ANFOR	Association Française de Normalisation
ANSI	American National Standards Institute
APAC	Asia Pacific Accreditation Cooperation
APLAC	Asia Pacific Laboratory Accreditation Cooperation
ASCLD	American Society of Crime Laboratory Directors
ASCLD/LAB	American Society of Crime Laboratory Directors/Laboratory Accreditation Board
ASTM	American Society for Testing and Materials
BSI	British Standards Institution
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketings Act
CCCA	Comprehensive Crime Control Act
CCCA	Credit Card Fraud Act
CCI	Certified Cyber Investigator
CDaCT	Certified Data Collection Technician
CERT	Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CFFC	Centre for Forensic Computing
CFFTPM	Computer Forensics Field Triage Process Model
CFIP	Certified Forensic Investigation Practitioner
CFL	Cyber Forensics Laboratory
CFReDS	Computer Forensic Reference Data Sets
CFIS	Certified Forensic Investigation Specialist
CFTT	Computer Forensic Tool Testing
CFVA	Certified Forensic Video Analyst

CFVT	Certified Forensic Video Technician
CLFP	Certified Linux Forensic Practitioner
CM	Common Model
CMFS	Certified Mac Forensics Specialist
CMA	Computer Misuse Act
CMI	Certified Malware Investigator
CMK	Ceza Muhakemesi Kanunu
CoP	College of Policing
CPIA	Criminal Procedure and Investigations Act
DCFL	Defense Computer Forensic Laboratory
DC3	Department of Defense Cyber Crime Center
DCSA	Digital Crime Scene Analysis
DEFR	Digital Evidence First Responders
DES	Digital Evidence Specialists
DFRWS	Digital Forensic Research Workshop
DIN	Deutsche Institut für Normung
EA	European Accreditation Association
ECPA	Electronic Communications Privacy Act
ECTEG	European Cybercrime Training and Education Group
eDCA	eDiscovery Certified Administrator
EIDIP	Enhanced Integrated Digital Investigation Process
EİK	Elektronik İmza Kanunu
ENFSI	The European Network of Forensic Science Institutes
FAIoT	Forensics-aware IoT
FSEK	Fikir ve Sanat Eserleri Kanunu
GDPR	General Data Protection Regulation
IAAC	Inter American Accreditation Cooperation
IACIS	International Association of Computer Investigative Specialists
IAF	International Accreditation Forum
IDIP	Integrated Digital Investigation Process
IHCFC	International Hi-Tech Crime and Forensics Conference
IICTC	International Information and Communication Technology Council

ILAC	International Laboratory Accreditation Cooperation
IOCE	International Organization on Computer Evidence
IR	Incident Response Process Model
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITL	Information Technology Laboratory
KVKK	Kişisel Verilerin Korunması Kanunu
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NPCC	National Police Chiefs' Council
NPIA	National Policing Improvement Agency
NSRL	The National Software Reference Library
OL-DCFL	Operating Location – Defense Computer Forensics Laboratory
PAC	Pacific Accreditation Cooperation
PACE	The Police & Criminal Evidence Act
POLKA	Police On-Line Knowledge Area
PPA	The Privacy Protection Act
RCFL	Regional Computer Forensics Laboratory
RIPA	Regulation of Investigatory Powers Act
SIS	Swedish Institute for Standards
SWG	Scientific Working Group
SWGDE	Scientific Working Group on Digital Evidence
TCK	Türk Ceza Kanunu
TWG	Technical Working Group

ŞEKİLLER

ÇİZELGELER

1. GİRİŞ

İnsanlığın varoluşuyla ortaya çıkan ve başkalarına zarar verici olarak nitelenen eylemler, yerleşik hayata geçiş ve hukuk düzeninin kurulması ile birlikte "suç" adını almış ve suç olarak kabul edilen bu fiiller, gittikçe büyüyen ve yerleşen toplumların refahı ve güvenliği için bir düzene oturtulmak amacıyla, belli bazı yaptırımlara bağlanmıştır. Toplumlar genişleyip geliştikçe suç niteliği taşıyan eylemler de çeşitlenmiş ve yeni suç tipleri ortaya çıkmaya başlamıştır.

20. yüzyılın sonlarına doğru bilgi toplumuna geçişle birlikte, bilimdeki gelişmelerin hızla yaygınlaşması ve yeni teknolojilerin üretilmesi sonucunda bilişim sistemleri hayatımızın neredeyse tamamına yakınında önemli roller üstlenmeye başlamıştır. Masaüstü bilgisayarların dizüstü bilgisayarlara ve hatta tabletlere evrimi, en nihayetinde cep telefonlarının çoğu durumda onların yerini alabilecek kadar gelişmesi ve fonksiyonlu hale gelmesi ile birlikte suç kavramı ve suç işleme stilleri de aynı paralelde ve hatta daha hızlı bir şekilde gelişmiş ve çeşitlenmiştir. Suçluların bilişim teknolojilerinin bu hızından ve gelişiminden yararlanarak işledikleri fiiller "Bilişim Suçları" denilen kavramı oluşturarak, bu kavramın literatüre ve ceza hukukuna giriş yapmasına vesile olmuş, elektronik sistemler de gerek bu suçların hedefi, gerekse aracı haline gelerek ilgili kanunlarda kendine yer bulmuştur.

Teknolojinin gelişimi ve yeni elektronik cihazların icadı düşünüldüğünde bilişim suçlarının yeni bir suç tipi olduğu düşünülebilir ancak aslında tarihi çok daha eskilere dayanmaktadır. İlk olarak hangi tarihte gerçekleştiği konusunda bazı belirsizlikler söz konusu olsa da, elektronik sistemlerin ilk üretiminden itibaren tarihin ilk bilişim suçlarının da ortaya çıkmış olabileceğini söylenebilir. 1834 yılında tahvil tüccarlığı yapan Blanc kardeşlerin Fransız Telgraf Sistemini hackleyerek finansal piyasa bilgilerini çalması, kayda geçmiş ilk siber saldırı olarak kabul edilmektedir (Ducklin, 2018). Hacklemenin ilk gerçek başarısı ise, 1903'de Nevil

Maskelyne'nin Guglielmo Marconi'nin kablosuz telgraf sistemine yönelik hakaret edici Morse kod mesajları göndermesi sayılmaktadır (Gingerich, 2017). 1939'da Alan Turing, Harold Keen ve Gordon Welchman'ın Alman Enigma-makine ile şifrelenmiş gizli mesajları deşifre edebilen elektromekanik bir cihaz olan "Bombe"yi geliştirmeleri bilinen en iyi askeri kod kırma olayı olarak kabul edilmektedir (Smith, 2014).

Telefon aramalarının nasıl yönlendirildiğinin bazı kişiler açısından merak konusu olması, 1950'lerde "*Phreaking*" teriminin ortaya çıkmasını sağladı. O dönemde, ücretsiz veya indirimli telefon hizmetleri almak amacıyla bir telefon ağındaki donanım ve frekans açıklarından yararlanmak olarak tanımlanan "telefon dolandırıcılığı suçu" 1970'lere doğru yaygınlaşmaya başladı (Rader ve Rahman, 2013, s:25). "Captain Crunch" olarak da bilinen John Draper'ın, ücretsiz telefon görüşmeleri yapmak için halka açık telefon sistemlerini kullanması Steve Jobs ve Steve Wozniak'a ilham oldu ve sonunda tanınmış bilgisayar şirketi Apple doğdu (Williams, 2015).

Belgelenen en eski virüsler 1970'lerin başında ortaya çıkmaya başladı. ARPAnet'teki DEC PDP-10 bilgisayarları aracılığıyla yayılan ve kendi kendini kopyalayan bir program olan "*Creeper Worm*" bilinen ilk virüs olarak kabul edilmektedir. "Ben bir sarmaşığım, yapabiliyorsan beni yakala! (*I'm the creeper, catch me if you can!*)" virüsün bıraktığı ünlü mesajdır (Loebenberger ve Wielpütz, 2007, s:2). 1974'te bir bilgisayara yüklenen göze çarpmayan bir program, kendisinin birçok kopyasını çıkararak sistem performansını düşürüp çökmesine neden oldu, hızlı çoğalabilmesi nedeniyle "Rabbit (*Wabbit*) Virüsü" olarak adlandırıldı.

Tarihteki ilk Truva atının ise 1975 yılında, John Walker tarafından yazılan "*Animal/Pervade*" olduğu düşünülmektedir. Kötü niyetli veya zarar verici bir amaçla üretilmeyen oyun, kendisinin bir kopyasını yerleştirerek oynanması sebebiyle kullanıcılar aracılığıyla birden çok bilgisayara yayıldı (Serbu, 2016).

1980'ler artık kişisel bilgisayarların (PC - *Personal Computer*) ortaya çıkması, insanların evlerde, okullarda ve iş yerlerinde iletişim kurmalarına, öğrenmelerine ve keşfetmelerine fırsat sunar hale gelmişti. Bilgisayarın ve internetin bu şekilde kişilerin hayatının bir parçası olmaya başlamasının, beraberinde farklı illegal faaliyetleri de getirmesi elbette kaçınılmazdı. Bu durum yeni korsan ticari yazılımların, virüslerin ve solucanların yaratılmasını ve serbest bırakmasını da içeriyordu. İlk siber saldırı olduğu kabul edilen "Mantık Bombası", 1982'de Soğuk Savaş sırasında, Rusya'nın Sibirya gaz boru hattını kullanmasını engellemek için oluşturuldu ve boru hattını kontrol eden bilgisayar sistemine kod eklenerek, fiziksel bir patlayıcı kullanılmadan bu boru hattı patlatıldı (Purdue University, 2014).

1988'lerden itibaren yıkıcı virüsler çağının başladığı kabul edilir. "*Festering Hate*" virüsünün ilk ortaya çıkışıyla birlikte, artık virüsler sabit sürücülerdeki, bellek sürücülerindeki ve disketlerdeki her dosyayı da yok edici bir özelliğe bürünmeye başlamıştı (Atamaniuk, 2020). 1988'de Cornell Üniversitesi'nde Bilgisayar Bilimleri alanında master öğrencisi olan Robert Morris, internetin büyüklüğünü keşfetme niyetiyle bilinen ilk solucanı yarattı (Morris Solucanı). Solucanın yayılma mekanizmasındaki bir hata sebebiyle çok daha hızlı bir şekilde bulaşmasına yol açtığı için kısa sürede kısır bir hizmet reddi saldırısı haline geldi (Kehoe, 1992, s:61). 1986'da kabul edilen Bilgisayar Sahtekarlığı ve Kötüye Kullanım Yasası (*Computer Fraud and Abuse Act*) uyarınca suçlu bulunan ilk kişi oldu ve bu olay sonucunda aynı yıl Bilgisayar Acil Durum Müdahale Ekibi (CERT - *Computer Emergency Response Team*) kuruldu (Kelty, 2011).

90'larda virüsler de internette e-postalar ve web siteleri aracılığıyla yayılmaya başladı. 1999'da "Melissa Virüsü" kendisini büyük bir ölçekte yaymak için elektronik postayı kullanılan ilk virüs olarak kabul edilmektedir. Bu virüs, kendisini alan her kullanıcının adres defterlerindeki ilk 50 adrese kötü amaçlı bir e-posta göndermek için tasarlandı ve virüs, bulaşan her bilgisayara en az 50 ek e-posta göndererek yayılmayı amaçladı (Harán, 2018).

Kurbanlarının banka bilgilerini yakalayabilen bir virüsün ortaya çıkışı 2007 yılında "Zeus" (*Zbot*) adlı virüs ile mümkün oldu. Bu virüs, kullanıcının bir bankacılık web sitesinde oturum açarken klavyesine girdiği tüm tuş vuruşlarını kaydederek, çevrimiçi hesaplarına erişmek için kullanılan karakter dizisini 'izlemekte' ve botun denetleyicilerine göndermektedir. 2011 yılında değişik bir formla tekrar ortaya çıktı (Etaher ve ark.,2015).

Önceki tarihlerde ortaya çıkan pek çok virüs zarar verme amacı olmayan birtakım denemelerin sınırının kontrol edilememesinden veya küçük çaplı zararlar verme amacından kaynaklanıyorken, 2010 yılında ortaya çıkan "Stuxnet solucanı" cihazlara fiziksel zarar verme amacıyla tasarlanmış gibi göründüğü (Farwell ve Rohozinski, 2011, s:24) ve arkasında kişiler yerine devletler bulunduğundan (Lin, 2012, s:519) şüphelenildiği için "dünyanın ilk dijital silahı" olarak adlandırıldı (Iasiello, 2013). Bu solucan Tahran'ın 1.000 nükleer santrifüjünü yok etti ve hedeflenen tesisin dışındaki 60.000'den fazla bilgisayara bulaştı.

2016'da başkanlık seçimleri zamanında Demokratik Ulusal Komite çok sayıda kimlik avı e-postası aldı ve Hillary Clinton'ın kampanya çalışanının hatası sebebiyle yaklaşık 60.000 e-postaya ulaşıldı ve daha sonra elde edilen bilgiler WikiLeaks'a sızdırıldı (Harding, 2016). 2017 yılında "*WannaCry*" olarak bilinen bir fidye yazılımı, birkaç gün içinde en az 150 ülkede, içinde pek çok banka, telekomünikasyon şirketi ve hastanenin de bulunduğu yüz binlerce işletme ve kuruluşun bilgisayarını kilitledi ve dosyalarını şifreledi. Saldırganlar, dosya kilidini açmak için kullanıcılardan yüzlerce dolar talep etti.

2018'de ortaya çıkan "Thanatos", Bitcoin Cash'te fidye ödemesini kabul eden ilk fidye yazılımı olarak kabul edilmektedir, çünkü fidyenin Ethereum, BitCoin ve BitCoin Cash ile transfer edilmesine izin verilir. Bu yazılım, şifrelenmiş her dosya için yeni bir anahtar kullanır ancak anahtarlar hiçbir yere kaydedilmemekte, fidye ödense bile dosyaların şifresini çözebilecek bir yöntem bulunmamaktadır. Haziran 2018'in sonlarında, Cisco'nun güvenlik uzmanları kötü amaçlı kodu kırmayı ve

ücretsiz bir "*ThanatosDecryptor*" oluşturmayı başardı (Palmer, 2018). 2019 yılında, aralarında Almanya Başbakanı Angela Merkel'in de bulunduğu yüzlerce politikacıya yönelik bir siber saldırı başlatıldı. Mali bilgiler, kimlik kartları ve özel sohbetler bilgisayar korsanlarının daha sonra çevrimiçi olarak yayınladıkları veriler arasında yer aldı (Connolly, 2020).

Elektronik aygıtların ve elbette internetin icadıyla birlikte, yukardakilerle sınırlı olmayan, yaygın olarak bilinen veya bilinmeyen çok sayıda saldırı faaliyetinin yaşanmasının temel nedeni, günümüzde bilişim suçu veya siber suç adı verilen bu suçların sınır ötesi nitelik kazanmasıdır. Özellikle internet kullanımının rahatlığı ve ucuzluğu, saldırganların dünyanın herhangi bir yerindeki bir bilişim sistemine girmesine olanak sağlamaktadır. Önceleri daha kişisel boyutta zararlar söz konusu olabiliyorken, artık devletler boyutunda ve ulusal güvenliklere yönelik tehditler içeren, daha büyük çaplı zararlar söz konusudur.

Ceza hukukunun bir bilim dalı olarak kabul edildiği yıllarda, suçun konusunu oluşturan klasik suç tiplerinde fail fiziki olarak belli bir mekanda suç işlediği için tespiti daha kolay olmaktaydı. Zamanla suçların uluslararası, hatta kıtalararası nitelik kazanması sebebiyle tespiti de haliyle zorlaşmaya başladı. Elektronik cihazların alınıp satılmasındaki hız, suç delillerinin yok edilmesi için bu cihazların imhasındaki kolaylık, başkalarının cihazlarını ya da sistemlerini kullanmadaki yaygınlık da suçluların tespitinin ve yakalanmasının zorluğunu arttıran etkenler olmaktadır. Bu sebeplerle, bilişim suçları ile mücadelede, suçun uluslararası niteliği de baz alınarak, tüm ülkelerde paralel hukuki ve teknik düzenlemelere ihtiyaç olduğu fark edilmeye başlandı. Birçok ülkede bağımsız ve detaylı olarak düzenlenmiş hukuki metinlerin olmadığı düşünüldüğünde bunun önemi daha da belirgin hale gelmektedir. Yetersiz düzenlemeler ve uygulamalar hem kişilerin hem toplumların hem de ülkelerin güvenliğini tehdit eden bir unsur niteliğindedir.

Adli bilişim sadece ceza hukuku tabanlı adli olaylarda suç ve suçlunun tespitinde değil, özel hukuk ilişkilerinde de uygulama alanı bulabilmektedir.

Elektronik cihazların söz konusu olduğu davalarda delil tespiti veya olay analizi için adli bilişim yöntemleri kullanılabilmektedir. Örneğin, boşanma davaları, internet üzerinden yapılan satın alma işlemleri, elektronik ortamda üretilen eserler, yazılan bilgisayar programları, finansal sistemler içindeki elektronik belgeler vb. özel hukukun konusuna girmektedir. Elektronik imza ve elektronik sertifika ile ilgili vakalarda da başvurulan bir yöntem olmakta ancak bu sayılanlar daha çok Doğrudan Bilişim Suçu yerine bilişim sistemleriyle bağlantılı Dolaylı Bilişim Suçları içerisinde kabul edilmektedir.

Adli bilişim aynı zamanda, şirketlerin kurumsal işlerinde, bilgi ile veri güvenliğinin sağlanmasında da başvurulan bir alan olmaya başlamıştır, başvurmayan şirketler için de ciddiye alınması gereken bir konu olduğu açıktır. Uluslararası ve küresel bazda iş yapan büyük çaplı şirketlerde çok sayıda verinin işlenmesi neticesinde, güvenlik ihtiyacı da aynı oranda artmış, gerek içeriden gerekse dışarıdan çok sayıda tehditle karşı karşıya kalmaya başlamışlardır. Sektörde başarılı ve iyi işleriyle anılan kuruluşlara yapılacak bir saldırı veya tespit edilecek bir güvenlik ihlali, eğer yeterli tedbir alınmamışsa, bu kuruluşlar için ciddi boyutlarda mali zararlara ve itibar kaybına neden olabilmektedir. Tıpkı suçla mücadelede, farklı elektronik sistemler için o sistemde uzman olan adli bilişimcilere ihtiyaç olduğu gibi, kurumlardaki farklı bilgi işlem hatalarını çözmek için de, ilgili alanda yetişmiş adli bilişim uzmanlarına ihtiyaç vardır. Ticari sırların rakiplerin eline geçmesi, fikri mülkiyet hırsızlıkları veya önemli verilerin çalınması gibi çeşitli şekillerde gerçekleşecek bu zararların önlenmesi için kuruluşlar önlemler almak ve bunu yapmak için bütçelerinin önemli bir kısmını adli bilişime, denetimlere ve güvenliğin sağlanmasına ayırmak zorundadır (Imtiaz, 2006).

Bireyler ve kurumlar kadar devletlerin birbirleriyle veya kuruluşlarla olan ticari ve siyasi ilişkilerindeki güvenliği için de adli bilişim oldukça önemlidir, çünkü istihbaratın ve iletişimin elektronik ortamlar aracılığıyla yürütülmesi, bu alanın güvenliğine azami özenin gösterilmesini gerektirmektedir. Bağımsız çalışan çok sayıda siyah şapkalı hackerın birçok farklı devlet kurumuna yaptığı saldırılara sıklıkla tanık olmaktayız. Bununla birlikte, geçmiş tarihlerde devletler arasında süre

gelen ve çok sayıda kişinin ölümüne yol açan fiziksel savaşlar, internetin önlenemez gelişimiyle yerini siber savaşlara bırakabilecektir. İletişimin ve istihbaratın gizlice dinlenerek devlet sırlarının öğrenilmesinden, kritik altyapılara yapılacak saldırılara kadar geniş bir yelpazede çok büyük riskler söz konusudur. Tüm bu durumlar siber güvenliğin özel kuruluşlar ve kamu kurumları tarafından büyük yatırımlar yaptığı ciddi bir ekonomik sektör haline gelmesine de sebep olmuştur (Öğün ve Kaya, 2013, s:164).

Elbette ki, adli bilişim ile siber güvenlik pek çok açıdan birbirlerine benzemekte ve benzer konulara yönelmektedir ancak aralarında birtakım farklılıklar da bulunmaktadır. Adli bilişim gerçekleşmiş veya gerçekleştiği düşünülen bir olayda delillerin toplanması ve analizi noktasında başvurulan bir yol iken, siber güvenlik söz konusu bu olayları gerçekleşmeden önce önlemeye, kuruluşları siber saldırılara karşı korumaya yönelik tedbirlerden oluşmaktadır. Bu durumda, gerekli önlemler alınmadığında veya alınıp başarısız olunduğunda adli bilişim suçun ve suçlunun tespitini yapmak ve tehlike altındaki verileri kurtarmak için devreye girecektir (Krakoff, 2021). Bu açıdan gerek siber güvenlik gerekse adli bilişim aynı ortak amaca değişik açılardan hizmet etmektedir.

Siber tehditler, kamudan özele tüm sektörler, kuruluşlar, işletmeler ve kişiler için var olan ve büyüyen bir tehdittir ve bu tehdidin önlenmesi ile bu tehditle etkin şekilde mücadele edilebilmesi için hem siber güvenlik açısından hem de adli bilişim açısından bilgili ve yetenekli uzmanlara ihtiyaç vardır. Bu sebeple devletlerin, kurumların ve özel sektörün siber güvenliğe yatırım yaparken adli bilişimi ihmal etmesi ve maliyetlerden kaçınması, yeni sıkıntıların doğmasına yol açacaktır. Olay mahallinde bulunan çok sayıda veri arasından kanıt niteliği taşıyanların bulunması, hatta bu işlemlerin bazı zamanlar hasar görmüş cihazlar üzerinden yapılması ve elde edilen verilerin değiştirilmeden ve güvenilir şekilde analiz edilmesi, adli bilişimin önemli görevler gerçekleştirdiğini ve siber güvenliğe faydalı bir yol arkadaşı olduğunun kanıtıdır.

Bahsi geçen tüm bu ve buna benzer sebeplerle, elektronik platformda veya bu platformlar aracılığı ile gerçekleştirilen çok sayıda eylemde, bu eylemler suç unsuru oluşturuyorsa faillerinin tespitinde elbette ki yine bilişim teknolojileri kullanılmakta ve bu teknolojilerin en verimli ve hukuka uygun şekilde işletilebilmesi için adli bilişim biliminin önemi bu çalışmada tarafımızca vurgulanmaktadır. Bu kapsamda, Adli Bilişim uygulamalarının ve bu uygulamaların standardizasyonlarının, laboratuvarların akreditasyonlarının, uzmanların sertifikasyonlarının ve hukuk sistemindeki mevzuatların incelenmesi ve karşılaştırılması neticesinde, varılacak en faydalı sonucun Türkiye'deki sisteme yönelik tavsiyelerinin yer aldığı bir çalışma oluşturmak amaçlanmıştır. Bu amacın gerçekleştirilmesinde yol haritası olarak, adli bilişim uzmanlarının ve araştırmacılarının ürettiği modellerden yola çıkarak, gelişen yeni teknolojilere uyum sağlayan, kapsamlı ve geniş bir araştırma için kullanışlı olduğu düşünülen bir "Öneri Model" de bu çalışma kapsamında sunulmuş olup, model basamaklarına uygun düşen, çalışmada bahsi geçen en iyi uygulamalar ve standartlara dikkat çekilmiştir.

Elbette çok sayıda ülkede kayda değer ve faydalı pek çok çalışma ve düzenleme yapılmaktadır ancak bu tez çalışması, gerek hukuki düzenlemeler, gerekse prosedürler açısından, en bilinen ve bu alanlara en çok yatırım yapan Amerika Birleşik Devletleri ile Birleşik Krallık üzerinden inceleme yapılmakla sınırlı bırakılmıştır. Çalışmanın son kısmında, Türkiye'deki durumdan bahsedilerek, hangi hususların ülkemizde uygulanabileceğine dair fikirler üretilerek, ileri bir dönemde yapılabilecek kanun çalışmalarına ve adli bilişimle ilgili herhangi bir gelişmeye yönelik rehber niteliği taşıyabilecek faydalı bir çalışma ortaya konulmaya çalışılmıştır.

Bu tez çalışmasının diğer bölümlerinde yapılan çalışmalar şu şekilde özetlenebilir:

- Adli bilişimin tanımı, tarihçesi ve farklı elektronik cihazlarla bağlantılı türleri ile bu cihazlardan elde edilen dijital deliller;
- Uzmanlarca gerçekleştirilen çeşitli süreç modelleri;

- En iyi uygulama rehberleri;
- Temel standartlar;
- Laboratuvar akreditasyon standartları;
- Uzmanların sertifikasyon ve eğitim prosedürleri;
- Hukuki düzenlemeler ve örnek mahkeme kararları.

1.1. Adli Bilişim

Nasıl ki bir insan şüpheli bir şekilde öldüğünde, ölüm sebebini ve suçun failini bulmak için ölü bedeni belli standartlara uygun şekilde açılıyor ve inceleniyorsa, bilişim sisteminin hedef alındığı veya aracı olarak kullanıldığı olaylarda da benzer uygulamalar söz konusu olmaktadır. Olaya dahil olan bilişim sistemi Adli Tıp bilimindekine benzer şekilde, belirlenmiş prosedürler dahilinde, belli standartlara sahip, özel bazı araçlar vasıtasıyla açılıp incelenmektedir. Adli bilişim aynı zamanda "Kriminalistik" bilimi ile de benzerlik göstermektedir; çünkü her ikisinde de, olay yerine gidilip deliller toplanmakta, laboratuvar ortamında incelenip analiz edilmekte, en sonunda da raporlaştırılıp mahkemeye sunulmaktadır. Burada hedeflenen, suçlunun ortaya çıkarılması olduğu kadar, masum kişilerin yanlış yere suçlanarak cezalandırılmasının da önüne geçmektir. Hem Adli Tıp bilimine hem de Kriminalistik bilimine benzer özelliklere vakıf olması sebebiyle, bilişim sistemlerinde ve elektronik cihazlarda vücut bulan adli olaylarda yürütülen prosedürler, bugün dünyada Adli Bilimler içinde kabul edilen bir bilim dalı olarak "Adli Bilişim" adını almıştır.

1.1.1. Adli Bilişim Nedir?

"Adli" kelimesi, 'forum' anlamına gelen Latince 'forensis' kelimesinden gelmekte ve genel olarak şüpheliyi mahkum etmek veya beraat ettirmek için

mahkemeye kanıt sunulması prosedürünü anlatmak için kullanılmaktadır (Iorliam, 2018).

En genel tanımıyla Adli Bilişim; bilişim sistemleri ile elektronik cihazlardan elde edilen dijital verilerin, ceza kanunlarında suç kabul edilen fiillerle olan ilişkisini ortaya çıkarmak ve bu delilleri ilgili adli makamlara sunmak amacıyla yürütülen uluslararası standartlara sahip işlemler bütünüdür (Emekci ve ark., 2016, s:10). Palmer, Adli Bilişimi "Sayısal kaynaklardan elde edilen dijital kanıtların korunması, toplanması, doğrulanması, tanımlanması, analizi, yorumlanması ve sunulmasına yönelik bilimsel olarak türetilmiş ve kanıtlanmış yöntemlerin, suç teşkil eden olayların yeniden inşasını kolaylaştırmak veya ilerletmek amacıyla kullanılması" şeklinde tanımlamıştır (Palmer, 2001, s:16). Koltuksuz'a göre ise; "Adli Bilişim, elektromanyetik – elektro optik ortamlarda muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmalarının bütününü oluşturmaktadır." (Koltuksuz, 2007, s:43).

Çeşitli dijital platformlar üzerinden elde edilen veriler, ilk bakışta anlaşılabilir nitelikte olmadıklarından, bu verilerin delil niteliğinin bozulmaması ve zarar görmemesi için gerekli tedbirler alınarak, adli makamlara sunulabilir hale getirilmesi gerekmektedir. Adli bilişim, tam da bu kapsamda, işlem görecek bilişim sistemine özel, uluslararası kabul görmüş bilimsel ve teknik prensiplerin uygulandığı bir bilim dalıdır.

Adli bilişim yapısı itibari ile birkaç disiplini bünyesinde birleştiren multi-disipliner bir alan olarak karşımıza çıkmaktadır. Bilişim sistemlerinin ve elektronik özellik gösteren verilerin incelenmesi bakımından Mühendislik Bilimleri ile suç niteliği kazanmış olayların soruşturulması ve kovuşturulması noktasındaki düzenlemeler açısından Hukuk Biliminin harmanlandığı bir alan olmakla birlikte,

olay yerinde gerçekleşen arama, kopyalama ve el koyma faaliyetlerinde Kolluk Kuvvetlerinin de sahnede olduğu bir usul bulunmaktadır.

1.1.2. Adli Bilişimin Tarihçesi

Adli bilimler tarihi çok daha eskilere giden bir alan olmakla birlikte, soruşturmalarda bir bilim dalı olarak kullanılması 19. Yüzyıl civarına denk gelmekte, ilk gerçek adli bilimler laboratuvarının kuruluşunun ise 1932'de FBI tarafından geliştirildiğini belirtilmektedir (Rudin ve Inman, 2002). Adli bilişim ise, 1980'lerde kişisel bilgisayarların kullanılmasından sonra yaygınlaşan elektronik ortamdaki suç faaliyetlerinin, klasik soruşturma yöntemlerine nazaran farklılık göstermesi sebebiyle dikkat çekmeye başlayan çok daha genç bir alandır (Parasram, 2017, s: 274).

Bilgisayarlar, 1960 - 1980 yılları arasında devlet kurumlarının, şirketlerin, araştırma merkezlerinin ve üniversitelerin kullandığı, sınırlı görevleri olan endüstriyel bir cihaz olarak ortaya çıkmıştı. O sıralarda işlenen az sayıdaki bilişim suçu, hem yöneticiler hem de devlet kurumları için üzerinde ciddiyetle durulması gereken bir mesele olarak görülmediğinden, bu durumlar için uygulanacak herhangi bir prosedür ve kural olmadığı gibi, araç ve bu araçları kullanabilecek bilgiye ve eğitime sahip uzmanlar da bulunmuyordu (Pollitt, 2010, s:6). IBM PC'nin ortaya çıkışı ile program kodu yazmanın, işletim sistemlerinin ve donanımların iç kısımlarına erişebilmenin mümkün hale gelmesi (Pollitt, 2010, s:6) ve farklı ülkelerdeki suç laboratuvar yöneticilerinin "Amerikan Suç Laboratuvarı Yöneticileri Derneği (ASCLD - *American Society of Crime Laboratory Directors*)"ni kurması (ASCLD, 2021) bugünkü adli bilişimin temellerinin atılmasını sağladı. Belirli bir adli disiplindeki uzman gruplar, standartları, en iyi uygulamaları ve protokolleri geliştiren organlara dönüşmeye başladılar. Bu alanda çalışmak üzere 1990'ların başında Teknik Çalışma Grupları (TWG'ler - *Technical Working Groups*) oluşturuldu. Daha sonra 1999'da ABD Adalet Bakanlığı tarafından desteklenen benzer şekilde görevlendirilmiş diğer gruplardan ayrılması amacıyla, TWG'lerin

isimleri Bilimsel Çalışma Grupları (SWG'ler - *Scientific Working Groups*) olarak değiştirildi (Whitcomb, 2002).

Birleşik Krallıkta oluşan ve devam eden farkındalık, kolluk kuvvetlerini ve uzmanları adli bilişime yönelik standart teknikler, protokoller ve prosedürler oluşturmanın gerekliliği konusunda harekete geçirdi. 1998 yılında İngiltere'de Baş Polis Memurları Birliği (ACPO - *Association of Chief Police Officers*), "Dijital Kanıtlar İçin İyi Uygulama Kılavuzu"nun ilk versiyonunu üretti. (ACPO yönergeleri, İngiltere'deki kolluk kuvvetleri için adli bilişim konusunda geçerli ana ilkeleri detaylandırmaktadır. Adli bilişim bilimi olgunlaştıkça bu kılavuz ilkeler ve en iyi uygulamalar yavaşça standartlara dönüşmüştür) (The Open University, Scotland, 2021).

Aynı durum Amerika'da da söz konusuydu. Özellikle FBI'ın öncülük ettiği çok sayıda konferans, adli bilişimle ilgili standartlar ve prosedürler hazırlama konusunda zemin oluşturdu. 1993 yılında 26 ülkeden temsilcilerin katılımıyla başlatılan ve her yıl farklı bir ülkede devam eden konferanslar dizisi (Uluslararası Bilgisayar Kanıtı Konferansı) (Pollitt, 2010, s:7) sonucunda Bilgisayar Kanıtı Hakkında Uluslararası Organizasyon (IOCE - *International Organization on Computer Evidence*) kuruldu (Whitcomb, 2002).

Washington DC'deki federal suç laboratuvarı müdürlerinin, karşılıklı ilgi alanlarını tartışmak için yılda iki kez bir araya geldikleri toplantılar sonucunda 1998'de Dijital Kanıt Bilimsel Çalışma Grubu (SWGDE - *Scientific Working Group on Digital Evidence*) ortaya çıktı (Whitcomb, 2002). Bilgisayarlardan elde edilen dijital deliller için en iyi uygulamalar üreten SWGDE, 1973'te kurulan ve o zamandan beri adli bilişimle ilgili olarak eğitimlerin, prosedürlerin ve en iyi uygulamaların geliştirilmesinde etkin olan Amerikan Suç Laboratuvarı Yöneticileri (ASCLD'ler - *American Society of Crime Laboratory Directors*) gibi başka kuruluşlarla da işbirliği yaptı (Parasram, 2017, s:274). ASCLD'ye bağlı olan Amerikan Suç Laboratuvar Yöneticileri Derneği - Laboratuvar Akreditasyon Kurulu

(ASCLD-LAB *The American Society of Crime Laboratory Directors/Laboratory Accreditation Board*) adli laboratuvarlar açısından belirli disiplinlerin karşılaması gereken kriterleri belirten bir akreditasyon sürecine sahiptir ve dijital delilleri bir laboratuvar disiplini olarak kabul etmiştir (Utica College, 2002, s:87).

ABD Savunma Bakanlığı bünyesinde, 1998 yılında "Savunma Siber Suç Merkezi (DC3 - *Department of Defense Cyber Crime Center*)" ve ona bağlı olarak "Savunma Adli Bilişim Laboratuvarı (DCFL - *Defense Computer Forensic Laboratory*)" kuruldu. DCFL daha sonra Siber Adli Bilişim Laboratuvarı (CFL - *Cyber Forensics Laboratory*) olarak yeniden adlandırıldı (Specht, 2020). Yine 1998 yılında, AFOSI, İşletim Yeri - Savunma Adli Bilişim Laboratuvarı'nı (OL-DCFL - *Operating Location – Defense Computer Forensics Laboratory*) kurdu (DoD DC3), 2019) 1999'da ise FBI'ın öncülüğünde, federal, eyalet ve yerel kanun uygulayıcı kurumlar arasında işbirliği oluşturmak gayesiyle ilk Bölgesel Adli Bilişim Laboratuvarı (RCFL - *Regional Computer Forensics Laboratory*) San Diego'da kuruldu. (Hayes, 2014; RCFL, 2021). 1999'un sonlarında IOCE, G-8 Yüksek Teknoloji Suçları Alt Komitesi (*High Tech Crime Subcommittee*) ve SWGDE adli bilişim ilkelerini yayınladı (IOCE, 2000).

Adli bilişim hakkında ilk kitap, SWGDE tarafından 2002 yılında, "Adli Bilişim için En İyi Uygulamalar" adıyla yayınlandı. Yine aynı yıl FBI tarafından, "siber temelli terörizm, internet üzerinden gerçekleştirilen düşmanca yabancı istihbarat operasyonları ve siber suçla en yüksek düzeyde teknik yeterlilik ve araştırma uzmanlığı uygulayarak mücadele etmek" için Siber Bölümü kuruldu (Farnan, 2003 ve FBI, 2016).

Adli bilişimin temelini oluşturan kuralları ve prosedürleri ortaya çıkaran kuruluşların tarihsel zemini elbette yukarıda anlatılanlarla sınırlı değildir. En iyi uygulamaları, standardizasyon, akreditasyon ve sertifikasyonları yaratan kuruluşların ortaya çıkış nedenleri ve süreçleri hakkında giriş niteliğinde olan bu bilgiler, bu tez çalışmasının çizdiği sınırları aşmamak adına sınırlı ve kısa tutulmuştur. Tezin

ilerleyen bölümlerinde anlatılacak hususlarla ilgili aşinalık oluşturmak amacıyla hazırlanan bu ön girişten sonra, adli bilişimle ilgili yapılan ilk model çalışmalarına geçmeden önce, öncelikle dijital delil kavramından ve Adli Bilişim dallarından bahsetmekte yarar vardır. Çünkü adli bilişim aşamalarının tümü aslında mahkemeye sunulacak dijital delillerin bulunması, toplanması, analizi ve sunulması noktasında düğümlenmekte, tüm çalışmalar bu sonuca ulaşmak için var olmaktadır. Dijital delilin olmadığı bir olay yerinde ne bir suç ne de bir araştırma söz konusu olacaktır ve dijital delillerin bulunduğu yerlere göre Adli Bilişim dalları ve uygulanan prosedürler de farklılık gösterecektir.

1.2. Dijital Delil

Elektronik cihazların ve internetin bu kadar yaygın olmadığı ve yapabileceklerinin henüz yeterince algılanamadığı yıllarda, ülkelerin Ceza Kanunlarına giren suç konusu fiiller için fiziki olarak bir ortamda bulunma zorunluluğu olduğu gibi, eylemlerin kanunlardaki tanımlarına göre suç oluşturabilmeleri için de belli fiziki hareketlerin yapılmış olması gerekiyordu. Oysaki günümüzde hırsızlıktan, dolandırıcılığa, sahtecilikten adam öldürmeye kadar birçok faaliyetin yeni şekillere büründüğüne tanık oluyoruz. Örneğin; bir kalp pilinin hacklenmesi neticesinde bir insanı öldürmek mümkün. Haliyle artık elde edilen deliller de suçun biçimiyle birlikte değişikliğe uğramış durumda. İlk sıralarda sadece bilgisayarlardan elde edilen bu deliller şimdilerde bilgi işleme özelliğine sahip olan ve üzerinde depolama üniteleri bulunan hemen her cihazda bulunduğu için adına "Dijital Delil" (Elektronik Delil/Sayısal Delil) denilmektedir.

Bir elektronik cihaz veya bilişim sistemi üzerinde yapılan bir işlem neticesinde sisteme girilen ham veriler belirli süreçlerden geçerek verinin anlam kazanmış biçimi olan bilgiye evrilmekte (5651 sk. 2007, md.2) ve bu bilgi adli bilişim araştırmaları sonunda çeşitli teknik donanım ve yazılımlar kullanılarak bir ispat vasıtası olan dijital delillere dönüşmektedir (Volonino ve ark., 2006). Bu deliller yapısı itibari ile

son derece hassas veriler olup, kolayca yok olabilme veya değişebilme özellikleri bulunmaktadır. İlk bakışta görülememeleri nedeniyle de ancak işin uzmanları tarafından bulunabilmekte ve yalnızca özel yazılımlar ile analiz edilebilmektedir. Dijital delillerin farklı uzmanlar tarafından bağımsız ve aynı adımlar takip edilerek incelenebilmesi, bu delillerin uygun teknikler ve ekipmanlar kullanılarak orijinaliyle tamamen aynı şekilde kopyalanabilmesiyle mümkündür (COE, 2017).

Dijital deliller, elektronik biçimde saklanan veya iletilen her türlü bilgi niteliğinde olduğu için, suç konusu bir olay neticesinde mahkemeye sunulduklarında mahkeme, bu delillerin dava konusu olayla ilgilisini, gerçek, orijinal ve kabul edilebilir olup olmadığını tespit edip/ettirip yargılamayı sürdürmektedir. Delillerin olmadığı hiçbir durumda maddi gerçeğe ulaşmak mümkün olamayacağından, suçun ispatı da söz konusu olamayacaktır. Dijital delil kavramı her ne kadar adli bilimler bazında aşina olunan fiziki deliller gibi olmasa da, elektronik aygıtların doğasından kaynaklanan maddi anlamda elle tutulamama özelliğine rağmen bilişim suçlarının ispatı açısından olmazsa olmaz araçlardır. Bu anlamda, bilişim sistemlerinden elde edilen verilerin insanlar tarafından algılanabilmesi, hukukun elde edilen dijital delilleri anlamlandırabilmesi, nihayetinde mahkemece niteliğine uygun şekilde değerlendirilebilmesi için bilgisayar bilimleri ile hukuk birleşerek Adli Bilişim bilimini bu önem ve ihtiyaç doğrultusunda ortaya çıkarmıştır.

Maddi gerçeğe ulaşma amacı güden ceza yargılamasında delil serbestisi ve vicdani delil sistemi bulunmaktadır (Akyürek, 2012, s:61; Centel ve Zafer, 2015, s:219). T.C. Anayasasının 38.maddesi; "Kanuna aykırı elde edilen bulgular delil olarak kabul edilemez" demek suretiyle hukuka uygunluk şartını açıkça belirtmiştir. Ceza Muhakemesi Kanunu'nun 217. Maddesine göre ise; "Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir. Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." şeklindeki düzenlemeyle ise takdir yetkisi kuralı kabul edilmiştir. Bu düzenlemelerde dikkat çeken husus, maddi gerçek için gerekli olduğı düşünülen her şey delil olarak sunulabilse de, sunulan her şeyin delil olarak kabul edilmeyebileceğidir. Maddelerde de açıkça belirtildiği gibi,

ancak hukuka uygun şekilde elde edilmiş ve değiştirilmemiş olduğu ispat edilmiş veriler, delil olarak kabul edilebilir ve hâkimler, bu deliller üzerinden vicdani kanaatlerine göre değerlendirme yaparak hüküm kurabilir.

Dijital delillerin, yasal bir süreçte mahkemede kabul edilebilir olması için bazı özelliklere sahip olması zorunludur. Bu özellikler kısaca şu şekildedir: (COE, 2014 ve Henkoğlu, 2014, s:6).

- Hatasız ve doğru olmalıdır (*accurate*): kanıtların toplanması ve analizi sırasında yapılan işlemler hatasız gerçekleştirilmeli;
- Kabul edilebilir olmalıdır (*admisable*): mahkemeler açısından delil olabilecek nitelikte olmalı, mevzuata ve en iyi uygulmalara uygun olarak elde edilmiş olmalı; suç şüphesi dahilindeki olayı açıklayıcı özellikte olmalı; maddi gerçeği rasyonel ve mantık kuralları dahilinde yansıtmalı;
- Gerçek olmalıdır (*authentic*): kanıtlar, gerçeklere itiraz edilemeyecek ve asıl durumunu anlatacak özellikte olmalı, suçu işleyen fail ile meydana gelen netice arasında illiyet (nedensellik bağı) olmalı;
- Eksiksiz ve tam olmalıdır (*complete*): sanık/şüpheli ile ilgili suçluluğunu ve suçsuzluğunu gösteren tüm deliller eksiksiz toplanmalı, toplanan bu delillerin delil bütünlüğü bozulmamış olmalı;
- İnandırıcı olmalıdır (*convincing*): delil olarak sunulan tüm bulgular herkesin inanacağı ve anlayacağı özellikte olmalı;
- Güvenilir olmalıdır (*reliability*): adli bilişim süreçlerinde izlenen yol ve uygulanan yöntemler kurallara ve prosedürlere uygun olmalı, delilleri toplama ve analiz işlemleri konusunda şüphe uyandırıcı hiçbir şey olmamalı, delillerin güvenirliğine gölge düşmemeli;
- Tekrar edilebilir olmalıdır: araştırmayı yapanlar dışındaki kişiler, farklı zamanlarda aynı yöntemleri uygulayarak aynı sonuçlara ulaşabilmeli;
- Mevcut yasal düzenlemelere uygun olmalıdır: takip edilen tüm süreçler ve uygulanan her işlem hukuka ve kanunlara uygun şekilde yürütülmeli;

- Orantılı olmalıdır (*proportionality*): kanıt toplamak için kullanılan yöntemler adil ve adaletin menfaatleri ile orantılı olmalı; herhangi bir tarafın hakları kanıtın "ölçülü değerinden" ağır basmamalıdır.

Adli bilişim süreçlerinden elde edilen verilerin yukarıdaki özellikler dikkate alındığında delil olarak kabul edilmemesinin ise bazı sebepleri bulunmaktadır (Hosmer, 2002). Şöyle ki; dijital deliller, değiştirilmesi, yenisinin oluşturulması ve silinmesi kolay bilgiler oldukları için bütünlükleri rahatça bozulabilmektedir. İlgili verilerin şüpheli kişiyle birlikte yakalanması hallerinde dahi, aynısının oluşturulma kolaylığı çoğu zaman şüphelinin, bu verilerin polis tarafından oluşturulduğu/yerleştirildiği iddiasını gündeme getirebilmektedir. Bu sebeple, bu delillerin doğruluğunun ve şüpheli kişiye aidiyetinin ispatlanması gerekmektedir. Delillerin elde edildiği bilişim sisteminin, ele geçirilme zamanının, yapılan işlemlerin ve şüpheliyle ilgisinin sonradan inkar edilemeyecek şekilde tespiti, ispatlanma hususunda kolaylık sağlamaktadır. Bu bağlamda, dijital deliller elde edildikten sonra üçüncü bir şahsın bu delilleri inceleyebilmesi ise, deliller için gereken doğruluk ve şeffaflık zorunluluğunu sağlayarak, bu delillerin mahkemede kabul edilebilmesine dayanak oluşturmaktadır (Hosmer, 2002).

Dijital delillerin bu özellikleri tüm bilişim sistemleri açısından geçerli olan ortak hususlar olmakla birlikte, bu delillerin nitelikleri, bulundukları bilişim sistemleri ve elektronik cihazlar açısından farklılık gösterebilmektedir. Sistemlerin ve cihazların teknik özellikleri dijital delillerin niteliklerini farklılaştırırken adli bilişimin de alt dallara ayrılmasına yol açmaktadır. Delilleri arayan, analiz eden ve yorumlayan uzmanların ilgili dallara uygun olarak uzmanlaşması bu sebeplerle önem arz etmektedir.

1.2.1. Dijital Delillerin Bulunduğu Yerler

Bilişim suçlarının en yaygın görüldüğü sistemler en çok bilgisayarlar ve cep telefonları olsa da, çok sayıda elektronik cihaz da artık bu suçlardan nasibini almakta ve birçok dijital delili bünyesinde barındırmaktadır. Teknolojinin hızı neticesinde, nesnelerin interneti geliştikçe ve yapay zeka teknolojisi basamak atladıkça diğer birçok cihaz da bu gelişmelerle birlikte delil sağlama potansiyeli kazanmaktadır. Mevcut durum açısından dijital delillerin elde edilebileceği başlıca alanlar şunlardır (Henkoğlu, 2014, s:6):

- Veri depolama üniteleri (flash bellek, sabit disk, floppy disk, optik disk…);
- DVD, HD DVD, CD, Blu-ray Media'lar;
- Yazıcılar, Tarayıcılar, Fax ve Fotokopi Makineleri;
- Taşınabilir player'lar (MP3 Player, Ipod, Zune…);
- Cep telefonları, Kişisel asistanlar (PDA), Çağrı cihazları;
- Ses kaydedici ve Medya oynatıcı cihazlar;
- Kameralar, Fotoğraf makineleri;
- Hafıza kartları, Smart kartlar, USB'ler ;
- Sabit sürücü çoğaltıcılar;
- Telesekreterler;
- GPS'ler;
- Kredi kartlarını kopyalayan, çoğaltan ve basan cihazlar (Card Skimmer);
- Cep telefonlarını klonlayan cihazlar;

Kullanılan elektronik sistemler suça konu olduğunda, adli bilişim de sistemin özelliğine göre bölümlere ayrılmakta ve her biri için farklı prosedürler ve sisteme özgü programlar söz konusu olabilmektedir. Akıllı telefonlar, tabletler, avuç içi bilgisayarlar, akıllı tv'ler, vb. dijital ekipmanların artan işlem yetenekleri, siber suçlarda kullanım olasılığına göre adli bilişimi aşağıdaki dallara ayırmaktadır:

- Bilgisayar Adli Bilişimi
- Mobil Adli Bilişimi
- Medya Adli Bilişimi
- Disk Adli Bilişimi
- Ağ Adli Bilişimi
- Kablosuz Adli Bilişim
- Veritabanı Adli Bilişimi
- Kötü Amaçlı Yazılım Adli Bilişimi
- E-posta Adli Bilişimi
- Bellek Adli Bilişimi
- Yazılım Adli Bilişimi
- Canlı Adli Bilişim
- Bulut Adli Bilişim
- Nesnelerin İnterneti (IoT) Adli Bilişimi

➢ **Bilgisayar Adli Bilişimi** (*Computer Forensics*) :

Bilişim suçu işlemede en çok kullanılan araç olup, adli bilişimin çıkış sebebi olduğu söylenebilir. Bilgisayarlar, dizüstü bilgisayarlar, depolama aygıtları ve diğer elektronik cihazlarda saklanan dijital kanıtların bulunmasını ve analizini içerir.

➢ **Mobil Adli Bilişimi** (*Mobile Phone Forensics*) :

Suç mahallinde bulunan en yaygın ve en yararlı dijital kanıttır. Cep telefonu sadece iletişim için değil ayrıca resimler, sohbetler, belgeler, iletişim bilgileri ve ağ bilgileri vb. gibi önemli bilgileri de saklar. İlk ortaya çıkışından günümüze kadar büyük yapısal ve teknik değişikliklere uğrayan mobil cihazlar artık haberleşme özelliği olan birer küçük bilgisayar işlevi görmektedir.

- **Medya Adli Bilişimi** (*Media Forensics*) :

Soruşturma sürecinde ses, video ve görüntü kanıtlarının tanımlanmasını, toplanmasını, analizini ve sunumunu içerir. Bir kaydın orijinal olup olmadığı ve kötü amaçlı veya yanlışlıkla tahrif edilip edilmediği konusunda özgünlüğün oluşturulması amacıyla, görüntü dosyasının meta verilerini kurtararak özgünlüklerini doğrulamak için dijital olarak elde edilen fotoğrafik görüntülerin çıkarılması ve analizi, ses ve video kayıtlarının toplanması, analizi ve değerlendirilmesi işlemleridir.

- **Disk Adli Bilişimi** (*Disk Forensics*) :

Etkin, değiştirilmiş veya silinmiş dosyaları arayarak depolama ortamından veri ayıklama ile ilgilenir. Sabit disk, USB cihazları, Firewire cihazları, CD, DVD, Flash sürücüler, Disketler gibi dijital depolama ortamlarından çıkarma bilimidir.

- **Ağ Adli Bilişimi** (*Network Forensics*) :

Bir bilişim sisteminde veya ağda yetkisi olmayan bir kişi tarafından gerçekleştirilen izinsiz girişi tespit etmek için bilgisayar ağ trafiğini izlemeye ve analiz etmeye odaklanır. Ağ trafiği Yerel Alan Ağı (LAN) veya Geniş Alan Ağı (WAN) olabilir. Saldırıların, anormal ağ trafiğinin ve güvenlik ihlallerinin kaynağını keşfetmek için ağ etkinliklerinin veya olaylarının izlenmesi, yakalanması, depolanması ve analizini içerir.

- **Kablosuz Adli Bilişim** (*Wireless Forensics*) :

Kablosuz ağ trafiğinden veri toplamak ve analiz etmek için gereken araçları sunmakla ilgilenir. Hassas ve özel bilgileri çalma, gözetleme veya sahtekarlık yapma olaylarında, yakalanan saldırı verilerini inceler. Kablosuz teknolojiler genel olarak Kablosuz Yerel Alan Ağları (WLAN'lar), Kablosuz Kişisel Alan Ağları (WPAN'lar) ve Kablosuz Geniş Alan Ağları (WWAN'lar) olarak sınıflandırılır ve her teknolojinin çalışma mesafesine göre belirlenir.

- **Veritabanı Adli Bilişimi** (*Database, Log Forensics*) :

Veri tabanlarının ve ilgili meta verilerin araştırılması ve incelenmesi ile ilgilidir. Veri tabanı kullanıcısının eylemlerini araştırmak, doğrulamak, uçucu verilerin bulunduğu RAM incelemesi ve zaman damgalarının araştırılmasını içerir.

- **Kötü Amaçlı Yazılım Adli Bilişimi** (*Malware Forensics*) :

Virüs veya solucan gibi birçok kötü amaçlı yazılımı incelemek için kötü amaçlı kodun araştırılması ve analiz edilmesidir. Davranışsal kötü amaçlı yazılım analizi (dosya, kayıt, ağ ve bağlantı noktası izleme gibi) ve statik kod analizi (dosya tanımlama ve profil oluşturma, dizelerin keşfi, zırhlama / paketleme algılama, sökme, hata ayıklama gibi) yürütme araçları ve teknikleri hakkında derinlemesine bilgi sağlar (Aquilina ve ark., 2008).

- **E-posta Adli Bilişimi** (*Email Forensics*) :

Silinmiş e-postalar, takvimler ve kişiler dahil olmak üzere e-postaların kurtarılması ve analizi ile ilgilenir. E-postaların, özellikle mesaj aktarım yolları, ekli dosyalar ve belgeler, sunucuların ve bilgisayarların IP adresleri vb. hususların derinlemesine ve sistematik olarak incelenmesini içerir.

- **Bellek Adli Bilişimi** (*Memory Forensics*) :

Sistem belleğinden (sistem kayıtları, önbellek, RAM) ham biçimde veri toplanması ve ardından ham dökümünden veri işlemesi ile ilgilenir. Verilerin bilgisayarın sabit diskinde bırakılmasını önlemek için gizli olan gelişmiş bilgisayar saldırılarının araştırılmasıdır.

- **Yazılım Adli Bilişimi** (*Software Forensics*) :

Sadece yazılımlarla ilgili bir suçun araştırılması sırasında dijital delillerin tanımlanmasını, toplanmasını, analizini ve sunumunu içerir. Özellikle patent ihlali veya hırsızlığı içeren durumlarda bilgisayar yazılımı metin kodlarını ve ikili kodları araştıran bir bilim dalıdır.

- **Canlı Adli Bilişim** (*Live Forensics*) :

Canlı bir senaryo ile ilgili vakaların incelenmesi ve analizi ile ilgilenen adli bilişim dalıdır; yani açık konumdaki bir sistem üzerinde analiz yapma işlemidir ve bu, herhangi bir değişiklik ve kayıp olmadan kanıtların orijinalliğini korumaya yardımcı olur.

- **Bulut Adli Bilişim** (*Cloud Forensics*) :

Kanıtlar, ele geçirebilecekleri bir cihazda olmak yerine, büyük olasılıkla coğrafi olarak kolayca erişilemeyen bir servis sağlayıcıdaki veri merkezinde bulunur. Geniş ağ erişimine dayanması ile sistemlerin ve cihazların bu ağlara bağlı olması, bulut adli bilişimi, ağ adli bilişiminin bir alt disiplini olarak kabul etmeyi sağlamaktadır (DFRWS, 2001).

- **Nesnelerin İnterneti Adli Bilişimi** (*IoT Forensics*) :

IoT ile ilgili siber suçlarla ilgilenen bağlı cihazların, sensörlerin ve olası tüm platformlarda depolanan verilerin araştırılmasını içeren bir adli bilişim dalıdır. IoT cihazları çok yönlü ve çok çeşitli özellikte olup, "nesneler" herhangi bir elektronik cihaz veya dosya sistemi olabileceği için ve veriler bulut bilişimdeki gibi uzak bir yerde depolanıp işleneceği için hem ağ adli bilişimi hem de bulut adli bilişimi ile ilişkili olan bir tür olup, akıllı cihazın yapısına bağlı bir soruşturma yöntemi izlenmektedir (Mrdovic, 2021, s:218).

Dijital deliller hangi bilişim sisteminde bulunursa bulunsun, atılacak adımların ve izlenecek prosedürlerin artık belli bir sisteme oturtulduğu söylenebilir ancak hala birtakım eksikler ile hatalar söz konusudur. Gelişen teknoloji her seferinde öncekinden farklı ve yeni özellikli pek çok elektronik cihazın üretimine vesile olmuştur ve bu gelişimin şimdikilerle sınırlı kalmayarak daha da farklılaşacağı ve çeşitleneceği ortadadır. Ülkelerin bu durum karşısında ortak bir sistem benimseme çabaları birkaç yıldır devam etmekte ve en iyi uygulamalar, laboratuvar akreditasyonları, personel eğitim sertifikaları ve standartlaşma faaliyetleri şeklinde kendini göstermektedir. Hukuki düzenlemelerde ise uluslararası sözleşmelere uyumlaştırılan yerel kanunlarla, sınırsız nitelikli bilişim suçları için ortak soruşturma ve kovuşturma kuralları oluşturulmaya çalışılmıştır.

Adli bilişim için öngörülen bu sistemleşme ve standartlaşma faaliyetleri en iyi uygulamalar ve prosedürlerle desteklenmeye çalışılırken, temelini adli bilimlerdeki standart prosedürden almaktadır. Nasıl ki ceza yargılamasına konu olan fiziksel bir suç incelemesinde aşamaların sıralaması "olay yeri araştırması, delil toplama, delillerin korunması ve taşınması, laboratuvar ortamında analizi, raporlama, adli makamlara sunum" şeklinde ilerliyorsa, adli bilişim için de aynı sıralama üzerinden hareket edilmiştir. Fiziki deliller ile dijital deliller arasında yapısal anlamda çok sayıda farklılık olması sebebiyle, adli bilişim süreçleri ihtiyaçlar doğrultusunda evrimleşmiş, konuyla ilgilenen araştırmacı ve uzmanlar tarafından geliştirilmiştir. Bu kapsamda gerçekleştirilen bu çalışmalar birbiri ile benzer ve farklı noktalar barındıran birçok modelin üretilmesine sebep olmuştur. Bir sonraki bölümde bu modellerden birkaçı açıklanarak adli bilişim biliminin gelişme süreci adım adım takip edilecektir.

2. GEREÇ VE YÖNTEM

Adli Bilişimin hukuki ve teknik kurallara bağlı bir bilim dalı haline gelmesinde modeller, en iyi uygulamalar, standardizasyon, akreditasyon ve sertifikasyonlar ile harmanlanan yasal mevzuatlar ve yargılama prosedürleri, bu tez çalışmasının ana temasını oluşturmakla birlikte, yapılacak sonraki çalışmalar için de bir çerçeve çizme amacı taşımaktadır. Bu sebeple öncelikli olarak bahsi geçen bu konular izlenecek yol haritası için bir dayanak oluşturacaktır.

2.1. Adli Bilişim Süreçlerine Yönelik Modeller

Bilgisayar suçlarının ilk ortaya çıktığı zamanlarda, tüm araştırma sürecini tutarlı ve standart hale getirecek bir süreç modeli tanımlamak öncelikliydi. Suçların ve hedef aldıkları ya da aracı olarak kullandıkları elektronik sistemlerin yapısal farklılıkları düşünüldüğünde, yapılacak araştırmaları kusursuz şekilde gerçekleştirecek bir model bulmak neredeyse imkansızdır ancak yapılacak her işlem için en azından işe yarar bir genel çerçeve çizilmeye, işlemler bu çerçeve dahilinde kurallara uygun şekilde yürütülmeye çalışılmalıdır. İyi tanımlanmış bir çerçevenin, hızla gelişen ve çeşitlenen bu alana kolay uyum sağlamak ve yeni teknikleri benimsemek bakımından esnek ve kabiliyetli olması beklenmektedir (Xiaoyu Du ve ark., 2017).

Literatüre ve geçmiş çalışmalara bakıldığında birçok uzman tarafından çok sayıda model geliştirildiği görülmektedir. Temelini adli tıp standartlarından alan bu modeller pek çok ortak nokta barındırmakla birlikte, modeli geliştiren her uzmanın belirli kullanım durumları için kişisel gözlemleri ve yargıları dahilinde boşlukları doldurmaya ve diğer modellerde gördükleri eksiklerini tamamlama veya analizleri kolaylaştırma amacı güderek en iyi sistemi bulmaya odaklandığı anlaşılmaktadır.

Yapılan literatür araştırmaları sırasında, adli bilişimin gelişme sürecine en yüksek katkıları sağlayarak isim yapan, diğer uzmanların araştırmalarına kaynak olan ve görece diğer modellerden farklı hususları bünyesinde barındıran, tez çalışması dahilinde ortaya konacak "Öneri Model"in oluşturulmasında da faydalanılan modeller bu çalışmaya dahil edilmiş olup, ele alınacak modeller şunlardır:

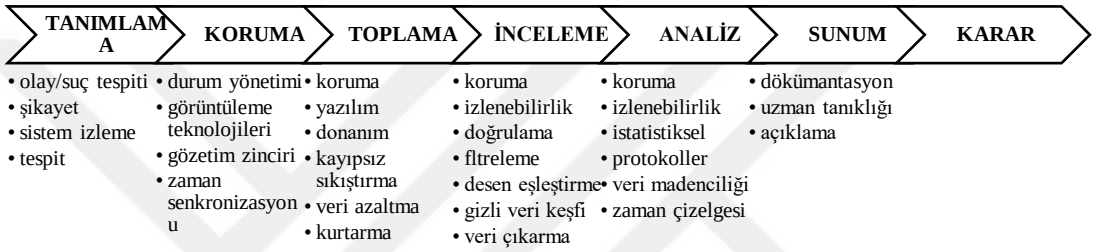
- Adli Bilişim Referans Modeli – RM (Dijital Adli Araştırma Çalıştayı - DFRWS)
- Olay Müdahale Süreci Modeli - IR
- Ortak Model – CM
- Soyut Adli Bilişim Modeli
- Entegre Dijital Araştırma Süreci – IDIP
- Gelişmiş Entegre Dijital Araştırma Süreci – EIDIP
- Genişletilmiş Siber Suç Araştırması Modeli
- Adli Bilişim Saha Triyaj Süreci Modeli - CFFTPM
- Malezya Araştırma Sürecine Dayalı Adli Bilişim Modeli
- Sistematik Adli Bilişim Araştırma Modeli
- Bulut Bilişime Yönelik Model
- Veri Madenciliği Modeli
- Nesnelerin İnterneti (IoT) Modeli

Bölümün sonraki kısmında yukarıda sıralanan modeller incelendikten sonra, tez kapsamında önerilen model açıklanacak ve bilinen modellerle karşılaştırılacaktır.

2.1.1. Adli Bilişim Referans Modeli – RM

Modellere ilişkin fikirlerin tohumlarının ilk olarak 2001 yılında, akademisyenlerin, adli bilişim uzmanlarının ve araştırmacıların katılımıyla New York'ta yapılan "Dijital Adli Araştırma Çalıştayı (DFRWS - *Digital Forensic Research Workshop*)"nda atıldığı söylenebilir. Bu çalıştayda olgunlaşan fikirler adli

bilişime yönelik modellerin oluşturulması noktasında referans olduğundan dolayı "Referans Model" olarak adlandırılması mümkündür. Dijital veriye yönelik değiştirme, silme gibi müdahaleleri tespit etmek için tasarlanan yöntemlerin önemi, delilerin müdahalelere karşı korunmasının güvence altına alınması, veri ve video sıkıştırma gibi birçok alanda güvenli bir temel oluşturmak için doğruluk standartları ihtiyacı, analiz edilen verilerin anlamlarını ve olayla bağlantılarını anlamak için yorumlama becerileri çalıştayın üzerinde durduğu temel konular olmuştur (DFRWS, 2001).



Şekil 2.1. DFRWS Süreci

Temelde, yedi basamaklı bir sistem öngörerek (Şekil 2.1.), gelecekteki dijital teknolojilere uygulanmasını sağlama amaçlı bir çerçeve çizilmektedir. Elektronik suçları ele alırken; eğitim, standartlar ve sertifikasyon, teknik destek, teknoloji geliştirme, politika ve yasal konularda hazırlanan programlar dahilinde ceza adaleti sağlamaya odaklanılması gerektiği belirtilmiştir (Palmer, 2001, s:12).

Çalıştaydan çıkan sonuç göstermiştir ki, en önemli zorluk, analitik prosedürler ve protokollerin standartlaştırılmaması, uygulayıcıların ve araştırmacıların standart terminoloji kullanmamasıdır. Standartlaştırılmış prosedürlerin, dijital kanıt toplamada bütünlüğü korumak ve aslına uygunluğu desteklemek için zorunlu olduğu, gerek laboratuvar akreditasyonunda, gerekse saha personelinin tam sertifikasyonunun sağlanmasında standartların, görev sınırını ve eksiksiz işlem kapasitesini belirlemede gerekli olduğu vurgulanmıştır.

Dijital delilin güvenilirliği ile gizli verilerin kurtarılması konularında, verilerin ilk elde edildiği andan itibaren değişmeden kalması ve verilerin olayları doğru ve gerçekçi şekilde temsil edip etmediği konuları da üzerinde durulan meseleler olmuştur.

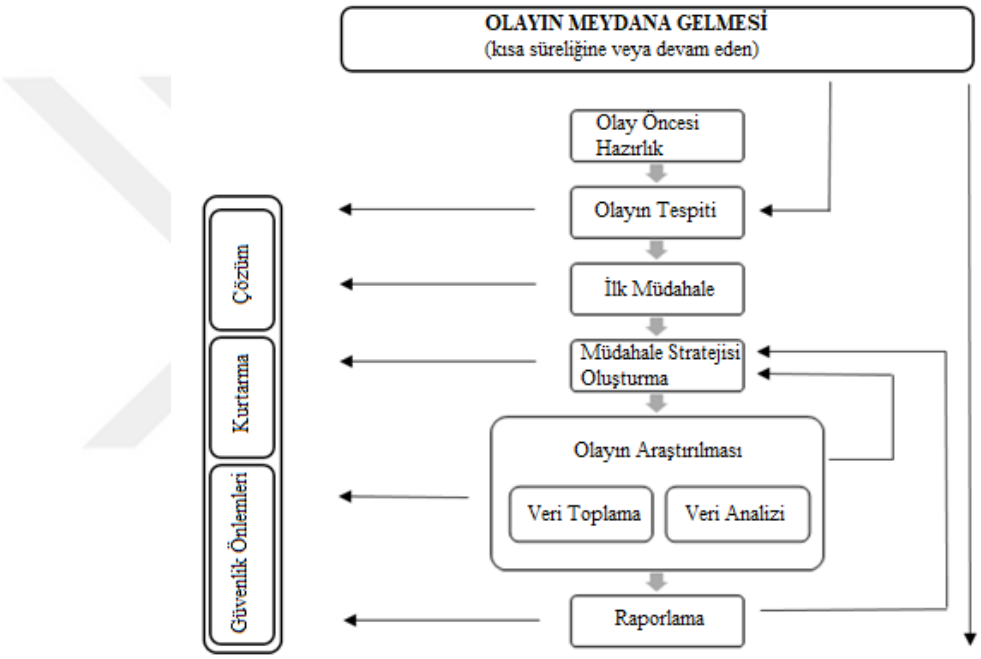
DFRW Çalıştayı adli bilişim alanında çalışma yapan uzmanların bu alandaki eksikliklere ve yanlışlara yönelik çözüm bulma hedefinde yol gösterici olmuştur. Hatta bazı yazarlar tarafından ayrı bir model olarak kabul edilmektedir. Sonraki süreçte konuyla ilgili her uzman bireysel veya grup halinde birçok model üreterek açığı kapatmaya çalışmıştır. Alanda büyük çoğunluğu birbiriyle ufak farklılıklar taşıyan çok sayıda model olmakla birlikte, bu tez çalışmasında daha önce de *belirtildiği* gibi, yalnızca en bilinen ve gelişime yön veren modellerden bahsedilmiş, ortak araştırma aşamaları bulunan modeller daha özet şekliyle açıklanmıştır.

2.1.2. Olay Müdahale Süreci Modeli - IR

2001 yılında özel ajanlar ve uzmanlar tarafından geliştirilen "Olay Müdahale Süreci Modeli (IR - *Incident Response Process Model*)", hemen her siber güvenlik ihlali için kullanılmak üzere aşağıdaki aşamalarla bir "olay müdahale metodolojisi"ni belirlemiştir (Şekil 2.2.) (Mandia ve ark., 2003, s:14 ve Carrier ve Spafford, 2003):

- **Olay Öncesi Hazırlık:** Bir olay meydana gelmeden önce, uygun altyapı ve gerekli eğitim ile hazırlanmak,
- **Olayın Tespiti:** Güvenlikle ilgili şüpheli bir durum belirlemek,
- **İlk Müdahale:** Olayın meydana geldiğini doğrulamak, temel ayrıntıları kaydetmek ve olay müdahale ekibini organize etmek,
- **Müdahale Stratejisinin Formüle Edilmesi:** Araştırma sonuçlarına dayalı olarak hukuki, idari, cezai vb işlemler için yanıt belirlemek,
- **Araştırma / Soruşturma Yapılması:** Kimin, neyi, nasıl ve ne zaman yaptığı ile nasıl önlenebileceği konularını belirlemek için kapsamlı araştırma yapmak,

- **Önlem Uygulamaları:** Sistemin yedeğini oluşturmak, sistemi orijinal durumuna geri yükleyerek kurtarmak, çevreyi kontrol altına almak, izolasyonu sağlamak, ağı gözlemleyerek saldırıları izlemek,
- **Raporlama:** Gerçekleştirilen adımları ve bulunan çözümleri karar vericilerin ve yargılama makamlarının anlayabileceği şekilde belgelemek,
- **Takip:** Güvenlik önlemlerini ve prosedür değişikliklerini uygulamak ve tespit edilen tüm sorunlar için uzun vadeli düzeltmeler geliştirmek.



Şekil 2.2. Olay Müdahalesinin Yedi Bileşeni (Mandia ve ark., 2003, s:15)

Model, bir bilgisayara, ağa veya canlı bir sisteme yönelik yasadışı eylemlere hazırlıksız yakalanmamak için, saldırıyı tespit etmeyi ve sistemi orijinal durumuna geri yükleyerek kurtarmayı hedeflemekte ve müdahale sürecinde teknik ve yasal olmak üzere farklı uzmanlıklara sahip kişilerin söz konusu olaylara verdiği yanıtlara odaklanmaktadır Amaç, araştırmacıların ve uzmanların süreci yürütürken daha az hata yapmasını sağlayacak bir sistem yapılandırmaya çalışmaktır (Freiling ve Schwittay, 2007).

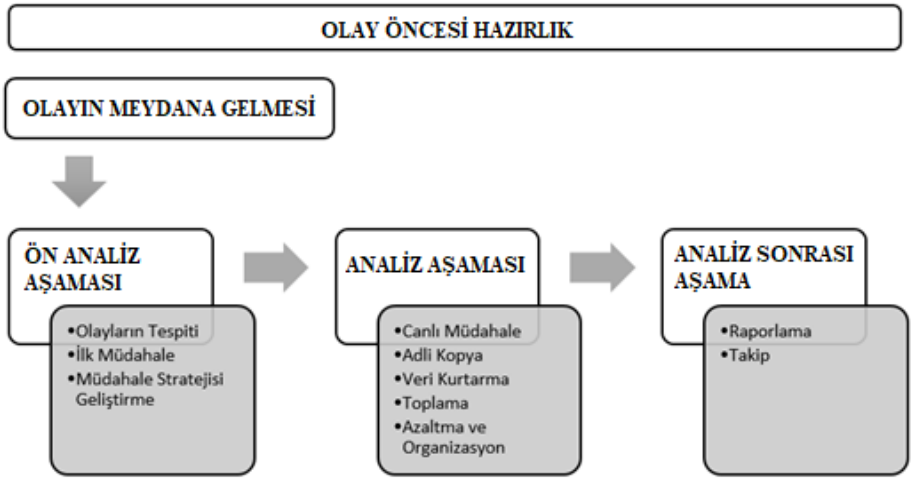
Olası suç faaliyetlerini bildiren bir suçlama veya ihbar alınması ile başlayan Adli bilişim (CF – *Computer Forensics*) sürecinde, olayın gerçekliğine ilişkin araştırma yapılarak dijital delilin ayrıntılı analizi ve dikkatli şekilde kullanılması konusunda bilimsel bir yaklaşım söz konusu iken, IR modelinde güvenlik yönetimi ve hızlı şekilde kontrol altına alma, soruşturmanın bir kuruluşun iş süreçlerine entegrasyonu ve hızlı dönüş hususları üzerine yoğunlaşılmıştır. Yönetim konuları içinde, kuruluşun itibarının korunması ile meydana gelen olayın vereceği hasarın hesaplanması üzerinde durulmaktadır. Aradaki temel farkı özetlemek gerekirse; adli bilişim kanıt toplamaya yönelirken, IP olayları tespit edip kontrol altına alma ile ilgilenmektedir (Freiling ve Schwittay, 2007). Ortak noktaları ise, her iki model de gerçekleşen çok sayıda farklı bilgisayar güvenliği olayını ve suç niteliğindeki eylemleri araştırmakta, öncelikleri ve hedefleri farklı olsa da bazı temel aşamaları paylaşmakta, hatta bunun için bazen aynı yöntemleri ve araçları kullanmaktadır (Schwittay, 2006).

Adli bilişim ile IP modeli arasındaki bu amaç ve yöntem farklılığı, benzerliklerinin de etkisiyle, bu iki modeli birleştiren başka bir modelin üretilmesini sağlamıştır: “Ortak Model”.

2.1.3. Ortak Model - CM

Adli bilişime bir yönetim yönü ve uygun yanıt stratejisi seçimi, Olay Müdahaleye ise, tam ölçekli bir adli analiz yapma seçeneği eklenerek harmanlanan Ortak Model (CM – *Common Model*), her biri birden fazla alt bölüme sahip temelde üç aşamaya ayrılmıştır (Freiling ve Schwittay, 2007):

- Ön analiz aşaması
- Analiz aşaması
- Analiz sonrası aşama



Şekil 2.3. Ortak Model (Freiling ve Schwittay, 2007)

Şekil 2.3.'de de görüleceği gibi, Ön Analiz Aşamasının üç adımı, IP modelindeki adımlarla benzerlik göstermekte, ancak son adım olan "Müdahale Stratejisinin Geliştirilmesi", IP'den farklılaşarak, tam ölçekli bir adli analizin yapılıp yapılmayacağına karar verilmesi gereken zamanı ifade etmektedir. Analiz aşamasında ise, canlı müdahale hariç, diğer adımlar adli bilişim sürecine eşdeğerdir. Analiz sonrası aşama adımları ise kendisini oluşturan modellerde yer alan aşina olduğumuz adımları oluşturur (Freiling ve Schwittay, 2007).

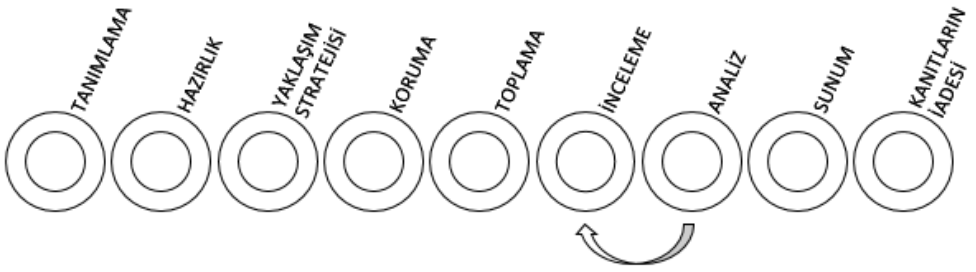
Freiling ve Schwittay Ortak Modeli, bir IP prosedürüne yerleştirilmiş bir adli bilişim soruşturmasına benzetmektedir. Gerçek analiz aşaması sırasında adli bilişim ilkelerini Olay Müdahale çerçevesine etkili bir şekilde entegre ederek, her iki modelin eksikliklerini gidermeyi hedeflenmişlerdir.

2.1.4. Soyut Adli Bilişim Modeli

2002 yılında, ABD Hava Kuvvetleri'ndeki araştırmacılar tarafından, çeşitli süreç modellerinin sahip olduğu ortak özellikler belirlenerek, FBI'ın standart fiziksel olay yeri arama protokolüne dayanan başka bir adli bilişim modeli önerilmiştir. "Soyut Adli Bilişim Modeli (*An Abstract Digital Forensics Model*)" adı verilen bu

modelin amacı, “adli bilişim alanında, tüm dijital suç mahalli araştırmalarının adli analizlerini kapsayan bir metodoloji geliştirerek, tutarlı ve standartlaştırılmış bir çerçeve sunmak; çerçeveyi gelecekteki dijital teknolojilere uygulamak için bir mekanizma yaratmak olarak tanımlandı ve DFRW modelinin iyileştirilmiş hali olarak düşünüldü. Bu modelde, tüm elektronik sistemlere uyarlanabilecek dokuz adım belirlenmiştir (Şekil 2.4.) (Reith ve ark., 2002, s:6):

Olayı ve suçu “**tanımlama**”; araçlara, tekniklere ve izinlere “**hazırlık**”; kanıt toplanmasının üst düzeye çıkarıldığı, mağdur zararının ise en aza indirildiği “**yaklaşım stratejisi**”; fiziksel ve dijital kanıtların “**korunma**”sı; kanıtları standartlara ve prosedürlere uygun olarak “**toplama**” ve derinlemesine “**inceleme**”; sonuç çıkarmak için “**analiz**” etme; sonuçların “**sunum**”u ve en son elde edilen tüm “**kanıtların iade**”si…



Şekil 2.4. Soyut Adli Bilişim Modeli Aşamaları

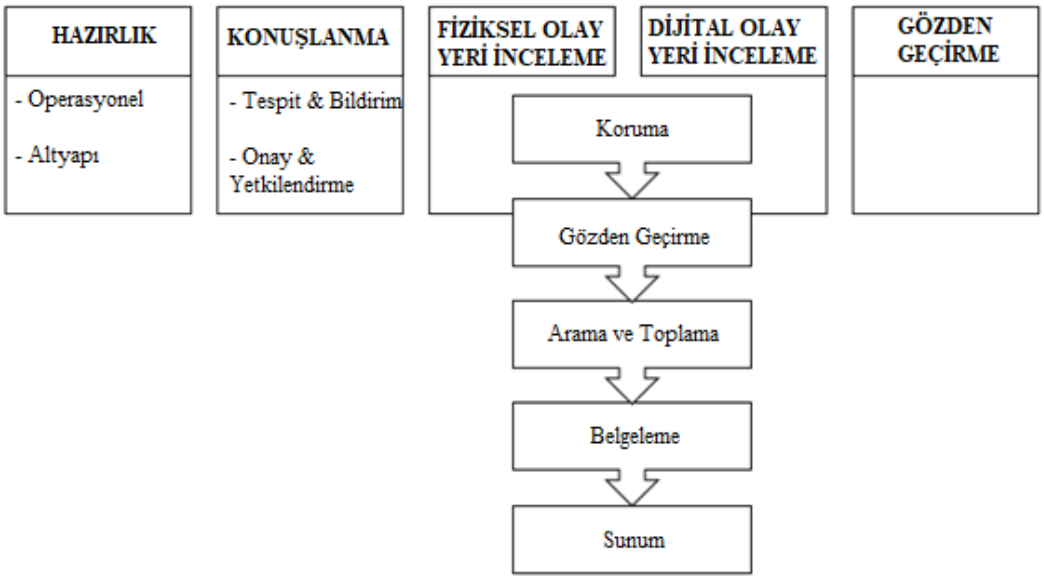
Görüldüğü gibi belirlenen adımlar klasik adli tıp prosedüründen çok da farklı değildir. Uzmanlar bunun gerekçesini, geleneksel adli tıp disiplinlerinde çok sayıda kanıtlanmış araştırma teknikleri ve yöntemlerinin bulunduğunu ve bunların siber uzayda uygulanmasının mümkün olduğunu fakat henüz güçlü şekilde değerlendirilmediğini belirtmişlerdir. Bu standart modelin, geçmiş, şimdiki veya gelecekteki dijital cihazlarla kullanmak için temel olması noktasında tutarlı bir metodolojiye izin verdiğini, bu modele teknolojik gelişmelerle birlikte uygun eklemeler yapılabileceğini de eklemişlerdir.

Geliştirilen her model belli bazı teknolojilere uyumlaştırılacak şekilde tasarlanmış olabilir oysaki bu model oluşturulurken, araştırma konusu olacak bilişim sistemini tam tanımlamadan uygulanabilecek bir model hedeflenmiş, bu esneklik, geçmiş, şimdiki ve gelecekteki elektronik cihazlarda da işe yarayacak şekilde oluşturulmaya çalışılmıştır. Bununla birlikte, modeli üreten kişiler, modelin pratik kullanım için fazla genel olduğu, herhangi bir alt kategori eklemenin ise hantallık yaratacağı ve bu modeli tecrübe edecek kolay bir yöntem olmadığı konusunda öz eleştiri yapmaktadırlar.

2.1.5. Entegre Dijital Araştırma Süreci – IDIP

2003 yılında Brian D. Carrier Eugene H. Spafford tarafından önerilen "Entegre Dijital Araştırma Süreci (IDIP - *Integrated Digital Investigation Process*)"de; dijital bir cihazın soruşturulmasını fiziksel suçlardaki olay yeri incelemesine benzeterek, bir bilgisayarın kendisinin suç mahalli niteliğinde olduğunu kabul etmiş ve fiziksel bir suç mahalli için uygulanan soruşturma yöntemleri dijital alana uyarlanmıştır. Bir bilgisayar için, ilk dijital olay yeri genellikle yerel işletim sistemi ve donanım tarafından oluşturulan sanal ortamdır (Carrier ve Spafford, 2003, s:6) ve bir olaya karışan her bilgisayar muhtemelen ayrı bir suç mahalli olacaktır.

Bu model hazırlanırken kendinden önceki modellere atıfta bulunarak eklemeler yapıldığı belirtilmiştir. Beş aşamadan oluşan (Şekil 2.5.) bu modelde hazırlık evresi diğer modellerle aynı hareketleri içermektedir. Konuşlanma aşaması olay yerini incelemek için gereken arama emri veya yasal onayın alındığı aşama olarak bu modelde bağımsız şekilde yer almıştır.



Şekil 2.5. Entegre Dijital Araştırma Süreci

Adli bilişim açısından dijital delilleri toplamak öncelikli olmakla birlikte, olay yerinde çok sayıda fiziki delil de yer almaya devam etmektedir. Fiziksel olay yeri araştırmalarında bilinen bir teori olan "Locard Değişim İlkesi" ne göre; "İki nesne temas ettiğinde, aralarında karşılıklı bir madde alışverişi gerçekleşecektir" (Miller, 2009, s:168). Bu demek oluyor ki, fiziki her türlü temas iz bıraktığından, dijital olay yeri araştırması yapılırken suçlunun DNA'sı gibi çok sayıda fiziksel delil toplanabilmektedir. Bu sebeple görülecektir ki geliştirilen modellerin birçoğu fiziksel ve dijital olay yeri ayrımına giderek, içerisinde ortak adımlar barındırmakla beraber, aşamalar delillerin yapısal özelliğine bağlı olarak kendi içinde farklılaşabilmektedir.

Venansius Baryamureeba ve Florence Tushabe'a göre IDIP modeli, dijital bir soruşturma gerektiren siber terörizm yeteneklerine uygundur çünkü olayların yeniden inşasını ve tüm görevi gözden geçirmeyi mümkün kılar (NIJ, 2002); bununla birlikte, olay yerleri arasında net bir ayrım yapılmadığından, bilgisayar suçlarını teyit etme ile, daha büyük ağlar ve özellikle İnternet (Kizza, 2003) ile uğraşırken geriye dönme sürecinin zor olabileceğini vurgularlar (Baryamureeba ve Tushabe, 2004, s:5).

2.1.6. Gelişmiş Entegre Dijital Araştırma Süreci - EIDIP

2004 yılında, Venansius Baryamureeba ve Florence Tushabe tarafından "Gelişmiş Entegre Dijital Araştırma Süreci (EIDIP - *Enhanced Integrated Digital Investigation Process*)" modeli önerilmiştir. EIDIP modeli temelini IDIP'den almaktadır ancak IDIP'deki iki kez yeniden yapılandırma zorunluluğu sorununu çözmek için geri izleme aşaması ve geri izleme aşamasında da birincil olay yerinin tanımlandığı yeni bir aşama bulunmaktadır (Şekil 2.6.) (Baryamureeba ve Tushabe, 2004, s:6):

Şekil 2.6. Gelişmiş Entegre Dijital Araştırma Süreci

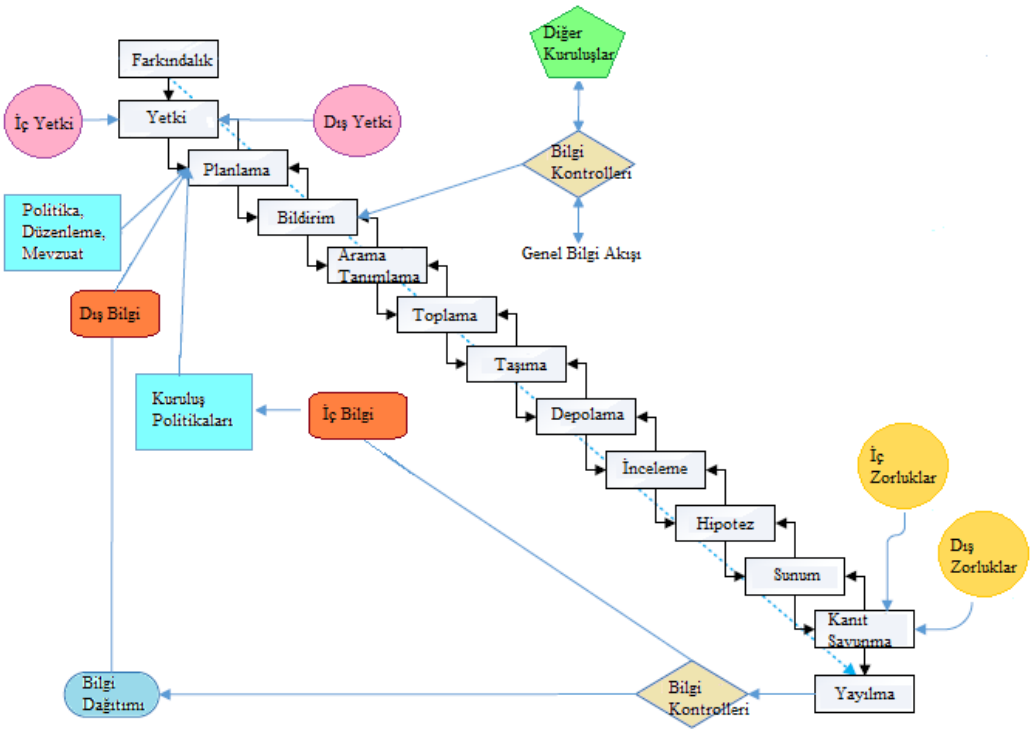
Burada bahsi geçen birincil ve ikincil olay yeri şeklinde yapılan bölünmelerde Kohn ile Eloff bu farklılığı şu şekilde tanımlamıştır: "Birincil olay yeri, suçun başlatıldığı yerdir; kötü niyetli faaliyetin hedefi olan ancak fiziksel veya dijital adli soruşturmanın bir parçası olmayan kurbanın konumu ise ikincil olay yeridir" (Kohn ve ark., 2013).

EIDIP, fiziksel ve dijital olay yeri inceleme süreçleri arasında net bir ayrım yapmakta, konuşlanma aşaması ile de onay ve yasal izin mekanizmasını işletmektedir. Geri İzleme/Kaynağını Bulma aşamasında, suçun icrasında kullanılan cihazları tanımlamak için fiziksel suç mahalli izlenmekte, Dinamit aşamasında, olay faillerini bulmak için birincil olay yerinde bulunan kanıt maddelerinin toplanması ve

analiz edilmesi amaçlanmaktadır. Yeniden Yapılandırma ise, gerekli tüm kanıtlar toplandığında yalnızca bir kez yapılmaktadır (Kohn ve ark., 2013).

2.1.7. Genişletilmiş Siber Suç Araştırması Modeli

Séamus Ciardhuain 2004 yılında diğer adli bilişim süreç modellerinde tespit ettiği eksiklikleri gidermek ve sadece kolluk kuvvetleri için değil, BT yöneticilerine, güvenlikçilere ve denetçilere de fayda sağlamak amaçlarıyla "Genişletilmiş Siber Suç Araştırması Modeli (*An Extended Model of Cybercrime Investigation*)"ni oluşturmuştur. Bu model şelale tarzını takip ederek gerekli faaliyetleri sırayla gerçekleştirilmekte ve yinelemeye izin vermektedir (Du ve ark., 2017).



Şekil 2.7. Genişletilmiş Siber Suç Araştırması Modeli (Ciardhuáin, 2004, s:21).

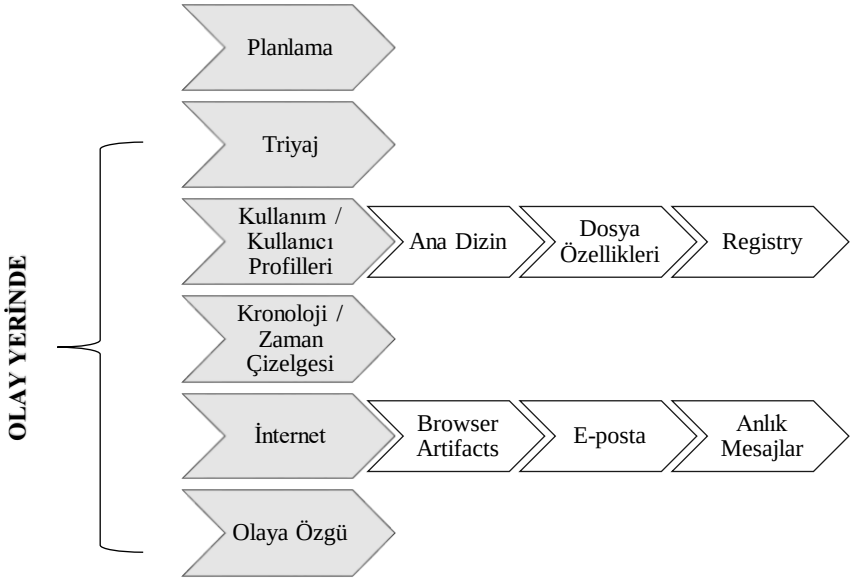
Ciardhuáin, mevcut modellerdeki en büyük eksikliklerin, araştırmalardaki bilgi akışlarını açıkça tanımlamamaları ve siber suç soruşturmasının tüm yönleri yerine,

araştırma sürecinin orta kısmı olan kanıtların toplanması ve incelenmesi üzerine yoğunlaşma eğiliminde olmaları olduğunu belirtmiştir. Bu sebeplerle, modeli; "mevcut modelleri birleştiren, genelleştiren ve bunlara dahil olmayan belirli etkinlikleri açık bir şekilde ele alarak genişleten bir araştırma modelidir. Önceki modellerden farklı olarak, bu model bir araştırmadaki bilgi akışlarını açık bir şekilde temsil eder ve yalnızca kanıtların işlenmesinden ziyade bir araştırmanın tüm kapsamını yakalar." şeklinde tanımlamıştır (Ciardhuáin, 2004, s:1).

Modelde açıkça görülen ve diğer modellerde bulunmayan "Farkındalık" bölümüdür (Şekil 2.7.). Soruşturmaya neden olan olaylar araştırma türünü ve işbirliklerini etkileyebilmektedir. Suçun bir makama bildirildiği durumlarda araştırmacıların izleyecekleri yola ilişkin fikrin oluştuğu aşama farkındalık aşamasıdır**.**

2.1.8. Adli Bilişim Saha Triyaj Süreci Modeli - CFFTPM

2006 yılında uzmanlar, "Adli Bilişim Saha Triyaj Süreci Modeli (CFFTPM - *Computer Forensics Field Triage Process Model*)**"** ni geliştirdiler. Bu model standart ilkelere bağlı olmakla birlikte, suçluyu kaçmadan önce yakalayabilmek için süreci hızlandırmak amacıyla, sistemleri laboratuvara götürmeden, dijital kanıtların sahada analiz edilmesi ve yorumlanması fikrine dayanmaktadır. Geleneksel modellerde sonuçların alınması haftalara, aylara hatta yıllara sarktığından dolayı, kayıp, istismar, pedofili ve çocuk kaçırma gibi olaylarda suçlular kaçabilmekte ve etkili bir müdahaleye geç kalınabilmektedir (Rogers ve ark., 2006, s:20). Bu sebeple olay yerindeki ilk triyaj tamamlandıktan sonra, bilişim sisteminin veya depolama ortamının daha kapsamlı bir inceleme ve analiz için bir laboratuvar ortamına götürülmesi prosedürü işlerliğini sürdürmektedir.



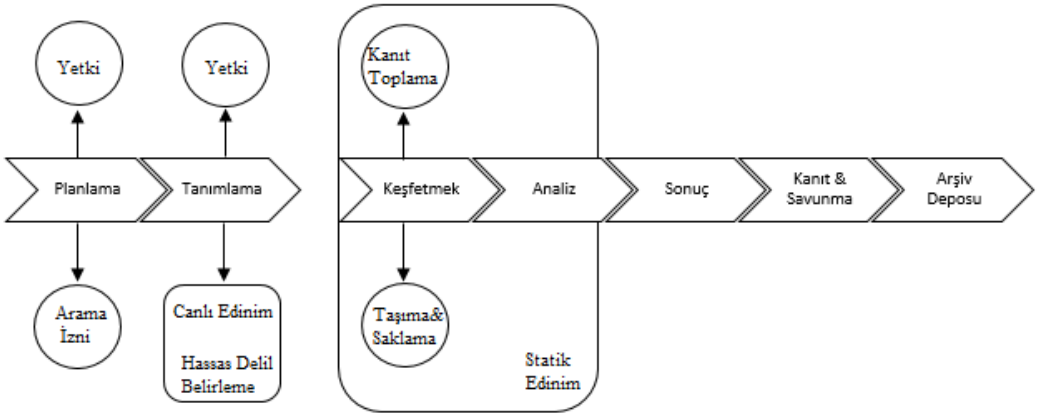
Şekil 2.8. Adli Bilişim Saha Triyaj Süreci Modeli

Model, kullanılabilir kanıtların bulunmasına, risk altındaki mağdurların belirlenmesine ve suçlunun topluma yönelik tehlikesinin doğru bir şekilde değerlendirilmesine odaklanır; aynı zamanda IDIP modeli ile Rogers'ın Dijital Suç Mahalli Analizi (DCSA - *Digital Crime Scene Analysis*) modelinden türetilen aşamaları kullanır.

Şekil 2.8.'de modelin aşamaları gösterilmiştir ve Triyaj aşamasını modelin uzmanları "Her şeyin önem veya öncelik açısından sıralandığı, en önemli veya en geçici olan verilerin ya da potansiyel kanıtların ilk önce ele alındığı, aynı zamanda da zaman kısıtlaması dahilinde yapılıp yapılamayacağının belirlendiği süreç" olarak tanımlamış ve tıbbi triyajdaki acil tedaviye ihtiyacı olanlara öncelik tanınması kuralının uygulanmasına dayandırmışlardır. Ayrıca modelin triyaj usulü bir model olmasının geleneksel laboratuvar analizi ve incelemesini engellemediğini vurgulamışlardır.

2.1.9. Malezya Araştırma Sürecine Dayalı Adli Bilişim Modeli

Sundresan Perumal tarafından 2009 yılında geliştirilen "Malezya Araştırma Sürecine Dayalı Adli Bilişim Modeli (*Digital Forensic Model Based On Malaysian Investigation Process*)"nin Malezya'da adli bilişime fazla önem verilmemesi sebebiyle oluşan boşluğu doldurma ihtiyacından doğduğu belirtilmiştir (Perumal, 2009, s:40).



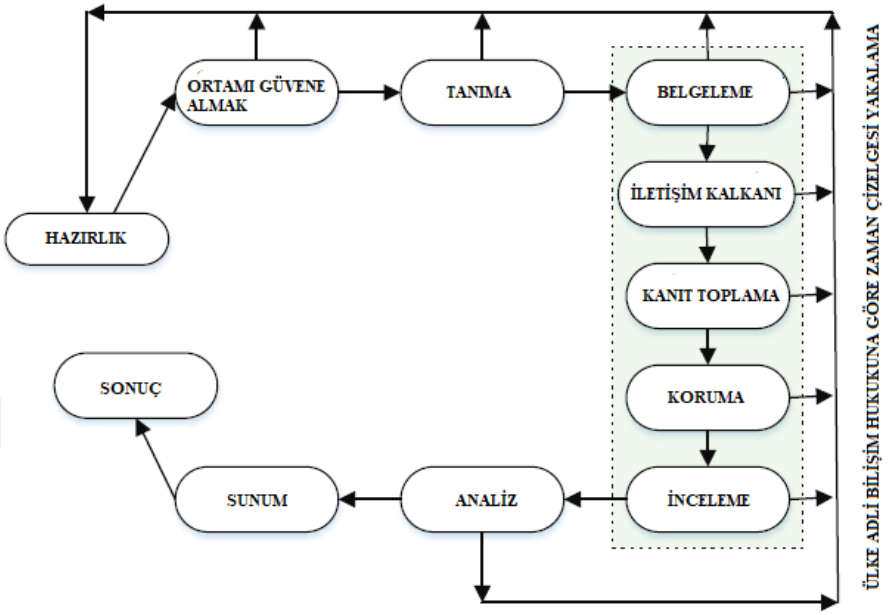
Şekil 2.9. Malezya Araştırma Sürecine Dayalı Adli Bilişim Modeli

Bu model, siber suç soruşturmasında canlı veri toplama ve statik veri toplama konusunda daha ayrıntılı işlemlere odaklanarak (Şekil 2.9.) (Du ve ark., 2017) hassas delillerin kurtarılmasında kovuşturma sürecinin daha başarılı sürdürülmesine vesile olmak amacını taşımaktadır. Arşiv depolama aşamaları da veri madenciliğine odaklanması bakımından diğer modellerden ayrılan bir özellik taşımaktadır.

2.1.10. Sistematik Adli Bilişim Araştırma Modeli

Agarwal ve arkadaşları 2011 yılında bilgisayar dolandırıcılığı ve siber suçlara odaklanan "Sistematik Adli Bilişim Araştırma Modeli (*The Systematic Digital Forensics Investigation Model*)"ini geliştirdiler (Du ve ark., 2017). Bu modelde diğerlerinden farklı olarak bağımsız bir "İletişim Kalkanı" aşaması bulunmaktadır. Cihazın kapalı konumda görünüp aslında çalışır durumda olduğu hallerde, kablosuz,

Bluetooth veya senkronizasyon gibi özelliklerin etkinleştirilmesi dijital delillerin bozulmasına sebebiyet verebileceği için, olası tüm iletişim bağlantılarının cihazla temasının engellenmesi fikrini vurgulamıştır.



Şekil 2.10. Sistematik Adli Bilişim Araştırma Modeli (Agarwal ve ark., 2011, s:124)

Modelde ayrıca verilerin uçuculuk sıralaması yapılmakta ve uçucu verilere öncelik verilmektedir. Özellikle vurgu yapılan nokta, cihazın pil durumunun verilerin kurtarılması noktasındaki önemidir. Elde edilen elektronik aygıtlarda pillerin bitmesi verilerin kaybolmasına sebep olacağından, bu durumun engellenmesi gerekmektedir. Bunun için, güç adaptörü kullanmak veya pilleri değiştirmek, güç sağlamak mümkün değilse pil ömrünü korumak için cihazı kapatmak tedbirleri önerilmektedir (Agarwal ve ark., 2011, s:126).

2.1.11. Bulut Bilişime Yönelik Model

Martini ve Choo, 2012 yılında bulut adli bilişimdeki ihtiyaçları ve eksiklikleri tespit etmiş, bulut bilişim ortamında dijital adli incelemeler yürütmek için, McKemmish (1999) ve NIST'in (Kent, 2006) yaygın olarak kullanılan iki çerçevesini

birleştiren bir model üretmişlerdir: **"Bulut Bilişim İçin Entegre Bir Kavramsal Dijital Adli Çerçeve (***An İntegrated Conceptual Digital Forensic Framework For Cloud Computing***)".** Uzmanlar, bulut bilişimin yapısal özelliğinden kaynaklı olarak, verilerin fiziksel konumu, birden çok sunucuya veya depolama cihazına ve yargı bölgesine dağıtılması vb. nedenlerle bulut bilişim ortamında "toplama" aşamasına özellikle vurgu yapmışlardır (Martini ve Choo, 2012, s:71).

Bulut adli bilişim aşamalarının, temelini aldığı diğer iki modeldeki aşamalarla karşılaştırılması Çizelge 2.1.'de gösterilmektedir (Martini ve Choo, 2012, s:74):

Çizelge 2.1. Bulut Adli Bilişim Modelinin Diğer Modellerle Karşılaştırılması

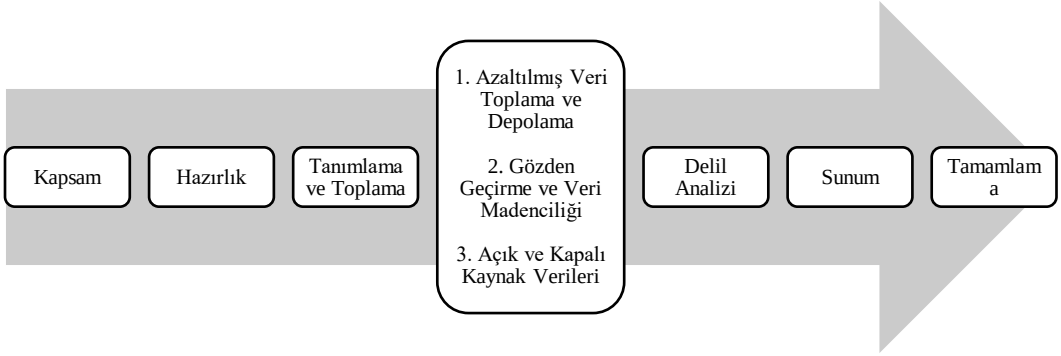
BULUT ADLİ BİLİŞİM MODELİ (Martini ve Choo, 2012)	MCKEMMISH MODELİ (1999)	NIST MODELİ (Kent, 2006)
Kanıt Kaynağı Tanımlama Koruma	Tanımlama	Toplama
Toplama	Koruma	İnceleme
İnceleme Analiz	Analiz	Analiz
Rapor Sunum	Sunum	Rapor

Bu modelde diğerlerinden farklı olarak, 3.aşama olan inceleme ve analiz aşamasında bulut bilişim kullanımına dair kanıt keşfedilirse, yineleme söz konusu olmaktadır. Eğer kanıt kaynağı tanımlama ve koruma ile başlar ve bu (ikinci) yineleme sırasında toplanan verilerin incelenmesi ve analizi sırasında daha fazla kanıt kaynağı belirlenirse, başka bir (üçüncü) yineleme başlayacaktır. İlk yineleme sırasında tespit edilen delillerin muhtemelen masaüstü bilgisayarlar, dizüstü bilgisayarlar ve mobil cihazlar gibi fiziksel bir aygıt olacağı, ikinci yineleme sırasında ise, vakayla ilgili bulut hizmetlerinin / sağlayıcılarının devreye gireceği ve bulut sağlayıcısı ile depolanan olası kanıtların ve bu potansiyel kanıtların korunmasına yönelik süreçlerin tanımlanacağı belirtilmiştir.

Mantıksal bir açıdan bakıldığında da, bir araştırma sırasında bulut hizmetlerinin kullanılıp kullanılmadığını anlamak için önce diğer kanıtlar incelemeli (Beverly ve Garfinkel, 2011), hangi hizmetlerin kullanılacağı, elde edilen verilerin hangi formatta olduğu ve bu verilere yasal erişimin nasıl sağlanacağı gibi konular belirlenmelidir.

2.1.12. Veri Madenciliği Modeli

Adli bilişim süreçlerinde ele geçirilen ekipman sayısındaki ve veri hacmindeki büyüme, bulut bilişimin kullanılmasındaki yaygınlık ve depolama kapasitesindeki artış, adli bilişim laboratuvarlarını etkileyecek kadar büyük sayıda kanıtın birikmesine neden olmakta olup, bununla ilgili bir çözüme ihtiyaç duyulmaktadır. Quick ve Choo, veri azaltma, veri madenciliği, artırılmış işleme gücü, dağıtılmış işleme, yapay zeka ve diğer yenilikçi yöntemler (Choo ve Quick, 2014) ile bu soruna bir çözüm üretebilmek adına 2014 yılında veri azaltma ve veri madenciliği hakkında bir çerçeve model geliştirdiler: **"Veri Azaltma ve Veri Madenciliği Çerçevesi** ***(Digital Forensic Data Reduction and Data Mining Framework)***". Çerçeve, dijital adli soruşturmada karşılaşılan zorlukları göz önünde bulundurarak, adli analizin yedi gereksinimini listelemektedir: daha hızlı toplama, azaltılmış depolama, zamanında inceleme, istihbarat, araştırma, bilgi yönetimi, arşivleme ve erişim. Önerilen çerçevede, depolama taleplerini azaltmak için bir veri azaltma yöntemi ile daha verimli bir adli veri alt kümesi toplama süreci öngörülmektedir. Adımlar şu şekilde belirlenmiştir (Şekil 2.11):



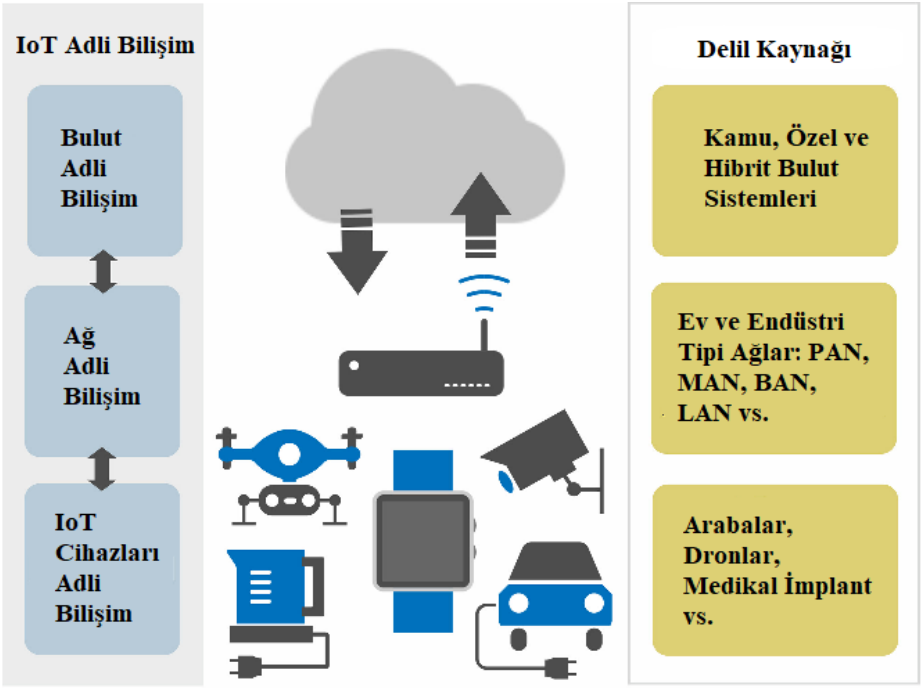
Şekil 2.11. Adli Bilişim Veri Azaltma ve Veri Madenciliği Yapısı

Soruşturmanın odağını ve kapsamını ana hatlarıyla belirleyerek başlayan araştırma sürecinde, veri azaltma işlemi imaja veya fiziksel medyaya uygulanarak, mantıksal kanıt muhafaza deposu adli alt kümesi oluşturulmakta, alt küme verilerinin incelemesini yapmak için adli bilişim ve istihbarat analizi metodolojisi kullanılmaktadır. Halka açık kullanılan sosyal hesaplardaki veriler, bloglar vb. açık kaynak verilerini, gizli bilgi kaynakları ise kapalı kaynak verilerini oluşturmaktadır. Model, raporların ve dosyaların yedeklenmesi ve geri bildirim ile tamamlanmaktadır (Quick ve Choo, 2014).

Triyaj, önceki modellerde de bahsedildiği gibi, öncelik sıralaması yöntemini benimseyerek veri azaltma sürecine destek sağlamaktadır. Bazı cihazlar olayla ilgili potansiyel kanıtların büyük çoğunluğunu bünyesinde taşırken, bazı cihazlarda kayda değer kanıtlar bulunmayabilir veya bazı deliller uçuculuk özellikleri sebebiyle özel ve hızlı analize ihtiyaç duyarken bazılarının bekletilmesi herhangi bir soruna yol açmayabilir. Triyaj ve veri azaltma süreci bu sebeple, verilerin hızlı bir şekilde aranmasını, toplanmasını, işlenmesini sağlar, zaman ve maliyet kaybını önleyerek sağlıklı sonuca ulaşılmasına yardımcı olabilir.

2.1.13. Nesnelerin İnterneti (IoT) Modeli

Akıllı evlerin kontrolünden, gelişmiş şehir yönetim sistemlerine kadar uygulama alanı yaygınlaşan IoT cihazları, suça konu bir olay meydana geldiğinde adli bilişim açısından faydalı veriler bulundurma ihtimali yüksek sistemlerdir, çünkü milyarlarca kablosuz aygıtın internete bağlanması sonucunda bireysel ve toplu olarak, büyük miktarlarda veri üretilip tüketilmektedir (Hegarty ve ark., 2014, s:163). Bununla birlikte, daha yeni yeni gelişmeye başlayan IoT cihazları adli bilişim için kullanılan araçlar ve uygulanan yöntemler tarafından desteklenmemektedir, bu da araştırmacıların bu alanda özel olarak uzmanlaşmış bilgi birikimine sahip bir uzman yardımı olmadan analiz edilmesini zorlaştırmaktadır (Servida ve Casey, 2019, s:1).
IoT ile ilgili kanıt kaynakları Şekil 2.12.'de gösterilmektedir:



Şekil 2.12. IoT Adli Bilişim Modeli Çalışma Prensibi (Stoyanova ve ark., 2020)

Standart adli bilişim aşamaları IoT cihazlar söz konusu olduğunda yeterli gelmemekte ve beklenen etkiyi maalesef gösterememektedir. Suça konu olay gerçekleştiğinde, araştırılacak verilerin depolandığı yer ile bu verilerin nereden geldiğinin belirsizliği, arama ve el koyma aşamaları için sorun oluşturmaktadır.

IoT cihazlarının çoğu düşük depolama kapasitesine sahip olduğundan, bu cihazlarda üretilen verilerin işlenmesi ve depolanmasında, geniş kapasitesi ve kolay erişilebilirliği sebebiyle bulut sistemlerinden faydalanılmaktadır. Ancak adli bilişim açısından bulut sistemlerinin kendisi birçok soruna sahip olduğundan, benzer sorunlarla IoT cihazları da karşılaşmaktadır.

Tüm bu belirsizlikler sebebiyle, Shams Zawoad ve Ragib Hasan **"FAIoT** *(Forensics-aware IoT)***"** modelini oluşturdular. Model, "IoT altyapısının yüksek oranda dağıtıldığından ve cihazlar arasında standardizasyon olmadığından, kanıt toplama ve analiz sürecini kolaylaştırmak için merkezi bir güvenilir kanıt havuzu

önermekte", cihazların bu güvenli kanıt havuzu hizmetini kaydetmesini yeterli görmektedir (Zawoad ve Hasan, 2015, s:4).

Model, üç modülden oluşur; Güvenli Kanıt Koruma Modülü, Güvenli Kaynak Modülü ve Uygulama Programlama Arayüzü (API - *Application Programming Interface*) aracılığıyla kanıta erişim. **Güvenli Kanıt Koruma Modülü,** tüm kayıtlı IoT cihazlarını sürekli olarak izleyecek ve kanıtları kanıt havuzunda güvenli bir şekilde saklayacaktır. **Güvenli Kaynak Modülü**, dijital veri gizliliğinin ve gözetim zincirinin korunmasından sorumludur. **API Aracılığıyla Kanıtlara Erişim,** bir soruşturma sırasında, kanıtlara ve kaynaklara yalnızca mahkemenin ve araştırmacıların erişimine imkan vermektedir. Bu model ayrıca, genel-özel anahtar tabanlı şifreleme kullanarak verilerin gizliliğini korumakta, böylece verileri yalnızca araştırmacılar görüntüleyebilmektedir (Zawoad ve Hasan, 2015, s:4). IoT'nin yapısındaki belirsizlik ve adli bilişim açısından öngörülemezliği nedeniyle başka uzmanlar tarafından üzerinde çalışılan bir alan olmaya devam etmektedir.

2.2. En İyi Uygulamalar

Dijital suçların araştırılması ile adli bilişim yöntemlerinin uygulanmasında uzmanlarca oluşturulan modellerin en uyumlu kombinasyonu, tüm ülkelerin yararlanmasına açık en iyi uygulama rehberlerine (*best practices*) dönüştürüldüğünde ve ülkeler eylem planlarını ve prosedürlerini bu rehberlere uygun şekilde oluşturduğunda, birbirleriyle benzer nitelikte uygulamalar ve farklılık gözetmeyen hukuka uygun yargılamalar söz konusu olabilecektir.

Başta Amerika Birleşik Devletleri olmak üzere, Birleşik Krallık, Avustralya, Çin, Fransa gibi pek çok ülke birçok en iyi uygulama rehberi yayınlamıştır. Görülecektir ki, tıpkı adli bilişim modellerinde söz konusu olduğu gibi en iyi uygulamalarda da birçok husus benzerlik göstermektedir. Söylenebilir ki, araştırma, inceleme, soruşturma ve yargılama faaliyetlerinde senkronizasyon sağlanması için de bu benzerlikler anlaşılabilir durumlardır. Bu çalışmada da konunun anlamsal

bağlamının sağlanması açısından birçok benzerlik yer alacak ancak özellikle farklılık arz eden hususlar aktarılmaya çalışılacaktır.

Bu kapsamda uzmanlara, araştırmacılara, kolluk kuvvetlerine ve yargı mensuplarına yol gösterici ve bilgilendirici özellikleri olan bu en iyi uygulama rehberlerinin bazı bölümleri bu alanla ilgili hususları eksik bırakmamak adına bu tez çalışmasının amacıyla örtüşmesi sebebiyle aşağıda anlatılmaktadır.

2.2.1. Ulusal Adalet Enstitüsü - NIJ

1968 yılında Amerka Birleşik Devletleri'nde Adalet Bakanlığı'nın araştırma, geliştirme ve değerlendirme kuruluşu olarak kurulan Ulusal Adalet Enstitüsü (NIJ - *National Institute of Justice*) kuruluş amacını; "suçla mücadele edebilmek ve adaleti yürütebilmek için benzersiz uzmanlıklar öğrenmek, araştırmalar yaparak bilgi toplamak ve standartlar geliştirerek uygulayıcılara ve politika yapıcılara yardımcı olmak" olarak özetlemiştir (NIJ, 2021). NIJ'in farklı dijital cihazların araştırılmasıyla ilgili en iyi uygulamaları olduğu gibi, olay yerine ilk müdahale edenlere yol gösteren kılavuzları ve kanun uygulama rehberleri de bulunmaktadır.

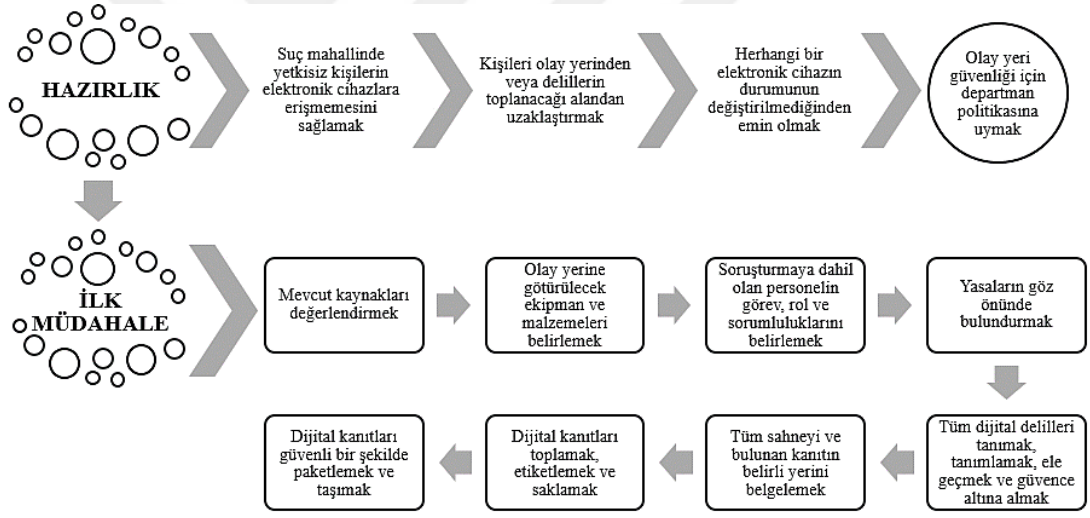
2.2.1.1. NIJ - Elektronik Suç Mahalli Soruşturması, İlk Müdahale Edenler İçin Rehber

Soruşturmaya konu olan bir olay meydana geldiğinde, olay yerine giden ilk müdahale ekiplerinin delillerle ilk karşılaşan kişiler olmaları sebebiyle, bu delillerin bütünlüğünü ve değişmezliğini sağlama noktasında yüksek sorumlulukları bulunmaktadır. Bu deliller özellikle elektronik nitelik taşıdığında, standart adli bilimlere ilişkin araştırmalardan farklı bir sistem altında toplanması ve araştırılması söz konusu olacağından, ilk müdahalecilerin bu alanda eğitim almış tecrübeli kişiler olması hayati önem taşımaktadır. İlk müdahalecilerden bahsederken sadece delilleri araştırıp toplayanları değil, olay yeri ile ilk karşılaşan herkesi; suç mahallini

inceleyen personeli, o personeli denetleyenleri, kuruluşu yöneten kişileri de içine alan daha geniş bir perspektiften bakmak faydalı olacaktır.

Adli bilişimin ilk basamağını oluşturan hazırlık ve olay yeri inceleme süreçlerinde görev alacak nitelikli ve bilgili personelin net şekilde belirlenmesi, harici kişilerin ise olası bir hataya yer vermemek adına olay yerinden uzaklaştırılması, elektronik cihazlarla temasının engellenmesi azami özen gösterilmesi gereken konulardır.

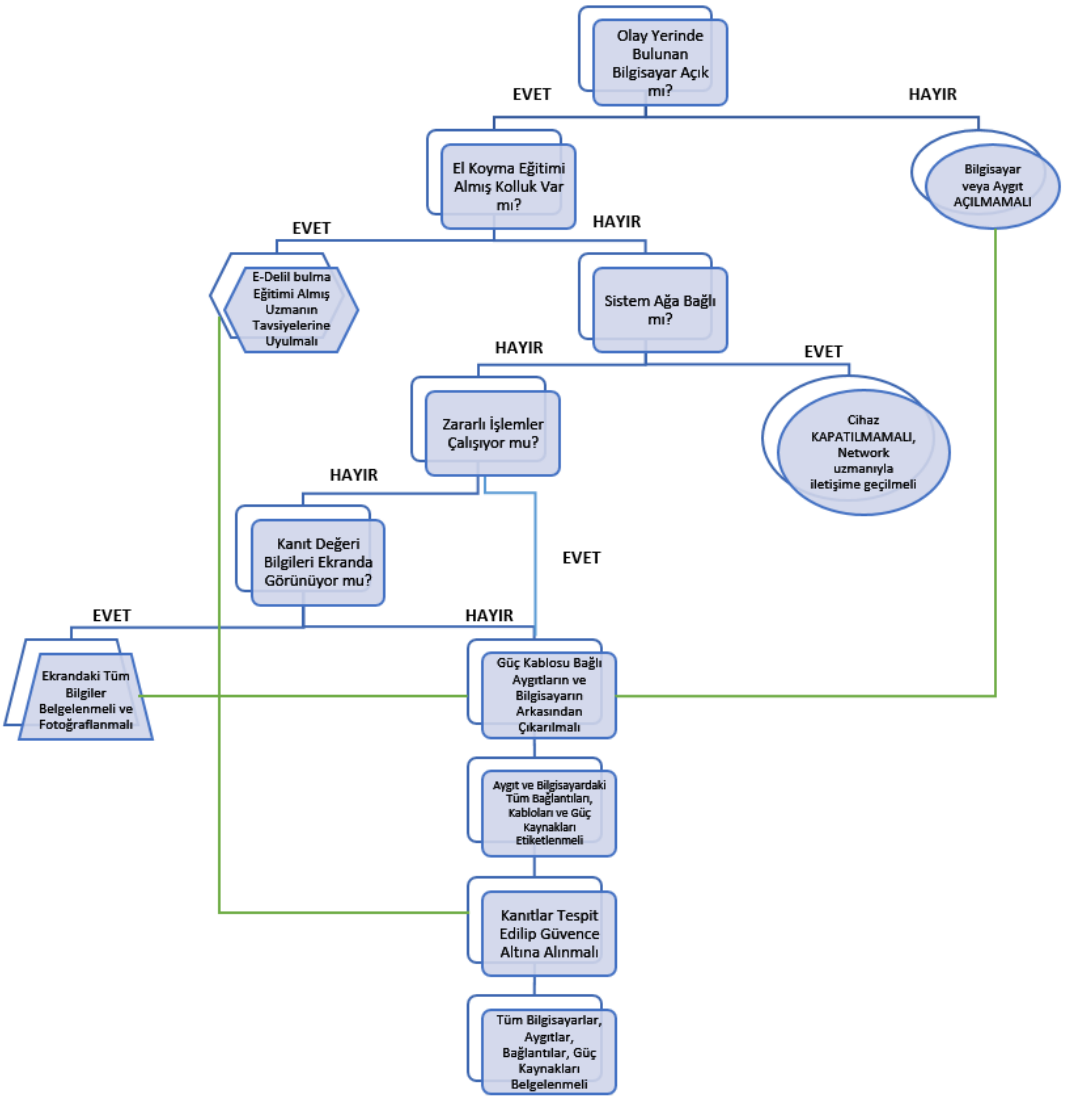
Bu hususta rehberde öne çıkan bazı noktaların akış şeması ile gösterimi şu şekildedir:



Şekil 2.13. İlk Müdahale Edenlerin Delil Elde Etme Süreci

Olay yerinde cihazların ve materyallerin konumu, inceleme sırasında olayı yeniden canlandırabilmek adına fotoğraf ve videolarla kayıt altına alınmalı, notlarla detaylandırılmalıdır. Aynı durum açık halde bulunan elektronik cihazların ekran görüntülerinden yapılan işlemlere ilişkin detayları toplarken de geçerlidir. Cihazın türü, yeri ve konumu, bileşenleri ve çevre birimleri ile diğer elektronik cihazlarla temasları dahil olmak üzere tüm konumu içermelidir. Kullanıcıların e-posta hesapları, internet siteleri, sosyal ağlar ya da diğer elektronik işlem yaptıkları

platformların hesap bilgileri ve şifreleri kullanıcılar tarafından unutulmamak adına kaydedilmiş olabilir. Gerek olay yerinde gerekse laboratuvar ortamında yapılan incelemelerde işlemlerin hızlı, kolay ve erişilebilir olmasını sağlamak adına, bu bilgilerin toplanması önemlidir. Benzer şekilde, internet servis sağlayıcısı bilgileri, güvenliğe ilişkin bilgiler, saha dışı depolama alanları, yüklü programlar-yazılımlar, internete erişim türü gibi bilgiler de kaydedilmelidir.



Şekil 2.14. Dijital Kanıt Toplama Akış Şeması (NIJ, 2001)

Rehberde, Şekil 2.14.'de şema olarak gösterilen, olay yerinde karşılaşılan bilgisayarın aktiflik duruma göre uygulanacak adımlarla ilgili bilgiler verilmiştir.

Kapalı bilgisayarlarla karşılaşıldığında açılmaması ve ilgili tüm bağlantıların etiketlenerek birbirinden ayrılması temel kuralken, açık bilgisayarlarda yapılması gereken işlemler çeşitlenmektedir.

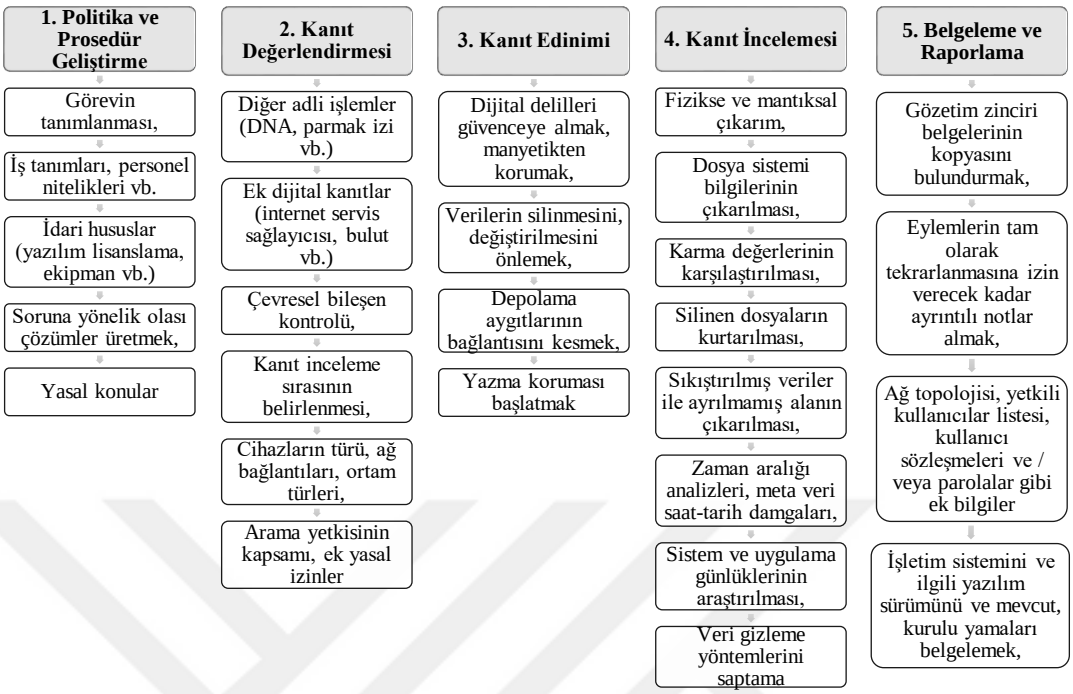
Tüm bu ihtimaller haricinde bazı durumlarda, güç durumuna müdahale edilmesi konusunda araştırmanın ve sonraki süreçteki soruşturmanın sağlıklı ilerleyebilmesini sağlayacak farklılıklar bulunmaktadır. Örneğin; araştırılacak cihazda yıkıcı bir işlem yapıldığına dair göstergeler ya da etkinliklerin ve bilgilerin silindiğine veya üzerine yazıldığına dair belirtiler varsa bilgisayarın gücünün kesilmesi en son yapılan işlemlerin (verilen komutlar, kullanılan belgeler, giriş yapılan zaman ile giriş yapan son kullanıcı vb.) ve diğer değerli bilgilerin korunmasını sağlamaktadır. Bu sebeple, her ne kadar cihazları mevcut konumlarında bırakmak (açıksa açık-kapalıysa kapalı) tercih edilen bir yöntem olsa da, ekranda suç kanıtı olduğuna dair bir belirti göründüğünde gücün kesilmesi önerilmektedir. (NIJ, 2001).

Dijital deliller yapıları itibari ile hassas ve yok olmaya müsait yapıda olup özel muamele gerektirmektedir. Radyo vericiler, hoparlör mıknatısları, manyetik alanlar, statik elektrik üreten cihaz veya malzemeler dijital delilleri bozma özelliğine sahiptir. Dijital kanıtların adli bilişim laboratuvarına götürülme sırasında ve ortamlarda bekletilmesi ile saklanması hallerinde, bu ve buna benzer faktörlerden arındırılmış ortamlarda taşınması, ısı, soğuk ve nemden, nakliye sırasındaki titreşim ve darbelerden korunması çok önemlidir. Her şeyden önce, elektronik yapıları manyetik ortamlardan uzak tutulmasını gerekli kılmakta, bu sebeple delillerin bozulmaması adına ilk müdahalecilerin faraday izolasyon torbaları veya alüminyum folyo gibi radyo frekans koruyucu malzemeler kullanması tavsiye edilmektedir. Bu malzemeler manyetik ortamlarla teması engellediği gibi, mobil cihazlar açısından arama, mesaj veya diğer iletişim sinyallerini almasını da önleyerek, delillerin değiştirilme ihtimalini ortadan kaldırmaktadır.

Dijital delillerin taşınması ve muhafazası konusunda göz ardı edilmemesi gereken önemli bir husus da elektronik cihazların pil durumlarını takip etmektir. Pilin araştırma yapmadan önce tükenmesi çok sayıda verinin kaybolmasına sebep olmaktadır.

2.2.1.2. NIJ - Dijital Delillerin Adli İncelemesi: Kanun Uygulama Kılavuzu

NIJ dijital delillerin incelenmesinden sorumlu kolluk kuvvetleri ve kolluk kuvvetlerinin diğer üyeleri tarafından kullanılmak üzere hazırladığı bu rehberde adli bilişimin temel aşamalarına girmeden önce, dijital delillerin korunması ve işlenmesi için Standart İşletim Prosedürleri (SOP - *Standard Operating Procedure*) geliştirilmesini önermekte, dökümantasyon aşamasının ise son sıraya bırakılmak yerine tüm aşamalara yayılması gerektiğini vurgulamaktadır (NIJ, 1999). Politika ve prosedürler, finansmanın sağlanması, özel eğitimli personel yetiştirilmesi, dijital kanıtları kurtarma tekniklerinin geliştirilmesi, lisanslı yazılımların kullanılması ve adli bilişim departmanlarının kurulup işletilmesini içermektedir (Şekil 2.15.).



Şekil 2.15. Dijital Delillerin Ele Alınması

Vaka detayını, donanım ve yazılımları, aranan potansiyel kanıtların ve incelenecek kanıtların elde edilmesini çevreleyen koşulları, arama emrini veya diğer yasal yetkileri gözden geçirerek kapsamlı bir değerlendirme yapılması rehberde tavsiye edilen noktalardandır. Olay yerinde arama ve el koyma yetkisini kapsamayan başka bir kanıt bulunursa, alınması gereken ek yetkilerin ve yasal işlemlerin hazırlığı yapılmalıdır.

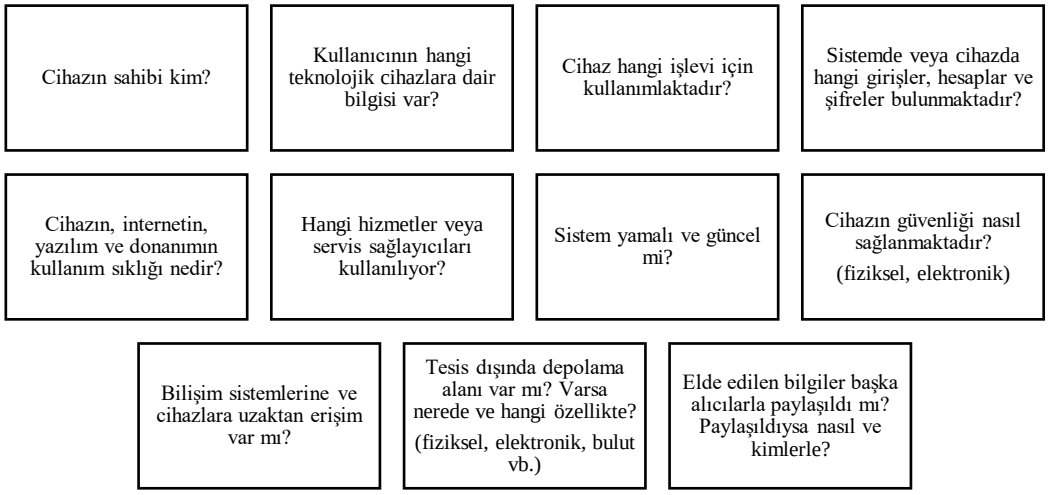
Rehberde kanıtların incelenmesi aşaması için Fiziksel ve Mantıksal Çıkarma olmak üzere iki bölümden bahsedilmektedir. Fiziksel sürücüde bulunan tüm verilerin, dosya sistemine bakılmaksızın tanımlanıp kurtarılması "Fiziksel çıkarma" olup, bölünmemiş alanlar dahil tüm bölümler incelenmektedir. "Mantıksal çıkarma"da ise, veriler veya dosyalar dosya sistemleri, uygulamalar ve/veya yüklü işletim sistemlerine bağlı olarak tanımlanıp kurtarılmakta ve tüm bölüm yerine sadece mantıksal bölümler esas alınmaktadır. Bir adli bilişim uzmanının, silinmiş ve

önceden tahsis edilmiş alanları içerdiği için tüm diskin fiziksel kopyasını hedeflemesi gerekmekte, ancak şifrelenmiş veriler söz konusuysa, fiziksel kopya yerine kilidi açılmış verilerin mantıksal bir kopyasını çıkarması tavsiye edilmektedir (CoE, 2017). Her ikisinde de veriler doğrudan bir depolama ortamından diğerine veya bir depolama ortamından bir hedef ortamdaki bir veya daha fazla görüntü dosyasına bit-bit kopyalanır; verileri bir görüntü dosyasına yazmak ise avantajlı olandır (CoE, 2017).

2.2.1.3. NIJ - Teknolojinin Araştırmacı Kullanımları: Cihazlar, Araçlar ve Teknikler Rehberi

NIJ bu rehberi "teknolojiyle ilgili suçlarla veya bu suçları araştırmak için mevcut araç ve tekniklerle sınırlı deneyimi olan veya hiç deneyimi olmayan kişilere (kolluk kuvvetleri personeli, soruşturmacılar, ilk müdahale ekipleri, dedektifler, savcılar vb.) kaynak olması" amacıyla oluşturduğunu, rehberde her detay bulunmamakla birlikte, en sık karşılaşılan tekniklere, cihazlara ve araçlara yer verildiğini belirtmektedir (NIJ, 2003).

Araştırmada kullanılan yazılım ve donanımlar, cihazlar, toollar ve teknikler, delillerin değişmeden elde edilmesi, incelenmesi, korunması, taşınması hususlarında önemli görevler üstlenmektedir. Rehber, bilgisayar, cep telefonu, dijital kamera, kişisel dijital asistan (PDA - *Personal Digital Assistant*), çağrı cihazı gibi çok sayıda elektronik cihazı kullanma becerisine sahip kullanıcıların bilgi düzeylerini ölçmek için şu soruların sorulmasını önermektedir (Şekil 2.16.):



Şekil 2.16. Kullanıcıların Bilgi Düzeylerini Analiz Soruları

Elektronik delillerin ve verilerin bulunduğu yer ile cihazların bulunduğu yer arasında farklılık olduğu durumlarda, uzaktan erişim veya bulut depolama sistemleri kullanılıyor olabilir. Diğer taraftan, olay yerinde bazı cihazların garanti belgeleri ve kullanım kılavuzları, hizmet veya ürün alımına ilişkin faturalar, çöpe atılmış USB'ler veya fiziki belgeler vb. birçok değişik yerde ve farklı nitelikte delil ihtimali olabilecek bilgiler de bulunabilir.

Araştırmalar sırasında olay yerinde bulunabilecek ses kaydı, video görüntüsü, resim ve fotoğraflar için örneğin videolarda format görüntüleyici, kalite düzeltici; resimlerde ise kaliteyi iyileştirmek için ilgili teknolojiler kullanılmaktadır. Ses kaydının analizinde kayıtların kalitesini iyileştirilmesi, gürültülerden arındırılması, arka plandaki önemli olabilecek seslerin veya konuşmaların ayıklanması, faydalı bilgilerin elde edilmesini sağlayabilir.

Bilgisayar kullanıcılarının internet veya bilgisayar ağları üzerinden telefon görüşmeleri yapmalarına olanak sağlayan İnternet Protokolü Üzerinden Ses İletişimi (VoIP - *Voice over Internet Protocol*)'nin sakladığı abone ve işlem bilgileri İnternet Servis Sağlayıcılardan bilgi almak için işletilen yasal sürece benzer bir yöntemle elde

edilmekle birlikte, bu iletişimlerin rızaya dayalı olmadan elde edilebilmesi için bir telefon dinleme yetkisi gerekmektedir.

Telesekreterlere bırakılan mesajlardan tarih ve saat bilgileri, bırakılan mesajın dinlenip dinlenmediği, şüpheli mesajların değiştirme veya silinme durumunun söz konusu olup olmadığı, kayıp, takip ve tehdit gibi vakalarda yönlendirici bilgiler içermektedir. Ancak telesekreterlerle ilgili önemli nokta; cihazın gücünün kesilmesi verilerin kaybolmasına sebep olabileceğinden, gücü kesmeden önce mesajların kaydedilmesi tavsiye edilmektedir. Ayrıca, telesekreterlerde mesajlara uzaktan erişimin mümkün olması, onların değiştirilip temizlenebilmesine imkan sağlamaktadır.

Kredi kartı dolandırıcılık cihazları olarak skimmer, kodlayıcı, three-track manyetik kart okuyucular ve satış noktası yetkilendiricilerde; kredi kartlarının manyetik şeridinde bulunan numara, son kullanım tarihi, kart sahibinin adı gibi bilgileri kopyalayan "*Skimmer*"; kredi kartı, ehliyet veya manyetik şeritli/çipli kartlara sahte bilgiler yazan "*Encoder* - Kodlayıcı"; kredi kartındaki manyetik şeritteki tüm verileri çözen ve doğrulayan "*Three-Track* manyetik kart okuyucular"; bir perakende satış mağazasındaki ödeme alanındaki işlemleri kaydeden ve kredi limitlerini kontrol etmek için kullanılan "Satış Noktası Yetkilendiriciler" olay yerinde bulunabilir ve büyük hacimli boş manyetik şeritli kartlar, sahtekarlık veya yasa dışı eylemin göstergesi olabilir. Bu cihazlar üzerinde çok sayıda kredi kartı bilgisi bulunabileceğinden, bunların analizi için uygun ekipmanlar kullanılmalıdır.

Kameralar, manuelden dijital sistemlere geçişle birlikte boyutları gittikçe küçülerek çok sayıda legal ve daha çok da illegal faaliyette kullanılmaya başlandı. Kalem, çakmak gibi nesnelerin içine gizlenebilecek kadar küçük boyutlara ulaşan bu kameralar özel hayatın gizliliğini ihlalden, kişisel verilerin izinsiz kaydedilmesine varan geniş yelpazede pek çok suçun da aracı konumuna sahiptir. Dijital kameralarla yakalanan veya saklanan veriler resim, video veya sesten oluşmakta, bu veriler cihazdan silinmiş olsa bile bazı durumlarda kurtarılabilir nitelik taşımaktadır.

Bir ortamda bulunan faks makineleri eski veya yeni teknoloji ürünü olabilir, bağımlı veya bağımsız şekilde çalışabilir. Eski modellerde eski fakslar film kartuşlarından okunabilirken, yeni modellerde bilgisayar tabanlı olup olmamasına göre farklılık gösterebilir. Eğer bilgisayar kullanılarak faks gönderiliyorsa bilgiler sabit sürücüde bulunur ve bilgisayarın incelenmesi gerekir, eğer bilgisayar tabanlı değil ise, bilgiler dahili bellekte tutulabilir. İnceleme yapılmadan önce bu cihazların geçici ve sınırlı bellekleri olduğu unutulmamalıdır.

Küresel konumlandırma sistemi (GPS - *Global Positioning System*) alıcıları adli bilişim araştırmacılarına kişileri veya araçları takip etmede, olay yerinin haritasını çıkarmada, arama emrinde belirtilen yeri bulmada yardımcı olmaktadır. Elde taşınan GPS alıcılarında veriler, cihaz içinde veya eşlik eden medyada depolanmaktadır.

Rehberde araştırmacıları özellikle dikkat etmesi gereken cihazlardan birinin evlerde keyifli vakit geçirmek için kullanılan video oyun konsolları olduğu ve bu cihazların elektronik bilgileri saklamak için modifiye edilebileceği belirtilmektedir.

Araçlarda bulunan navigasyon sistemleri ve kara kutular, aracın fiziksel konumu, durumu, hızı, daha önce seyahat ettiği rotalar ve işletim geçmişi gibi bilgileri yakalamakta, araç iletişimlerini izlemeye yaramaktadır (NIJ, 2003).

Tuş vuruşu izleme araçları, birtakım yazılım veya donanımlar kullanarak, bir bilgisayardaki klavye etkinliğinin izlenmesine ve kaydedilmesine yarar. Hangi web sitelerine gidilip kimlerle iletişim kurulup ne gibi veriler oluşturulduğuna ilişkin bilgiler içerebilir. Halka açık makinelerden alınan kimlik hırsızlığında kullanılan bilgiler, kurumsal bilgisayarlardan alınan ekonomik bilgiler, kullanıcı adları ve şifreler gibi çok sayıda veri için de kullanılabileceği belirtilmektedir.

Fotokopi makineleri, yazıcılar gibi çoğaltım araçları yazılım korsanlığının, telif hakkı ihlalinin veya kaçak materyalin kopyalanmasının kanıtını oluşturabilir çünkü bu cihazlar kayıt tutma özelliğine sahiptir.

Kişisel dijital asistan (PDA)lar adı üzerinde bir asistan gibi tüm hayatımızı düzenleyip, yapılacakları hatırlatan ve her türlü eylemin ve bilginin yer aldığı cihazlardır. Genellikle bir veya birden fazla bilgisayarla senkronize hareket etmeleri ise onları faydalı birer delil depolama aracına dönüştürmektedir. PDA'ları inceleme konusunda da bilgisayarlardaki kurallar geçerli olacaktır; PDA'nın bataryasının bitmesine müsaade edilmemeli, cihaz kapalı bulunmuşsa açılmamalı, açık bulunmuşsa ekran fotoğrafı çekilip bilgiler kaydedilmelidir.

Sniffer (Koklayıcı), kullanıcının internet trafiğini gerçek zamanlı olarak "koklaması" yani izlemesine yarayan, bilgisayardan akan tüm verileri yakalayan bir araçtır. Üniversiteler, devlet kurumları ve kurumsal bilgi teknolojisi departmanları veya şirket yöneticileri tarafından ağları üzerinden düzenli trafik akışını kontrol etmek ve sorunları saptamak için yasal şekilde kullanım alanı bulurken, diğer taraftan çoğunlukla illegal olarak oturum açma şifrelerine, kimlik ve kart bilgilerine ve finansal ayrıntılara erişmek için kullanılmaktadır. Siber suçlular, snifferların indirilmesi için sosyal mühendislik veya kimlik avı dolandırıcılıklarından yararlanabilmekte veya halka açık Wi-Fi ağlarını kullanabilmektedir (Belcic, 2020). Sniffer verilerinin kullanımı yasal olarak hassastır ve telefon dinleme yasalarını ilgilendirebilir.

Steganografi, bir mesajın varlığını basitçe başka bir dosya görüntüsünün veya videonun içine gizleyerek üçüncü kişilerin eline geçmesini engellemek için kullanılan tekniktir ve Yunanca "*Staganos*" (örtülü, gizli veya korumalı) ve "*Graphein*" (yazı) kelimelerinden türetilmiştir (Kessler ve Hosmer, 2011). Bilgileri gizlemek için kullanılan en yaygın dosya türleri görüntü dosyaları olsa da, diğer dosya türlerinde gizleyecek programlar da mevcuttur.

Rehberde adli bilişim uzmanlarının ve araştırmacıların karşılaşabilecekleri, olması kuvvetle muhtemel bazı senaryolar üzerinden konu anlatılmaya çalışılmıştır. İlk bakışta suç konusu olayı aydınlatma hususunda ne gibi faydaları olacağı kestirilemeyen bazı elektronik cihazlarla ilgili bilgi vermesi bakımından bu senaryolar oldukça aydınlatıcıdır. Örneğin; suç konusu olayın şüphelisi, yapılan sorgu sırasında, suçun işlendiği sırada iş yerinde olduğunu söylemiş, ancak yapılan araştırmalar, şüphelinin çalıştığı şirkette anahtar kart erişim sistemi kullanıldığını ve şüphelinin o gün işe gitmediğini saptamıştır. Diğer bir olayda ev alarm sisteminin kurulup kurulmamasının şüphelinin olayla bağlantısı olup olmadığı konusunda oldukça belirleyici olabileceği görülmüştür. Kayıp veya kaçırıldığı düşünülen bir kişinin, bankadaki video kaydından ATM'den para çekmesi neticesinde kaçırılmadığı ve tek başına olduğu tespit edilmiştir.

2.2.2. Dijital Kanıt Üzerine Bilimsel Çalışma Grubu - SWGDE

1998 yılında kurulan SWGDE'nin amacı, "dijital delillerin kurtarılması, korunması ve incelenmesi için disiplinler arası yönergeler ve standartlar geliştirmek için adli bilişim alanında aktif olarak görev yapan kolluk kuvvetleri, akademik ve ticari kuruluşları bir araya getirmek"tir (Sammons, 2012, s: 8).

IOCE tarafından yürütülen standardizasyon çabalarının ABD merkezli bileşeni olarak kabul edilmekte olup, IOCE'nin tüm hukuk sistemlerinde tutarlılık ve ortak dil sağlama ile dijital delillerin adli bilişim sürecindeki akıbeti konusunda kurallara uygunluk gibi pek çok amacı ile de örtüşen bir yapıya sahiptir (SWGDE, 2000a).

Alt bölümde, SWGDE'nin herbiri ayrı bir tez konusu olacak nitelikte ve çok sayıda farklı elektronik aygıtı içerecek kadar geniş yelpazede en iyi uygulama rehberlerinden özet halde ve önemli görülenlerle sınırlı bilgi verilecektir.

2.2.2.1. SWGDE Adli Bilişim için En İyi Uygulamalar Rehberi

Rehber, adli bilişim incelemeleri sırasında bulunan verileri toplamak, elde etmek, analiz etmek ve belgelemek için en iyi uygulamaları açıklamak amacıyla oluşturulduğunu belirterek, özellikle silme yazılımları ve diğer anti-adli bilişim tekniklerine dikkat edilmesi ve bulut bilişim gibi uzak depolama ortamlarının bulunup bulunmadığının gözetilmesi gerektiğini belirtmiş, elde edilen delillerin fiziki ve elektronik olarak korunmasını sağlamak için önlemler alınması gerektiğini eklemiştir (SWGDE, 2014a).

2.2.2.2. SWGDE Canlı Sistemlerin Yakalanması

Canlı/çalışan bilgisayar sistemlerinden veri elde ederken, verileri kullanılabilir bir formatta kaydetmek için gerekli olan prosedürlerin bahsedildiği bu rehber, verileri uçuculuk sırasına göre ayırarak, veri toplama sıralamasının en uçucu verilerden başlayarak yapılması gerektiğini vurgulamış ve sıralamayı; 'RAM, çalışan sistemler, ağ bağlantıları, sistem ayarları, depolama ortamı' şeklinde özetlemiştir. Uçucu veriler sistem kapatıldıktan sonra kaybolacağı için, 'canlı edinme' sistemi benimsenerek veriler kaydedilmelidir. Bunun için de, canlı hafıza, canlı fiziksel edinim gibi yöntemler benimsenmekte, bu işleme özgü yazılım tabanlı araçlar kullanılmaktadır (SWGDE, 2014b). Rehberde özellikle vurgulanan husus, canlı edinimin, sistemde birtakım değişiklikler yapma riski bulunması, bu sebeple araştırmayı yapacak kişinin bu risklerin farkında olması gerektiğidir.

2.2.2.3. SWGDE Adli Bilişim Edinimleri için En İyi Uygulamalar

Başta bilgisayarlar olmak üzere, üzerinde depolama üniteleri olan bilişim sistemlerinden dijital delil elde etmede dikkate alınması gereken şifreleme anahtarları, meta veriler gibi alanlarla, eşleştirilmiş cihazlardaki ve uzak konumlardaki veriler rehberin dikkat çektiği hususlardır. Araştırma yapan kişiler

çeşitli elektronik cihazlardan, o cihazlara özgü verileri uygun ve güvenilir yazılım ve donanımlarla incelemelidir. Bu kapsamda, inceleme yapılacak cihazlarla, fiziksel ve elektronik depolama ortamlarının steril yani temiz/güvenli olması çok önemlidir (SWGDE, 2018a).

2.2.2.4. SWGDE Mobil Telefon Adlli Bilişimi için En İyi Uygulamalar

Rehberde Mobil Adli Bilişim konusunda cihazın özelliğine veya araştırmanın niteliğine göre farklılaşan analiz yöntemlerinden bahsedilmiştir: Telefonun ekranını çalıştırmak, tuş takımını kullanmak ve dahili bellekteki verileri açmak için "Manuel işlem", telefonun sökülmesini gerektiren (invazif) ve gerektirmeyen (invazif olmayan) biçimde fiziksel verilerin alınmasını sağlayan "Fiziksel işlem", dosya sisteminin bir bölümünü çıkaran "Mantıksal işlem", mikroskop kullanarak bellek hücrelerini incelemeye yarayan "*MicroRead*" işlemi, bellek yongasının çıkarılarak okunması işlemi ve dosya sistemine erişim işlemi (SWGDE, 2013a).

Kullanıcıların bazı işlemlerini gizleyen mobil uygulamalar bu cihazlarda bulunabilmekte ve bu uygulamalar, içindeki içerikleri maskelemek için özel olarak tasarlanarak, cihaza üretim sırasında standart olarak yüklenmiş uygulamalar gibi görünebilmektedir (örn., Hesap Makinesi +) (SWGDE, 2020b). Adli bilişim uzmanının araştırmalar sırasında bu gibi detayları atlamadan inceleme yapması gerekmektedir.

2.2.2.5. SWGDE Bulut Depolamadan Kanıt Edinimi için En İyi Uygulamalar

Bulut Depolama, kullanıcının bilgisayarı, mobil cihazı veya fiziksel bir aygıtı tarafından gerçekleştirilen işlemler neticesinde ortaya çıkan verilerin, cihazın kendi depolama alanına kaydedilmek yerine uzak bir depolama alanına iletildiği sistemlerdir (SWGDE, 2018b). Bulut sistemleri, bilişim sistemlerinin depolama

alanlarının, kaydedilen verilerin sayısı ve boyutuna göre yeterli gelmediği durumlarda depolama kapasitesini artırmak ve kaydedilen verilere ilgili elektronik cihazlara bağlı kalmadan birçok bilişim sisteminden uzaktan erişim yöntemiyle ulaşmak için tercih edilmektedir.

SWGDE rehberinde bulut depolama cihazları üç türe ayrılmıştır (SWGDE, 2018b):

- Kapı zili kameraları veya dadı kameraları gibi ev veya iş ortamında kullanılan, bilgisayar, telefon gibi fiziksel bir cihazla kontrol edilen, videoyu cihazın kendisinde değil de, doğrudan internette depolayan sistemler.
- İşyerlerinin güvenlik sistemlerinde yaygın olarak kullanılan merkezi konumda site dışında depolama yapan sistemler.
- Dijital video kaydediciden aktarılarak Google Drive, Dropbox vb aracılığıyla paylaşım için buluta aktarılan sistemler.

Suç konusu olay araştırmaları sırasında bulut sistemlerinin kullanıldığı tespit edildiğinde, şifreleme ile ilgili farklı durumlar ortaya çıkabilmektedir. Verilerin ilk kaydedildiği bilişim sistemleri şifre ile korunurken bulut sistemde herhangi bir şifre koruması bulunmayabilir veya tam tersi söz konusu olabilir ya da her iki sistemde de veriler şifrelenmiş olabilir (SWGDE, 2020c). Bu durumlarda diğer elektronik cihazlarda uygulanan prosedür dahilinde şifrelerin ilgililerinden elde edilmeye çalışılması söz konusu olacaktır. Bununla birlikte, arama iznine sahip araştırmacıların bulut hizmeti sağlayan cihazları fiziksel olarak araması da mümkündür.

Bulut hizmet sağlayıcısının hizmet politikasının incelenmesi, kullanıcılarını bilgilendirmeleri noktasında önem kazanmaktadır. Bu durum, durumdan haberdar olan kullanıcılar tarafından delillerin yok edilmesi veya değiştirilmesi ihtimaline binaen, mümkünse, sağlayıcının bildirim yapmasının engellenmesi ve verilerin korunmasının istenmesi önleyici bir çözüm olmaktadır (18 U.S. Code § 2705b). Bu

noktada eğer hizmet sağlayıcısından veri talep edilmişse, bu verilerin orjinal halleriyle istendiği özellikle belirtilmelidir. Bununla birlikte, eğer özel formatta veri aktarımı söz konusu olmuşsa, bu verilerin işlenmesi, dönüştürülmesi, şifrelerinin çözülmesi gerekebileceği için verilerin okunabilir bir formatta istenmesi de gerekebilir.

2.2.2.6. SWGDE Görüntü Bütünlüğünü Korumaya Yönelik En İyi Uygulamalar

Suç soruşturmasında elde edilen deliller arasında dijital görüntüler bulunduğu takdirde, bu görüntülerin bütünlüğünün, doğruluğunun, oluşturulduğu yer ve zaman ile oluşturanın kimliğinin tespiti araştırmanın hedefi olmaktadır. Görüntülerin değiştirilmeden ve sıkıştırılmadan saklanması, gerekli incelemelerin kopyalar üzerinde yapılması, görüntüler içerisinde yer alan çok sayıda bilginin bozulmasını ve kaybolmasını da önlemektedir. Görüntüleri oluşturan veya saklayan ekipmanlarla, incelemesini yapan araçlar arasında sürüm, format veya güncelleme açısından uyumsuzluk olduğunda, eksiksiz bir incelemenin yapılabilmesi için gerekli ayarlamalar yapılmalıdır (SWGDE, 2017c).

Rehberde bir görüntünün bozulup bozulmadığını anlamak için karma doğrulama ile görsel doğrulama yöntemlerinden bahsedilmektedir. '*Hash*' adı verilen adli bilişim sürecinin olmazsa olmazı sayısal değerler, görüntü analizinde de doğruluğu kanıtlayan temel yöntem olmaktadır. Orijinal görüntü ile incelenen görüntünün görüntü işleme araçları ile analiz edilerek değiştirilip değiştirilmediğinin kontrolü ise bir diğer yöntemdir.

Görüntü soruşturma açısından önemli bir konumdaysa, dosyalara yetkisiz erişimi önlemek için güvenlik duvarı, şifre koruması gibi yazılım tabanlı cihazlar veya işletim sistemi kullanılması, dijital imzalarla güvenliklerinin sağlanması, görsel inceleme yöntemleri kullanılarak doğruluğunun saptanması önerilmektedir (SWGDE, 2017c).

2.2.3. Polis Şefleri Derneği - ACPO

ACPO (Polis Şefleri Derneği - *The Association of Chief Police Officers*) 1948 yılında İngiltere'de kurulmuş olsa da, tarihi 1900'lere kadar uzanan, İngiltere, Galler ve Kuzey İrlanda tabanlı bir birlik olup, şirketleşmeleri 1997 yılında gerçekleşmiştir. 2015 yılında ise Ulusal Polis Şefleri Konseyi (NPCC - *National Police Chiefs' Council*) ACPO'nun yerini almıştır (NPCC, 2021).

2.2.3.1. ACPO Dijital Deliller İçin En İyi Uygulama Rehberi

Rehberde, işletim sistemleri ve diğer programların, elektronik depolamanın içeriğini, kullanıcıya farkettirmeden otomatik olarak değiştirme, ekleme ve silme durumlarından bahsederek, orijinal verilerin korunmasını sağlamak amacıyla, tüm cihazın fiziksel / mantıksal bir blok görüntüsü veya kısmi / seçici verileri içeren mantıksal bir dosya görüntüsünün alınması tavsiye edilmektedir (ACPO, 2012).

Bir olay söz konusu olduğunda olay yerinde, araştırılan konuyla ilgili olan veya olmayan birçok cihaz, medya ve veri bulunmaktadır. Rehbere göre, konuyla ilgisiz materyallere sadece aynı ortamda bulundukları için el konulmamalı, araştırmacıların bunun için haklı gerekçeleri olmalıdır. Elde edilen kanıtlar açısından ise, kanıtın bulunması kadar, nasıl ortaya çıktığının belirlenmesi de olayın aydınlatılması için araştırmacının sorumluluğunda kabul edilmektedir.

Rehberde birçok bilişim sisteminin analizi için detaylar belirtilmekle birlikte, ağ adli bilişim için önemli bazı hususların altı çizilmiştir. Ağa bağlı delil depolama özelliği bulunan cihazlarda, verilerin nerede tutulduğu konusunda belirsizlikler olabilmekte, bağlı cihazlardan herhangi birinde bulunabilmektedir. Bu cihazlar arasındaki veri alışverişi veya uzaktan erişim ihtimali araştırma sırasında göz önünde bulundurulmalıdır.

2.2.3.2. ACPO E-Suç Soruşturma Yöneticileri için İyi Uygulama ve Tavsiye Kılavuzu

Yargılama öncesinde işlenen suçun özel nitelik taşıması hallerinde herhangi bir sorun söz konusu olduğunda bilirkişilerin görüşüne ihtiyaç duymakta, bu ihtiyaç bazen savcılık makamından bazense savunma makamından gelebilmektedir. Birleşik Krallık nezdinde, bu ihtiyaç avukatlar tarafından ileri sürüldüğünde, avukatlar savunma uzmanlarına savcılığın yaptığı suçlamalar ve işlemlerle ilgili araştırma yetkisi verebilmektedir. Bu kapsamda savcılığın bulguları elektronik ortamda savunma uzmanlarınca test edilebilir, araçlar kullanılarak incelenebilir ve her iki tarafın uzmanları iletişim halinde olabilir (ACPO, 2008).

2.3. Temel Standartlar

Standardizasyon kavramı yakın tarihle ilişkilendirilse de standartlaşma ihtiyacı tarihin çok eski dönemlerinde karşımıza çıkmaktadır. Eski Mısırlıların kanalizasyon ve su yapıları, ev inşaatları, şehir ve peyzaj planlamalarında standart kalıplar, Sümerlerin çivi yazılarını yazdıkları plakaların özellikleri, Babillerin ürettikleri mallar ve üzerine koydukları etiketler, Perslerin ve Finikelilerin standart ölçü kalıpları ve birimleri gibi nesnelerin, yerleşik hayatın ve toplumlaşmanın getirdiği yaşam tarzında kolaylık ve sürdürülebilirlik sağlaması için birçok antik uygarlık standartlaşma yoluna gitmişlerdi.

1700'lerin sonunda Amerikan ordusunun 10.000 adet tüfek üretimindeki tüfek parçalarının birleştirilme işlemlerinin ilk standartlaşma örneği olduğu söylenebilir. Sonrasında her devlette teker teker kurulan birlikler, standartlaşma hareketlerini resmi zemine oturtmuştur.

1901 yılında İngiltere'de kurulan "Standartlar Birliği" (bugünki adıyla İngiliz Standartları Enstitüsü: BSI - *British Standards Institution*), 1918'de Amerika'da Amerikan Standartlar Komitesi (bugünki adıyla Amerikan Mühendislik Standartlar Komitesi: ANSI - *American National Standards Institute*), Almanya'da 1917 yılında Alman Standartları Birliği (DIN - *Deutsche Institut für Normung*),1922 yılında İsveç'te İsveç Standartları Komisyon (SIS - *Swedish Institute for Standards*), 1926 yılında Fransız Standartları Birliği (ANFOR - *Association Française de Normalisation*) gibi ulusal yapıların oluşturulması, uluslararası bir örgütün tek çatı altında toplama ihtiyacını körüklemiş ve temeli daha eski tarihlerde atılmakla birlikte 1947 yılında 25 ülke ile "Uluslarararası Standartlar Örgütü" (ISO - *International Organization for Standardization*) oluşturulmuştur.

ISO, Standardizasyonu; "Belirli bir faaliyet ile ilgili olarak ekonomik fayda sağlamak üzere bütün ilgili tarafların yardımı ve işbirliği ile belirli kurallar koyma ve bu kuralları uygulama işlemidir." şeklinde tanımlamaktadır. Mal ve hizmetlerin üretiminde, geliştirildikleri veya analiz edildikleri laboratuvarlarda ve kalite sistemlerinde aranacak özellikler standartlar vasıtasıyla düzenlemektedir.

Tez çalışmasının bu bölümünde aşağıda listelenen, adli bilişim konusunda ve onunla uzantılı diğer alanlarda genel kabul görmüş ulusal ve uluslararası standartların temel özelliklerinden bahsedilecektir:

- ISO - Uluslararası Standartlar Örgütü
  - ISO 27037 Standardı
  - ISO / IEC 27035 Standardı
    - ISO 27035-1
    - ISO 27035-2
    - ISO 27035-3
    - ISO 27035-4
  - ISO 27041 Standardı
  - ISO 27042 Standardı

- ISO 27043 Standardı
- ISO 30121 Standardı

➢ IOCE - Bilgisayar Kanıtı Hakkında Uluslararası Organizasyon

➢ ASTM International
- ASTM E2763 - 10
- ASTM E2825 - 12
- ASTM E2825 – 19

➢ BSI - British Standards Institution
- BIP 0008
  - BIP 0008-1
  - BIP 0008-2
  - BIP 0008-3
- BIP 0009
- BS 10008

➢ NIST - Ulusal Standartlar ve Teknoloji Enstitüsü

2.3.1. Uluslararası Standartlar Örgütü - ISO

Uluslararası alanda uygulanması amaçlanan ilk kalite standardı çalışmaları ISO tarafından 1947 yılında başlatılmış olup, özetle, bilimsel, ekonomik ve teknik alanlarda karşılıklı anlaşmaları sağlamak, ulusal standartları uyumlaştırmak, birleştirmek, önerilerde bulunmak ve dünyada standardizasyonu geliştirmek amacı taşıdığı belirtilmektedir.

ISO, neredeyse tüm faaliyet alanları ile ilgili ürünler, hizmetler ve en iyi uygulamalar için standartların geliştirilmesi ve yayınlanmasıyla ilgilenmektedir.

Örneğin, ISO 27000 standartları ailesi, dijital adli soruşturma dahil olmak üzere bilgi güvenliğine odaklanmakta, potansiyel dijital delillerin tanımlanması, toplanması, elde edilmesi ve korunması sırasında izlenmesi gereken prosedürleri özetlemektedir (Şekil 2.17.) (Veber ve Klíma, 2014):

Şekil 2.17. ISO Bilgi Teknolojisi ve Güvenlik Teknikleri Serisi Standartları

ISO'nun özellikle adli bilişim süreçleri için hazırladığı bu standartlar, daha özel detaylara sahiptir. Adli bilişim araştırmaları sırasında elde edilen değişik nitelikte verilerin (normal veriler, kişisel veriler, hassas veriler vb.) işlenmesi, korunması ve gizliliği noktasında ayrı düzenlemeler bulunmakla birlikte, bu verilerin

delil özelliği kazanarak soruşturma ve inceleme konusu olması dolayısıyla klasik prosedür uygulamaları için ayrı düzenlemeler yapıldığı görülmektedir.

2.3.1.1. ISO 27037 Standardı

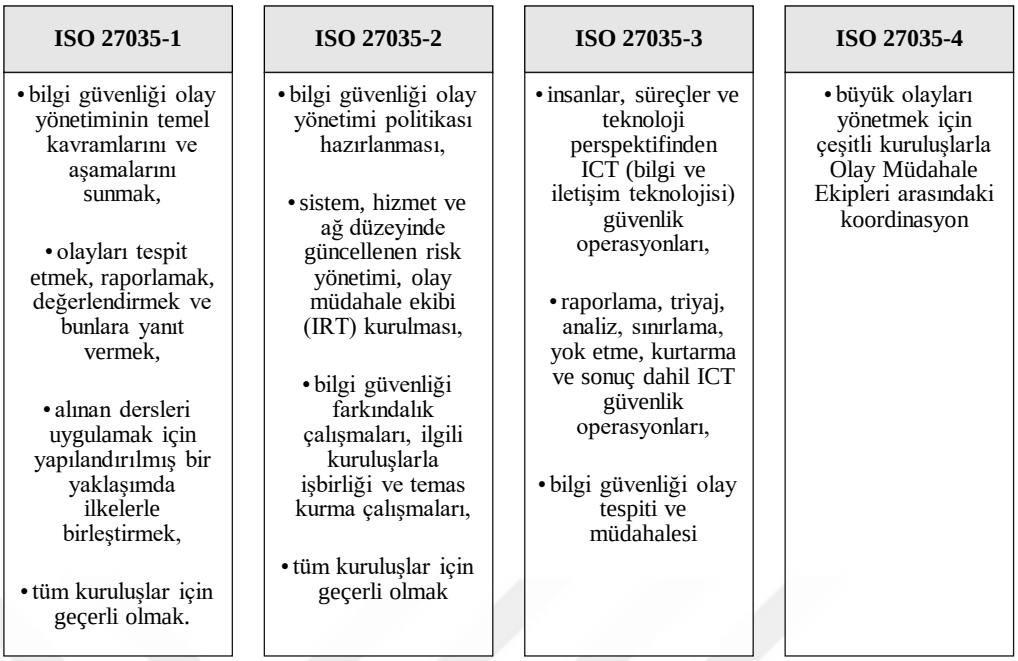
Üzerinde depolama üniteleri bulunan bilişim sistemlerinin analizindeki temel ilkeleri düzenlemektedir. Dijital delillerin tanımlanması, taşınması, analizi ve korunması faaliyetleri ile, delillerin bütünlüğünü herhangi bir müdahaleye karşı korumak, yerel ülke kanunları ve kurallarına uygun hareket ederek gerçekleştirmekle ilgili düzenlemeler içermektedir.

Bu kapsamda standart, adli laboratuvar yöneticileri, dijital delile ilk müdahale edenler (DEFR – *Digital Evidence First Responders),* dijital delil uzmanları (DES – *Digital Evidence Specialists*) ve olay müdahale uzmanlarına yöneliktir (Veber ve Smutny, 2015, s:296).

2.3.1.2. ISO / IEC 27035 Standardı

Bilgi güvenliği olay zincirini gözden geçirmekte, bir kuruluşun güvenlik olay yönetimini planlama ve oluşturma amacını gütmektedir. Delilleri sağlam, gerçek ve hukuka uygun hale getirecek önlemler üzerinde çalışmaktadır.

ISO 27035 dört bölüme ayrılmaktadır: 27035-1 “Olay Yönetim İlkeleri”, 27035-2 “Olay Müdahalesini Planlama ve Hazırlama Kılavuzu”, 27035-3 “Olay Müdahale Operasyonları Klavuzu” ve 27035-4 “Koordinasyon” (Şekil 2.18.):



Şekil 2.18. ISO / IEC 27035 Standardı Bölümleri

Bilgi güvenliği olay yönetiminde, önce hazırlık yaparak planlama, daha sonra tespit edip değerlendirmeler yapma ve en son karar verme aşamaları bulunmaktadır. Delillerin güvenli ortamlarda işlenip saklanması da bu standardın konusuna girmektedir çünkü bu standart da ISO 27000 serisine mensup olduğundan bahsi geçen sorumlulukları taşımaktadır.

2.3.1.3. ISO 27041 Standardı

"Bilgi güvenliği olaylarının araştırılmasında kullanılan yöntem ve süreçlerin 'amaca uygun' olmasını sağlamak için mekanizmalar hakkında rehberlik sağlar, gereksinimlerin tanımlanması, yöntemlerin açıklanması ve yöntem uygulamalarının gereksinimleri karşıladığının gösterilebileceğine dair kanıt sağlamaya yönelik en iyi uygulamaları içerir." (ISO/IEC 27041, 2015)

2.3.1.4. ISO 27042 Standardı

Bir bilgi güvenliği olayını araştırmak için kullanılabilecek dijital delillerin süreklilik, geçerlilik, tekrarlanabilirlik konularını ele alacak şekilde tanımlanması ve değerlendirilmesi için potansiyel dijital delillerin analizi ve yorumlanması konusunda genel çerçevede bir rehberlik sağlar. Araştırma ekibinin yetkinliğini ve yeterliliğini göstermek, karmaşık konuları anlaşılabilir bölümlere ayırmakla ilgilenir (ISO/IEC 27042, 2015)

2.3.1.5. ISO 27043 Standardı

"Olay öncesi hazırlıktan soruşturmanın tamamlanmasına kadar olan süreçleri ve bu tür süreçlerle ilgili genel tavsiye ve uyarıları içerir. Yönergeler, yetkisiz erişim, veri bozulması, sistem çökmeleri veya kurumsal bilgi güvenliği ihlalleri ve diğer dijital soruşturmalar dahil ancak bunlarla sınırlı olmamak üzere çeşitli soruşturmalar için geçerli süreçleri ve ilkeleri açıklar." (ISO/IEC 27043, 2015)

2.3.1.6. ISO 30121 Standardı

Kuruluşların yönetim organları için (sahipler, yönetim kurulu üyeleri, direktörler, ortaklar, üst düzey yöneticiler vb.) bir organizasyonu dijital araştırmalara başlamadan önce hazırlamanın yolunu sağlar (ISO/IEC 30121, 2015). Bu uluslararası standart, dijital delillerin kullanılabilirliği, erişimi ve maliyet etkinliği ile ilgili stratejik süreçlerin ve kararların geliştirilmesine uygulanır. Kurumsal sistem içinde dijital adli riskler için yönetim organının, performansı ölçme ile, ilkeler, süreçler ve en iyi uygulamalar için çerçeve çizme amacını taşır (Grobler, 2012, s:4).

2.3.2. Bilgisayar Kanıtı Hakkında Uluslararası Organizasyon – IOCE

ABD'nin federal, eyalet ve yerel kolluk kuvvetlerinin 70'e yakın temsilcisinin ve FBI üyelerinin katıldığı 1993 yılında yapılan "Bilgisayar Kanıtı Hakkında Uluslararası Kanun Yaptırımı Konferansı"ndaki tüm temsilciler adli bilişim standartlarının önemi, gerekliliği ve eksikliği konusunda fikir birliğine varmışlardı. Bu konferans her yıl farklı ülkelerde tekrar toplanarak sonunda IOCE'nin kurulmasıyla sonuçlandı (Whitcomb, 2002, s:2) ve 1997 yılında elektronik kanıtların değişimi ve kurtarılması için uluslararası standartların geliştirilmesi ile görevlendirildi.

IOCE, "bileşenlerini ilgilendiren konuları belirleyip tartışmak, bilginin uluslararası yayılımını kolaylaştırmak ve üye kurumlar tarafından değerlendirilmek üzere öneriler geliştirmek" amacı gütmekte ve üye kurumlar arasında iletişimi geliştirerek iş ilişkilerinin kurulmasına yönelik konferanslar düzenlemektedir (SWGDE, 1999).

1999'da Londra'da düzenlenen Uluslararası Yüksek Teknoloji Suçları ve Adli Bilişim Konferansı'nda (IHCFC - *International Hi-Tech Crime and Forensics Conference*), dijital delillerin ele geçirilmesi işlemlerinin standartlaştırılması için IOCE tarafından geliştirilen uluslararası ilkelerin aşağıdaki nitelikleri taşıması gerektiği kararlaştırılmıştır (SWGDE, 1999):

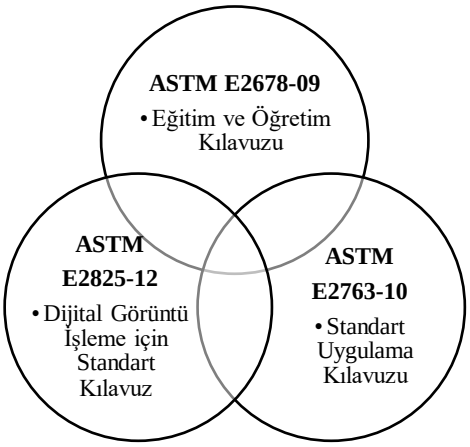
- Dayanıklılık;
- Ortak bir dilin kullanımı;
- Uluslararası sınırları geçme yeteneği;
- Kanıt bütünlüğünün sağlanması;
- Tüm yasal sistemlerle tutarlılık;
- Tüm adli kanıtlara uygulanabilirlik;
- Birey, kurum ve ülke dahil her düzeyde uygulanabilirlik;
- Araçların, tekniklerin ve eğitimin doğrulanması ile uluslararası akreditasyon konusunda adli uzmanlık ve anlaşma oluşturma ihtiyacı;

- Dijital kanıtların incelenmesine yönelik uygulamalar ve prosedürlerle ilgili sorunlar;
- Etkinlikler, araçlar ve teknikler gibi yüksek teknoloji suçları ve adli bilişimle ilgili bilgilerin paylaşımı.

2.3.3. ASTM International

Tarihi 1898'lere kadar giden ve 1902 yılında kurulduğunda "*American Society for Testing and Materials*" olarak bilinen ASTM International, çeşitli ürünleri, hizmetleri, malzemeleri ve sistemleri, geliştirilmiş teknik standartlar altında toplayan uluslararası bir standartlar kuruluşudur. Standart "International" olarak adlandırılmakla birlikte, Amerika Birleşik Devletleri'ndeki adli bilişim uygulamaları için ulusal özellikli standartlar sınıfına girmektedir. ASTM, "ürün, hizmet ve malzemeler için kaliteyi iyileştirmek, güvenliği artırmak, pazara erişimi kolaylaştırmak, ticareti yaygınlaştırmak ve tüketici güveni sağlamak" amacında olduğunu ve yaklaşık 13.000 ASTM standardının bu amaçlarla oluşturulduğunu belirtir (ASTM, 2021).

Bunların içinden adli bilişimle alakalı olan ve önemli görünen standartlar şunlardır:



Şekil 2.19. ASTM Standartları

2.3.3.1. ASTM E2763 -10 Standardı

"Bu standart bir ceza soruşturmasında uygulanacak adli bilişim teknikleri ve prosedürlerini açıklamakla birlikte, medeni hukuk davalarına da uygulanabilmektedir. Dijital delillerin ele geçirilmesini, uygun şekilde işlenmesini, dijital görüntüleme, adli analiz/inceleme, dökümantasyon ve raporlamayı açıklamaktadır." (ASTM E2763-10, 2019).

2.3.3.2. ASTM E2825 – 19 Standardı

"Bir mahkemede kanıt olarak kullanılmak üzere kaliteli adli görüntülerin üretimini sağlamak için dijital görüntü işleme yönergeleri sağlar ve üç kategoride görüntü işleme ve ilgili yasal hususları ele almaktadır: Görüntü geliştirme, Görüntü onarımı ve Görüntü sıkıştırma." (ASTM E2825 – 19).

Diğer ASTM standartları "Sertifikasyon" bölümünde açıklanacaktır.

2.3.4. İngiliz Standartlar Enstitüsü - BSI

Avrupa Kıtasına gelindiğinde, Birleşik Krallıkta BSI'ın BIP 0008 serisi ile BS 10008:2008 standardı önemli standartlardandır. **BIP 0008;** İngiliz Standartlar Enstitüsü tarafından 1996 yılında yayınlanmış; orijinallik ile dökümanların yönetimi, taranması, arşivlenmesi ve saklanması süreçlerinde atılması gereken adımlar ve bağlılığın ispat edilebilirliği temel ilkeler olarak kabul edilmiştir (BSI BIP 0008, 1996). Standart, diğerlerinde de belirtildiği gibi, genel gereksinimlere uygun olarak, her tür kuruluş tarafından kullanılabilecek ve her türden elektronik bilgiye uygulanabilecek şekilde hazırlanmış olup, üç uygulama kuralını kapsamaktadır (Li ve ark., 2015, s:47):

Şekil 2.20. BIP 0008 ve 0009 Standartları

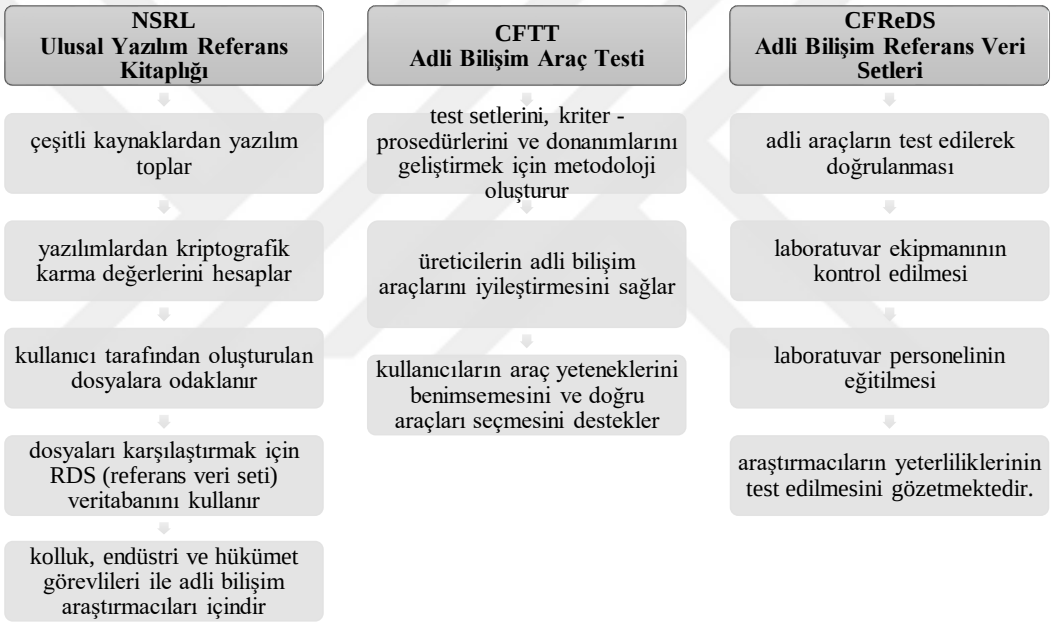
BS 10008; "bilgilerin depolanması ve aktarımı da dahil olmak üzere elektronik bilgi yönetim sistemlerinin uygulanması ve çalıştırılması için en iyi uygulamaları özetleyen İngiliz Standardıdır. Bilgi depolamanın yasal güçlüklerinden kaçınmak için, tüm bilgilerin doğrulanmasına yardımcı olmak amacıyla tasarlanmıştır (BSI BS 10008, 2020) ve temeli BIP 0008 İngiliz Standardı (Yasal Kabul Edilebilirlik ve Kayıt Tutma İçin İngiliz Yasası - *British Code for Legal Admissibility and Record Retention*)'na dayanmaktadır. Denetim ve yönetim incelemeleri dahil, sistem izlemeleri, bakımı ve iyileştirilmesi konularıyla birlikte, elektronik imza, elektronik kimlik ve elektronik telif hakkı konularını da içerir (BSI BS 10008, 2008).

2.3.5. Ulusal Standartlar ve Teknoloji Enstitüsü - NIST

1901 tarihinde, ülkenin bilim adamları ve sanayicilerinin yetkili yerel ölçüm ve standartlara olan ihtiyaçları, ABD'de NIST (*National Institute of Standards and Technology*)'in kurulmasına sebep olmuş, elektrik, uzunluk, kütle, sıcaklık, ışık ve zaman standartları oluşturularak, bunların halka aktarımı için bir sistem yaratılmıştır (NIST, 1901). Sonraki süreçte, teknoloji çağına atılan adımla birlikte, NIST, bilgi

güvenliğini sağlamak için standartlar ve yönergeler geliştirerek yoluna devam etmiştir.

NIST'in araştırmacılar için kaynak sağlayan üç adli bilişim projesi bulunmaktadır: ticari yazılım paketleri ile bu paketlerdeki her dosyaya ilişkin veri tabanı içeren NSRL; araç özelliklerini, test prosedürlerini, test setlerini ve donanımını kullanan adli bilişim yazılım araçlarını test etmek için metodoloji oluşturan CFTT; araştırmacılara inceleme için belgelenmiş simüle edilmiş dijital kanıt setleri sağlayan CFReDS (Şekil 2.21.) (Lyle ve ark., 2008):



Şekil 2.21. NIST Projeleri (NIST, 2018 ve NIST CFReDS Project, 2019)

Silinmiş dosyaları kurtarma ve adli görüntüleme araçlarının yanı sıra, çeşitli yazılım yazma ve donanım yazma blok cihazları hakkında test raporları yayınlamaktadır (Lyle ve ark., 2008). NIST Bilgi Teknolojisi Laboratuvarı (ITL - *The Information Technology Laboratory*) ise, bilişim sistemlerinin verimli şekilde kullanılması ile test uygulamaları ve teknik analizler geliştirerek, elde edilen bilgilerin uygun maliyetli gizliliği ve güvenliğini sağlamak için fiziksel, teknik, idari

ve yönetim standartlarının ve yönergelerinin oluşturulmasını sağlama sorumluluğu altındadır (Kent ve ark., 2006).

2.4. Laboratuvar Akreditasyon Standartları

Sınır ötesi nitelikli bilişim suçlarında tüm ülkelerde senkronizasyonun sağlanması amacıyla modellerin, prosedürlerin, en iyi uygulama rehberlerinin ve standartların oluşturulması, adli bilişim araştırmalarının en önemli süreçlerinden biri olan analiz sürecinin belkemiği niteliğindeki laboratuvarların akreditasyonunu zorunlu kılmaktadır. Usulüne uygun ve tüm teknik ve hukuki kurallara uyarak toplanan ve muhafaza edilen delillerin, adli makamlar önüne çıkarılmadan evvel derinlemesine ve eksiksiz incelenmesi laboratuvarlarda kullanılan yazılım ve ekipmanların yetkinliğine, becerisine ve güvenirliğine dayanmaktadır. Bu sebeple bu laboratuvarlardaki uygulamalar için de standart ihtiyacı doğmuş ve ilkeler oluşturulmuştur.

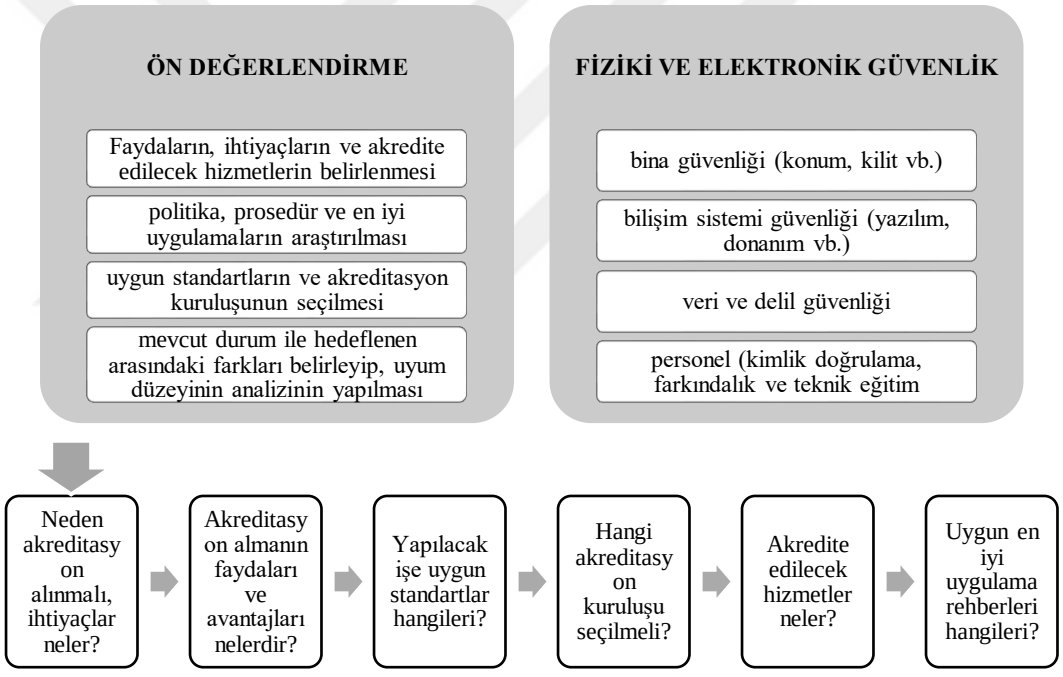
Akreditasyon; laboratuvarın verdiği hizmetin kalitesinin, yeterliliğinin, tarafsızlığının ve uyumluluğunun tanınmış standartlara göre sertifikalı bağımsız bir kuruluş tarafından değerlendirilmesidir (SWGDE, 2017a).

Adli bilişim uzmanları uzmanlıklarını, aldıkları eğitim ve sertifikalarla kanıtlarken, laboratuvarlar da ekipmanlarının, operasyonlarının, fiziki tesislerinin, güvenlik ve sağlık prosedürlerinin tümünün ulusal ve uluslararası standartları karşıladığını akreditasyona sahip olmasıyla kanıtlamaktadır (SWGDE, 2017b).

Bir laboratuvar öncelikle kendi içinde ön değerlendirme yaparak kendini akreditasyon sürecine hazırlamakta, akreditasyon standartlarına uygun önlemler alıp hazırlıklar yapmaktadır (Şekil 2.22.) Bu noktada, laboratuvarlar için kontrol listeleri, kullanım kılavuzları, kalite süreci belgeleri ve eğitim rehberleri hazırlanmalı, teknolojik gelişmeler ve yeni üretilen yazılımlar takip edilmeli, laboratuvardaki

eksiklikler tespit edilip tamamlanmalıdır. Sonrasında, laboratuvar bağımsız bir akreditasyon kuruluşuna başvurmakta, akreditasyon kuruluşu tarafından bu başvuru değerlendirilerek denetlenmekte ve nihayetinde laboratuvar akredite edilmektedir.

Adli bilişim incelemelerinde kullanılan, donanım ve yazılımların verilen hizmete uygun olduğu, kullanılan cihazlar, ekipmanlar ve hatta metotların denetlendiği, güvenilir yöntemlerle analiz yapıldığı, çalışan her seviyeden personelin yetkinliği ve belirli görevleri yerine getirmeye yetkili olduğu, yapılan inceleme neticesinde laboratuvarın akredite edilmesiyle birlikte resmi olarak ispatlanmış sayılmaktadır.



Şekil 2.22. Laboratuvarların Akreditasyona Hazırlığı (SWGDE, 2017a)

Laboratuvar akreditasyon kuruluşu oluşturmanın maliyeti, büyüklük, kapasite, istihdam ve ekipman çeşitliliğine bağlı olarak değişiklik gösterebilmektedir. Bir laboratuvarın akreditasyon alması, yetkinlikleri, güncellikleri ve eksiklikleri noktasında kendilerini sürekli olarak denetleyip gözden geçirdikleri ve yenileyip geliştirdikleri bir sürece girmeleri anlamına gelmektedir (SWGDE, 2017b).

Şekil 2.22.'de de gösterildiği üzere, laboratuvarların akreditasyonlarının sağlanması konusunda dikkate almaları gereken hususlar bulunmaktadır. Bunlar:

- **Fiziki Güvenlik**

Olayla bağlantılı olduğu düşünülen ve hassas özelliklere sahip dijital delillerle fiziksel delil niteliğindeki verileri depolamak ve araştırmak için kurulan laboratuvarların yeterli güvenliğe sahip olması, izinsiz ve yetkisiz girişleri önleyecek yapılara ve sistemlere sahip özelliklerde kurulması gerekmektedir. Delillerin korunması asıl amaç olarak görülse de, gerek olayla ilgili kişilerin, gerek araştırmacı ve uzmanların, gerekse çalışan personelin kişisel bilgileri, kişisel verileri ve araştırmalarda kullanılan yazılım ile donanımların güvenliği de başka açılardan korunması gerekenler arasındadır. Güvenlik en basit haliyle güçlü fiziksel kilitlerden, elektronik tuş takımları, elektronik kartlar, CCTV ve biyometrik teknolojilere kadar farklı yöntemlerle sağlanabilir. Delillerin ve verilerin bulunduğu odalara, giriş ve çıkış kapılarına alarm sistemleri kurulabilir, pencereler için de güçlendirici ekipmanlar takılabilir, öyle ki, pencerelerin olabildiği kadar az sayıda olması veya hiç olmaması tavsiye edilir (COE, 2017). Elbette tehlike sadece insan faktörüyle sınırlı değildir, elektrik sisteminin devre dışı kalması, yangın veya deprem gibi olayların gerçekleşme ihtimali de göz önüne alınarak önlemler hazırlanmalıdır. Kurulacak laboratuvarın fiziksel konumu, delillerin binaya taşınması, yapının fiziki dayanıklılığı, herhangi bir saldırıya karşı koyma durumu gibi pek çok faktörün düşünülmesi ve uygun bir binanın tasarlanması oldukça önemlidir.

- **Elektronik Güvenlik**

Adli bilişim analizlerinde kullanılan yazılımların, incelenecek cihaz, gereksinimler, kullanım kolaylığı ve delil güvenliği açısından iyice araştırılması ve lisanslı olanların tercih edilmesi tavsiye edilmektedir. Gerekli yazılımsal, donanımsal ve ekipmansal ihtiyaçları belirleyip temin etmek, bunların tamiri, bakımı ve

güncellenmesi, kalite kontrol ve yönetim politikaları konusunda da gerekli özen gösterilmeli ve bunlarla ilgili politikalar oluşturulmalıdır, çünkü adli bilişim analizlerinin kalitesi ve güvenirliği, önce bağlı olduğu yapının kalitesi, güvenirliği ile sektör içindeki ve dışındaki imajından etkilenmektedir. Laboratuvarın tümünün yönetimi ile harici iş ve işlemlerin yapılması noktasında da yetkin ve uzman personele ihtiyaç devam etmektedir.

- **Veri Güvenliği**

Adli bilişim laboratuvarında, bir veri saklama politikasına sahip olmak önemlidir, çünkü verileri depolamak için yeterli alanın belirlenmesi, prosedürlere ve yasal düzenlemelere uyumunun tespit edilmesi açısından politikalar yol göstericidir (COE, 2017). Elde edilen tüm veriler gerçek ve tüzel kişilere ait bilgilerden oluşmakta, analiz için toplanan bu veriler veri koruma hukuku nazarında farklı düzenlemelere tabi olmaktadır.

- **Personel Eğitimi**

İnsan gücü tüm işlemleri yapma konusunda kilit faktördür, dolayısıyla, yapılan işin önemi ve değeri, bilgi ve beceri gereksinimleri, dikkat ve özen yükümlülükleri, kurallara ve yasalara uyum konusundaki zorunlulukları konularında, alt kademeden üst kademeye kadar tüm insan faktörünün eğitimi ve bilinçlendirilmesi, tüm işlemlerin başarısı açısından aslında en önemli faktördür. Kullanılan yazılım, donanım ve materyallerin üretiminden başlayan bu sorumluluk, yapılacak tüm işlemler, alınacak tüm önlemler ve uyulacak tüm kurallar bakımından yine insan faktörüne kalmış durumdadır.

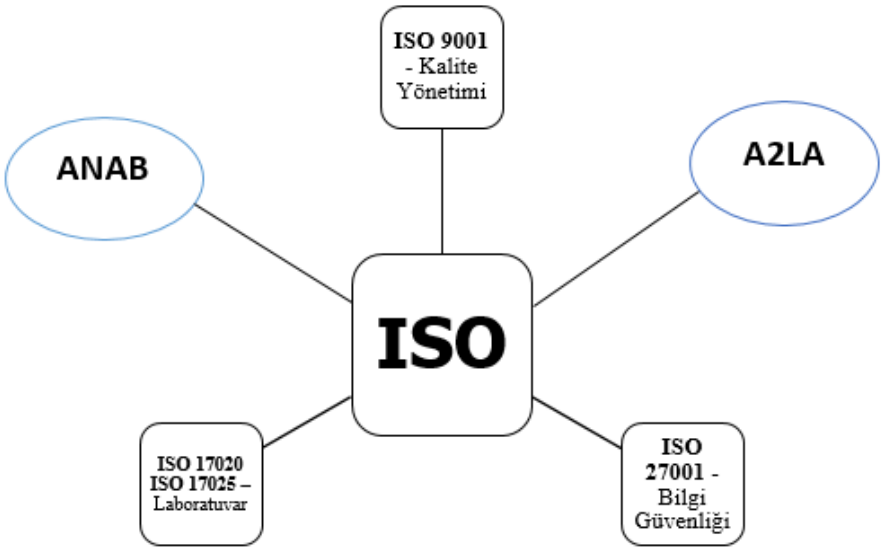
- **Dış Müdahaleler**

Soruşturmalar gerçek veya tüzel kişilerle ilgili olabileceği gibi, basit veya organize suçları kapsayan, örgüt veya terörist faaliyetlerinin söz konusu olabileceği

geniş yelpazeli suç tipleriyle ilgili de olabilir. Yapılan analizlerin ve çıkarılacak sonuçların kapsamı önem derecesine bağlı olarak müdahale sonucunu doğurabilir. Bu sebeple, yönetimin, uzmanların, analistlerin ve personelin yapılan işin bağımsızlığını, dürüstlüğünü, şeffaflığını ve kalitesini olumsuz yönde etkileyebilme potansiyeli olan her türlü mali, siyasi, ticarî ve benzeri müdahalelerden uzak tutulmasını sağlayacak düzenlemelere sahip olması zorunluluktur. Aynı durum, laboratuvar bünyesinde gerçekleştirilen işlemler açısından da geçerli olup, yapılan işin hukuka uygunluğuna gölge düşürecek her türlü güven zedeleyici davranışa karşı yaptırımlar belirlenmelidir. Söz konusu bu laboratuvarların kamu sektörü veya özel sektör bağlantılı olması sonucu değiştirmeyecektir. Çünkü çıkan sonucun rapor halinde adli makamlara sunumu, suçun veya suçsuzluğun ispatı ve adaletin sağlanması noktasında büyük sorumluluklar taşımaktadır.

Laboratuvar Akreditasyonuyla ilgili uluslararası nitelikli standartlar ve en iyi uygulama rehberleri oluşturularak, hem ülkelerin ve kuruluşların iç düzenlemelerini uyumlaştırmaları hem de herkes açısından aynı yol haritasının çizilmesi amaçlanmıştır. Bu kapsamda uluslararası nitelikli standartlar olarak ISO 9001 - Kalite Yönetimi, ISO 27001 - Bilgi Güvenliği, ISO 17020 ve 17025 – Laboratuvarlar için düzenlenmiş standartlar olup (SWGDE, 2017b) ISO 17020 dijital laboratuvarlar tarafından seçilen temel standarttır.

Kuruluşlar ise, ANSI-ASQ Ulusal Akreditasyon Kurulu (ANAB - *National Accreditation Board*) ve Amerikan Laboratuvar Akreditasyonu Derneği (A2LA - *American Association for Laboratory Accreditation*) olarak belirlenmektedir çünkü günümüzde özellikle bu kuruluşlar kabul görmektedir (Şekil 2.23.).



Şekil 2.23. ISO Laboratuvar Akreditasyon Şeması

2.4.1. ISO / IEC 17025 "Test ve Kalibrasyon Laboratuvarlarının Yeterliliği İçin Genel Gereksinimler"

Laboratuvarların test işlemlerini gerçekleştirmeleri için uymaları gereken genel şartları ve sahip olmaları gereken yetkinlikleri açıklayan, tarafsızlık ve bağımsızlığa odaklı, uluslararası bir standarttır. Bu standart, izlenmesi gereken ilgili yönetim stratejisini, laboratuvarda çalışan personel ile ilgili süreci, laboratuvarın riskleri ve fırsatları ele almak için gereken eylem planını, testlerin farklı kişiler tarafından, farklı yerde ve farklı zamanda yapılsa bile aynı sonucu vermesini sağlamaya yöneliktir.

Standarda sahip olmanın; analizlerin kalite düzeylerini arttırma, kaynakları iyileştirme, yazılımların, cihazların ve materyallerin düzenli kontrol edilmesi, bakımlarının ve güncellemelerinin yapılması, uzmanların ve personellerin yeteneklerinin geliştirilmesi, eğitimlerinin sürekliliği gibi pek çok faydası bulunmaktadır.

Bu standart, tüm laboratuvar türleri için hazırlanmış genel bir standart olup, özellikle adli bilişim laboratuvarlarına uygulanabilen, Birleşik Krallık Adli Bilim

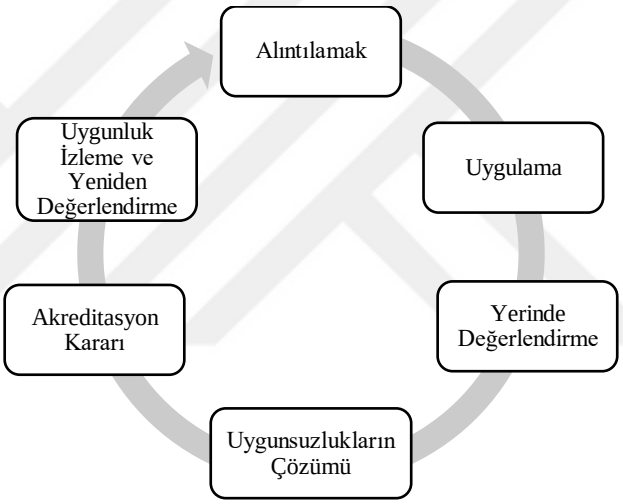
Düzenleyicisi (*UK Forensic Science Regulator*) ve ABD ASCLD / LAB tarafından tercih edilen bir standarttır.

Şekil 2.24. ISO 17025 Kalite Gereksinimleri (Ponciano, 2021)

17025 akreditasyon sürecinde laboratuvar kurulmasında belirli aşamalar söz konusudur. Öncelikle başlangıç hazırlıklarıyla başlanır; hedeflenen konular, kapsam, organizasyon şeması, çalışma ortamı, çalışma ekibi ve çalışma planı gibi mevcut durum analiz edilerek gereksinimler tespit edilir (Şekil 2.24.), standardın açıklanması, aşamaların anlatılması ve personelin bilgilendirilmesi ve eğitilmesi sağlanır. Talimatlar, prosedürler, kalite rehberleri ve organizasyon el kitabı hazırlanır. Laboratuvarın kurulduğu yer, mekan, çevre ve iklim koşulları, binanın fiziki ve yapısal özellikleri önemle dikkate alınır, çalışma ortamının bina ve çevre koşulları açısından iyileştirilmesi, yazılımların güncellenmesi, donanım ve ekipmanların bakımı sağlanır. Gerekli denetimler yapılır, eksiklikler tespit edilir, öneriler hazırlanır ve rapor oluşturulur. Tüm laboratuvar sisteminin hazır olduğuna kanaat getirildiğinde gerekli başvuru yapılır.

2.4.2. ISO / IEC 17020 "Uygunluk Değerlendirmesi - Muayene Yapan Çeşitli Kuruluş Türlerinin Çalışması İçin Gereksinimler"

Standart, kuruluşların verdikleri hizmetlerin gerek müşteriler gerekse denetim yapan yetkililer nezdinde kabul görmesi ve güvence altına alınması için bu kuruluşların uymaları gereken genel kriterleri belirler ancak kalite yönetim sistemi sertifikasyonunu kapsamaz. Standardın kapsamına süreçler, prosedürler, ürünlerin, malzemelerin ve hizmetlerin kalitesi ile kullanıma uygunluğu, kullanılan sistemler ile işletilen tesislerin güvenliği gibi çok sayıda faktör dahil edilmektedir (ISO, 2021). Bu kapsamda, standardın akreditasyon şeması Şekil 2.25.'deki gibi düzenlenmiştir:



Şekil 2.25. ISO / IEC 17020 Akreditasyon Şeması (ANAB ANSI, 2021)

Akredite edilmiş bir muayene kurumu, yapılacak muayeneler için gerekli nitelikleri, eğitimi, deneyimi ve bilgi seviyesini tanımlamalı ve belgelemelidir. Hem yöneticilerin, hem de teknik ve idari personelin görevlerini ve yetki sınırlarını açıkça gösteren güncel bir organizasyon şeması hazırlamalıdır. Bu kişilere gerekli eğitimin verilmesi ve görev bilincinin aşılanması, yasal hususlar ile gizlilik hükümlerinin sözleşmelerle imza altına alınması gereklidir (IPAC, 2019).

Akredite kuruluşları standarttaki gereklilikler uyarınca, sorumluluklarının farkında olarak risk analizleri yapmak, yükümlülüklerini belirlemek ve faaliyet

gösterdiği alanlardan kaynaklanan yasal veya teknik düzenlemeleri dikkate almak zorundadır.

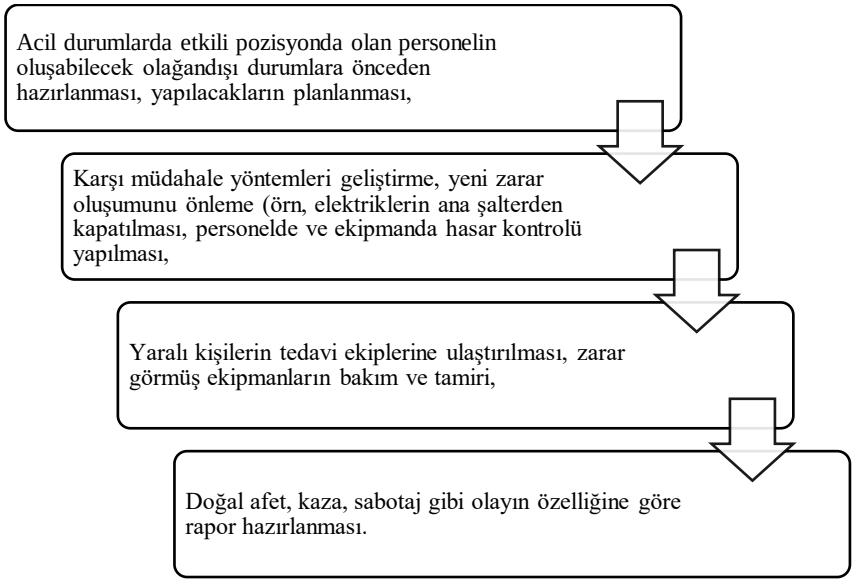
2.4.3. ISO / IEC 27001 "Bilgi Güvenliği Yönetim Sistemleri – Gereksinimleri"

Standart, bilgi güvenliği yönetim sistemlerinin (ISMSs - *information security management systems*) kurulması, yönetilmesi, gözden geçirilmesi, iyileştirilmesi ve sürdürülmesi için yöntemler belirlemekte, bilginin gizliliği ve güvenliği, bilgiye erişilebilirliğin ve değişmezliğinin sağlanması, uygulanan yöntemlerin doğruluğunun ve bütünlüğünün korunması, zayıflıkların ve eksikliklerin giderilmesi ile risklerin minimize edilmesi gibi konularını hedeflemektedir.

Standart, Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) "Bilgi Sistemleri ve Ağlarının Güvenliği Kılavuzları (2002)"nda da kendine yer bulan, bir ISMS'nin yönetimi, güncelliği ve sürdürülebilirliği için "Planla-Uygula-Kontrol Et-Önlem Al" modelini kullanır.

Kurumlar, şirketler ve laboratuvarlar gibi ilgili kullanıcılar, güvenlik sistemlerinin etkili çalışmasını sağlamak için, standartta işaret edilen 'bilgi güvenliği yönetim sistemi'ni kurarak risklerini saptayabilmeli, bu risklerin giderilmesi, sistem açıklarının ve sisteme yönelik tehlikelerin önlenmesi için gereken prosedür ve politikaları oluşturabilmeli ve teknolojileri işletebilmelidir (TSE 27001, 2021).

ISO 27001 yangın, deprem gibi doğal afetler ile kaza, enerji kesintisi gibi öngörülemeyen veya olağanüstü durumlarda, doğabilecek zararların oluşmasını engellemek ya da en aza indirmek adına uygulanmak üzere acil eylem planı oluşturmuş ve şu hususları ele almıştır (Şekil 2.26.):



Şekil 2.26. ISO 27001 Acil Eylem Planı

Herhangi bir saldırı hali veya veri sızdırılması gibi durumlar söz konusu olduğunda, tüm personel, sistemlerdeki zayıflıkların ve söz konusu ihlallerin farkına vardıkları anda geciktirmeden bilgi güvenliği yöneticisine bilgi vermek zorundadır. Bu hususta çalışanların sorumlulukları, alacakları önlemler, yapmaları ve yapmamaları gereken davranışlar konusunda bilgilendirilmeleri gerekir.

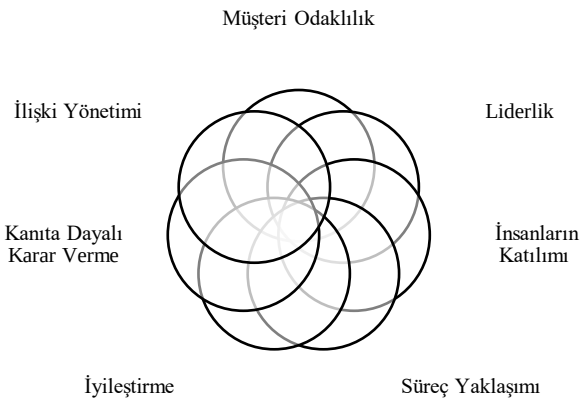
2.4.4. ISO / IEC 27002 "Bilgi Güvenliği Kontrolleri İçin Uygulama Kuralları"

Organizasyonun bilgi güvenliği risk ortamlarını dikkate alarak bilgi güvenliği yönetiminin tanıtılması ve uygulanmasından, sürdürülmesine ve geliştirilmesine kadar bilgi güvenliği standartları ve yönetimi uygulamaları için yönergeler içerir. Standart; güvenlik politikalarının oluşturulması, güvenlik organizasyonlarının kurulması, çalışan insan gücünün yönetimi ve eğitilmesi, iç ve dış çevre koşullarının iyileştirilmesi, güvenliklerinin sağlanması, erişim kontrolünün edinilmesi, risk değerlendirmesi yapılması ve ihlal prosedürlerinin hazırlanması, işgücü sürekliliği, varlık yönetimi, teknik ve yasal düzenlemelere uygunluk amaçlarını taşımaktadır.

2.4.5. ISO 9001 "Kalite Yönetim Sistemleri - Gereksinimler"

Kalite Yönetim Sistemlerinin kurulması esnasında uygulanması gereken teknik ve yasal şartların tanımlandığı ve belgelendirme denetimine tabi olan bu standart, küreselleşmeye bağlı değişim ve gelişime ayak uydurmak, beklentileri karşılamak ve bilgiye erişimi kolaylaştırmak gibi amaçlarla, belli aralıklarla gözden geçirilerek ihtiyaçlar doğrultusunda revize edilmekte ve ilgili taraflar için kullanışlı hale getirilmektedir (TSE 9001, 2015).

Tasarımdan üretime, kurulumdan çalıştırılmaya, geliştirilmeden servis işlemlerine kadar ürün, malzeme ve hizmetlerde ilgili kuruluşlar için kalite planlaması ve güvencesi ile kalite kontrol işlemlerinin sağlanması, kullanılan yazılım ve donanımlarda uygunluk, güncellik ve başarı özelliklerinin arttırılması, yapılan işlemlerde gerçeklik, doğruluk, belirlilik, ölçülebilirlik, ulaşılabilirlik ve zamana bağlılık şartlarının sağlanması, eksik, yanlış ve hukuka aykırı eylemleri önleyici ve düzeltici faaliyetlerin oluşturulması hedeflerini taşımaktadır.



Şekil 2.27. ISO 9001'in Kalite Yönetim İlkeleri (ISO 9001, 2019)

Şekil 2.27.'de de gösterildiği üzere, akreditasyon sürecinin özellikleri, yapılan işlemlerin sonuçları ve kuruluşun hedeflerine yönelik kapsamlı bir yaklaşım geliştirmek; iç ve dış ortamlardaki değişiklikleri iyi gözlemleyerek gerekli reaksiyonları zamanında gösterebilmek; müşterilerin ihtiyacını karşılayarak güvenlerini kazanmak ve onları korumak; temas kurulan ve beraber iş yapılan gerçek ve tüzel kişilerle olan ilişkileri sürdürebilmek; her kademede yer alan personelin eğitimli ve yetkin olmasını sağlamak; elde edilen verilere dayalı gerekli ve doğru kararlar vermek ve belirlenen riskleri bertaraf etmek; tüm süreçleri uyumlu, verimli ve üretken şekilde yürüterek başarıyı yakalamak standardın oluşturduğu kalite yönetim ilkeleridir.

Uluslararası Laboratuvar Akreditasyon Birliği (ILAC – *International Laboratory Accreditation Cooperation*) kendisini "dünya çapındaki akreditasyon kuruluşları ve paydaş kuruluşlardan oluşan bir üyeliğe sahip, test ve kalibrasyon laboratuvarları, muayene kuruluşları ve diğer kuruluş türlerinin dünya çapında yeterlilik ve eşdeğerlik gösterimini destekleyen altyapıyı sağlayan, laboratuvar ve denetim kuruluşu akreditasyonu konusunda uluslararası otorite" olarak tanımlamaktadır.

Adli tıp sürecine bir bütün olarak yaklaşan ve hem ISO / IEC 17020 hem de ISO / IEC 17025 için ortak rehberlik sağlayan tek bir üst düzey belgenin oluşturulması amacıyla, Avrupa Akreditasyon Birliği (EA - *European Accreditation Association)* ve Avrupa Adli Bilim Enstitüleri Ağı (ENFSI - *The European Network of Forensic Science Institutes*) (EA-5/03) tarafından adli laboratuvarlar için ILAC G19 hazırlanmıştır (ILAC, 2014).

2.4.6. ILAC-G19:2002 "Adli Bilim Laboratuvarları İçin Kılavuz"

Standart, adli analiz ve incelemeye katılan laboratuvarlar için ISO / IEC 17025 kapsamında işlem sağlamakta, kuruluşların laboratuvarlarının değerlendirilmesi ve

akreditasyonu için kriterler oluşturmaktadır. Adli bilişim adli bilimlerin bir alt dalı olarak kabul edildiği için, söz konusu kurallar uygun düştüğü ölçüde bilişim suçlarıyla ilgili vakalara da uygulanabilecektir.

Adli laboratuvar, soruşturma altındaki olayla ilgili belgeleri, kayıtları, test/muayene sonuçlarını, fotoğrafları, telefon görüşmesi kayıtlarını, makbuzları vb her türlü delil niteliğinde materyali belgeleme prosedürüne sahip olmalı, yapılan her işlemin sonucu, işlemi yapan kişinin haricindeki kişilerce tekrarlanabilecek ve yorumlanabilecek özellikte olmalıdır. Bu kapsamda analiz sırasında yapılan çalışmalar kaydedilmeli, gözlemler, test sonuçları fotoğraf veya elektronik formatta saklanmalı, test raporları dahil olmak üzere vaka kayıtları işlem yapan personel dışında en az iki kişi tarafından kontrol edilmeli, bu kontrollerin kimler tarafından yapıldığı kaydedilmeli, tüm bu hususlara ilişkin politika ve prosedürler belirlenmelidir (ILAC, 2002).

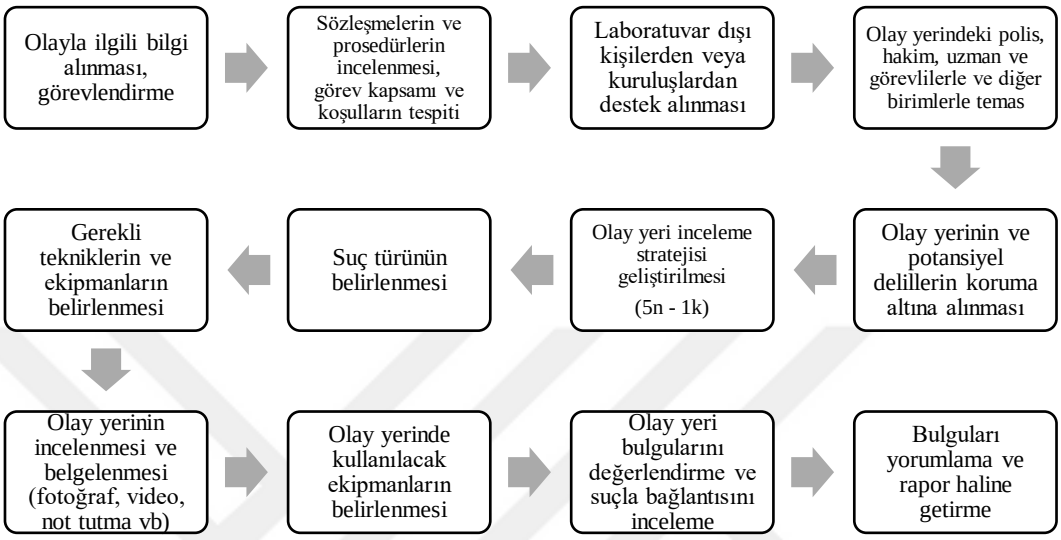
2.4.7. ILAC-G19: 08/2014 "Adli Bilim Sürecinde Modüller"

Bu rehber de özünde hem ILAC G-19 hem ISO 17020, hem de ISO 17025 ile benzer düzenlemeler içermekle birlikte, özellikle ISO 17020 standardına daha yakın durmaktadır.

Standart kapsamında laboratuvardaki genel düzenlemeler özetle şu şekilde belirtilmiştir (ILAC, 2014):

- İş ile ilgili tüm belgelerin kontrolü
- Çalışan personelin davranış kuralları, eğitimi ve yeterliliği
- Adli bilişim kayıtlarının oluşturulması ve muhafazası
- Çalışan personele sağlıklı ve güvenli bir çalışma ortamı sunulması
- Adli bilişim aşamalarıyla ilgili iç denetimlerin yapılması
- Uygun olmayan muayene, test ve yöntemlerin tespit edilmesi

- Kalite kontrol prosedürleri dahil tüm yöntemlerin doğrulanması, belgelenmesi
- Laboratuvar içindeki ve dışındaki çevre koşullarının iyileştirilmesi



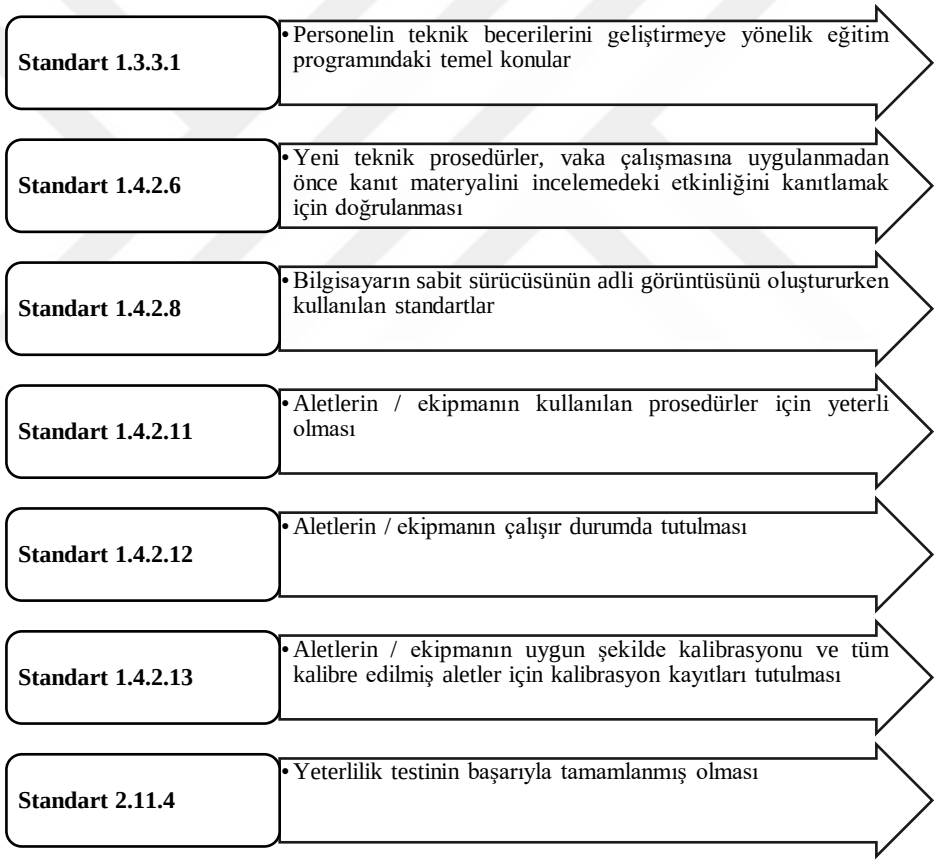
Şekil 2.28. ILAC-G19: 08/2014 Adli Soruşturma ile İlgili Düzenlemeler

Standartta, laboratuvarlarla ilgili genel düzenlemelerin yanında adli bilişim süreçleriyle ilgili de genel adli tıp prosedürüyle benzer düzenlemeler yapıldığı görülmektedir. Olayla ilgili bilginin alınmasıyla başlayan bu süreç, Şekil 2.28.'de gösterilen akışa uygun olarak yapılan analiz sonucunda elde edilen bulguların görevli makamlara sunumuyla sona ermektedir. Bu kapsamda standart önceki anlatılanlarla benzer noktalara değinerek farklı bir husus ortaya koymamaktadır.

Laboratuvar akreditasyonlarına ek olarak, adli bilişim süreçleriyle alakalı ama laboratuvarlarla ilgili hususları da destekleyici, birçok sektörün aşina olduğu diğer ilgili standartların da bu bölüme eklenmesi faydalı olacaktır.

2.4.8. Amerikan Suç Laboratuvarı Yöneticileri / Laboratuvar Akreditasyon Kurulu - ASCLD / LAB

ASCLD / LAB, kar amacı gütmeyen, dünyadaki en eski suç / adli tıp laboratuvarı akreditasyon organıdır ve şu anda Amerika Birleşik Devletleri'ndeki çoğu federal, eyalet ve yerel suç laboratuvarlarının yanı sıra dünyadaki adli tıp laboratuvarlarının çoğunu akredite etmektedir. 2008'den bu yana Inter Amerikan Akreditasyon İşbirliği (IAAC - *Inter American Accreditation Cooperation*) ve 2009'dan bu yana ILAC tarafından adli bilimler alanında ISO / IEC 17011 ile uyumlu bir akreditasyon kuruluşu olarak tanınmaktadır (Flashback Data, 2013).



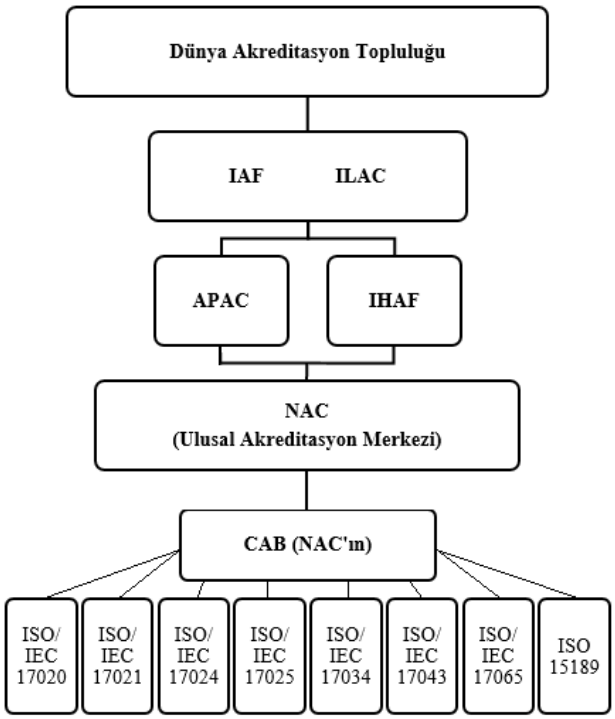
Şekil 2.29. ASCLD Standartları (Barbara, 2006)

ASCLD / LAB Kılavuzundan Bazı Standart Örnekleri Şekil 2.29.'da gösterilmekte olup, kanıtların elde edilmesinden incelenmesine, alet

kalibrasyonlarından personel yeterliliğine kadar adli bilişimi ilgilendiren konularda standartlar sözkonusudur.

2.4.9. Asya Pasifik Akreditasyon İşbirliği – APAC

APAC (*Asia Pacific Accreditation Cooperation*) 2019'da iki eski bölgesel akreditasyon işbirliğinin - Asya Pasifik Laboratuvar Akreditasyon İşbirliği (APLAC - *Asia Pacific Laboratory Accreditation Cooperation* 1992) ve Pasifik Akreditasyon İşbirliği'nin (PAC - *Pacific Accreditation Cooperation* 1995) birleşmesi ile kurulmuş olup, Uluslararası Akreditasyon Forumu (IAF - *International Accreditation Forum*) ve ILAC tarafından tanınan bir bölgesel işbirliğidir (APAC, 2021) (Şekil 2.30.).



Şekil 2.30. APAC ve Bağlı Kuruluşlar (APAC NAC, 2019)

APAC, üyeleri tarafından akredite edilmiş laboratuvarlar arasında testlerin ve kalibrasyon sonuçlarının karşılaştırılabilirliğini değerlendirmektedir. APAC akreditasyon kurallarını ISO eksenli alan bir kuruluş olup, kendi içerisinde rehberler de yayınlamıştır. Bunlardan bazıları şunlardır (APAC, 2021):

- APAC MRA-001 APAC Akreditasyon Kuruluşları Arasında Karşılıklı Tanıma Oluşturma ve Sürdürme Prosedürleri
- APAC MRA-002 APAC Karşılıklı Tanıma Anlaşması (MRA)
- APAC TEC1-008 RM Kullanımı ve Üretimine İlişkin APAC Kılavuzu
- APAC TEC1-009 Yabancı Düzenleyici Gereklilikleri Karşılamak için Laboratuvarların ve Muayene Kuruluşlarının Değerlendirilmesine İlişkin APAC Kılavuzu
- APAC TEC4-001 Akreditasyon Kapsamının Tanımına İlişkin Kılavuz
- APAC TEC4-002 ISO-IEC 17065 Organik Sertifikasyonun Uygulanmasına İlişkin Kılavuz
- APAC TEC4-003 Esnek Akreditasyon Kapsamlarına İlişkin Kılavuz

2.5. Uzman Sertifikasyonları

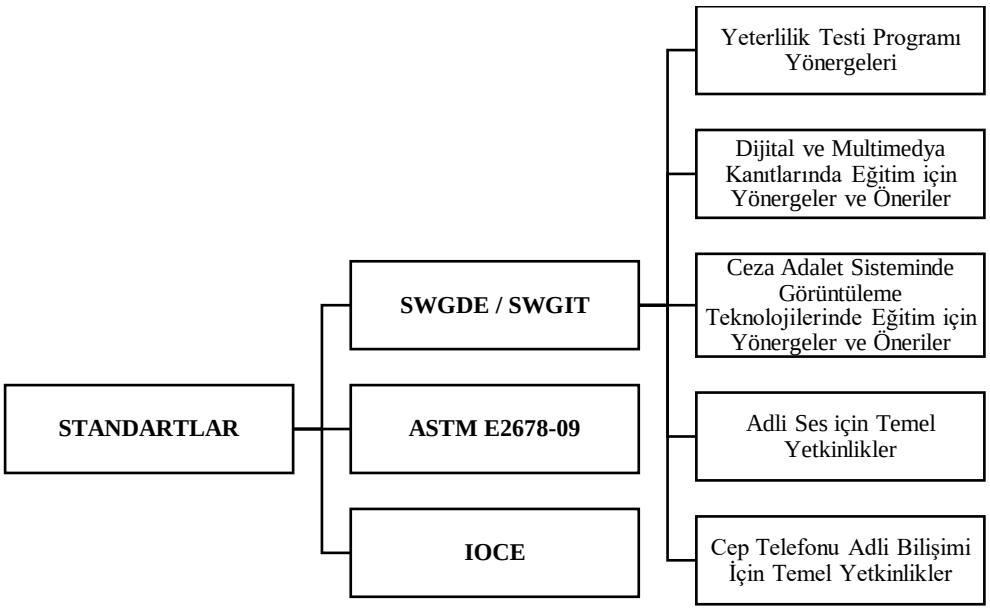
Her ne kadar bilgi çağında teknolojilerle içiçe yaşıyor olsak da, elektronik cihazları üretenler, kullananlar ve yenileyenler ile suçları işleyenler, araştıranlar ve yargılayanlar hala insanlar olmaktadır. Yarı otonom sistemlerin yaygınlaşıp tam otonom yapılara geçiş yapana kadar bu durum böyle devam edeceğine göre, insan faktörüne yapılacak kapsamlı bir yatırım birçok sorunu çözebileceği gibi, oluşmasını da engelleyebilecektir. Konumuzun esasını oluşturan adli bilişim uzmanları, araştırmacılar ve personel bu sürecin hakkıyla başarılması noktasında, bilgi, beceri, eğitim ve etkinlik açısından kilit faktörlerdir. Bu sebeple çalışacak bu insan gücünün en iyi şekilde yetiştirilmesi konusunda asla kolaya kaçılmaması gerekmektedir.

Adli bilişim uzmanlarının eğitimleri konusunda ilgili kuruluşlarca hazırlanan standartlar ve en iyi uygulamalar olduğu gibi, yazılım şirketlerinin, kamu ve özel

sektör ile üniversitelerin de eğitim programları ve kursları bulunmaktadır. Bu sebeple bu bölüm ikiye ayrılarak ilgili hususlar hakkında bilgilendirme yapılmıştır. Elbette yapılan çalışmalar aşağıdakilerle sınırlı değildir ve her geçen gün daha da gelişip çoğalmaktadır. Ama unutulmamalıdır ki, kaliteli uzmanlık için nicelikten ziyade nitelik daha önemlidir.

2.5.1. Standartlar ve En İyi Uygulamalar

Tez çalışmasının başında gerek tarihçesi, gerekse faaliyetleri hakkında açıklamaların yapıldığı IOCE, ASTM, SWGDE ve SWGIT gibi kuruluşlar standartlarını ve en iyi uygulamalarını oluştururken çalışacak personel ile adli bilişim uzman ve araştırmacılarının nitelikli şekilde yetiştirilmesi konusunda da gerekli düzenlemeleri yapmışlardır. Bu noktada en iyi uygulamalar bakımından en geniş ve detaylı bilgileri hazırlayan SWGDE'nin bu alanda da pek çok çalışma yaparak, araştırılacak her bir elektronik cihaz ile materyal konusunda ayrı uzmanlık sistemleri oluşturmaya çalıştığı görülmektedir (Şekil 2.31.).



Şekil 2.31. Adli Bilişim Uzmanlarının Yetkinliği için Düzenlenen Standartlar

Bu bölümde aşağıdaki standartlardan bahsedilecektir:

- IOCE "Eğitim Standartları ve Bilgi Becerileri ve Yetenekleri" (2002b)
- ASTM E2678-09 "Bilgisayar Adli Bilişiminde Eğitim ve Öğretim için Standart Kılavuz" (2009)
- SWGDE / SWGIT "Yeterlilik Testi Programı Yönergeleri" (2006)
- SWGDE / SWGIT “Dijital ve Multimedya Kanıtlarında Eğitim için Yönergeler ve Öneriler” (2010)
- SWGIT “Ceza Adalet Sisteminde Görüntüleme Teknolojilerinde Eğitim için Yönergeler ve Öneriler" (2010c)
- SWGDE "Adli Ses için Temel Yetkinlikler" (2011)
- SWGDE “Cep Telefonu Adli Bilişimi İçin Temel Yetkinlikler” (2013b)

2.5.1.1. IOCE "Eğitim Standartları ve Bilgi Becerileri ve Yetenekleri" (2002b)

Personel eğitimi için hazırlanacak eğitim konularını ve yetkinlik ile nitelik kazanmaları için gereken tecrübeyi sağlacak eğitim standartlarını ana hatlarıyla belirleyerek, yasal konularda bilinçlenmeleri için ayrıca mahkeme modeli geliştirmektedir. Bunun için harcanacak maliyeti ve yönetim ile işbirliği açısından özel eğitim ilkelerini de belirlemektedir.

2.5.1.2. ASTM E2678-09 "Bilgisayar Adli Bilişiminde Eğitim ve Öğretim İçin Standart Kılavuz" (2009)

Kılavuz, adli bilişim alanında bir kariyer için akademik kurumlara müfredat ve model sunarak adli bilişim uzmanı olmak isteyen kişiler için gerekli olan bilgi, yetenek ve becerileri sağlamayı amaçlamaktadır. Profesyonel sertifikalar, 2 yıllık ön lisans, lisans ve yüksek lisans derecelerini içeren eğitimlerin oluşturulmasını hedeflemektedir.

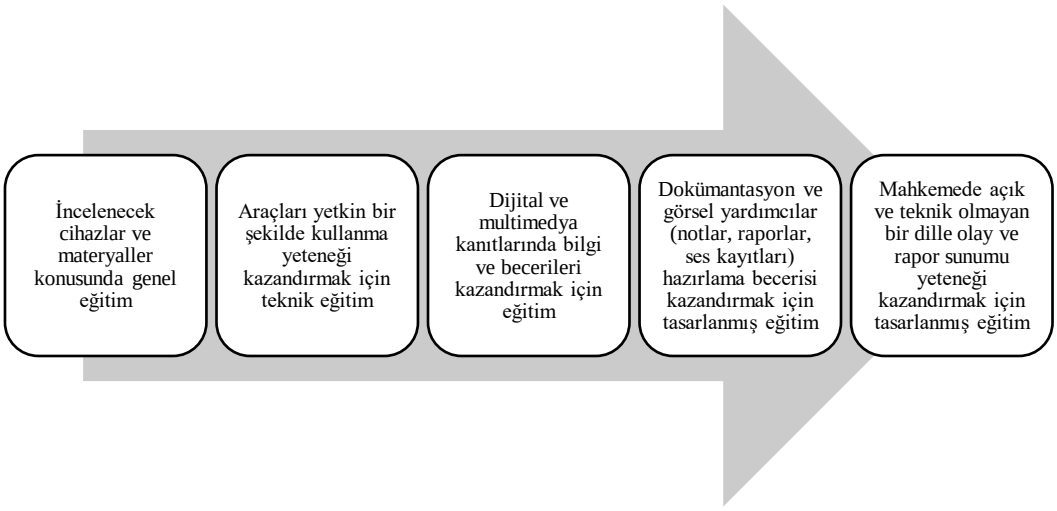
2.5.1.3. SWGDE / SWGIT "Yeterlilik Testi Programı Yönergeleri" (2006)

Başta dijital ve multimedya kanıtı (DME) olmak üzere, bilgisayar, görüntü, video ve adli ses analizi alanlarında adli bilişim uzmanlarınca uygulanan teknikler için yeterlilik testi programı sağlayarak işlemlerin ve sonuçların kalite standardına uygunluğunu belirlemektedir. Yeterlilik testi için tasarımlar ve hazırlıklar yapılması, süreç içerisinde incelemelerde bulunulması ve sonuçların belgelenmesi konularında rehberlik sağlamaktadır.

Çalışan personel için yılda en az 1 kez, kurum onaylı protokollere göre yeterlilik testi uygulaması ile başarıların ölçülmesi amaçlanmakta, test sonuçlarının ise kuruluşça belirlenecek kalifiye personel tarafından değerlendirilmesi öngörülmektedir.

2.5.1.4. SWGDE / SWGIT "Dijital ve Multimedya Kanıtlarında Eğitim İçin Yönergeler ve Öneriler" (2010)

Rehber, araştırmacıların, uzmanların ve personelin adli bilişim konusundaki eğitimleri noktasında şunları önermektedir:



Şekil 2.32. SWGDE / SWGIT Dijital ve Multimedya Kanıtlarında Eğitim Konuları

Eğitimlerin temel amacı, adli bilişim sürecinin aşamaları, teknolojiler, özel uygulamalar, teknik beceriler ve yasal işlemler konusunda farkındalık yaratma, beceri oluşturma ve yetkinlik kazandırmaktır. Bu hususta teorik ve pratik uygulama yöntemleri ile sertifikalar ve yükseköğretim programları uygulanabilmektedir. Eğitimlerin bir kez verilmesi gelişen teknoloji ve dönüşümle yetersiz kalacağı için uzmanların ve araştırmacıların belirli aralıklarla denetlenmesi, bilgilerinin ve becerilerinin sınanması amaçlarıyla yetkinlik ve yeterlilik testlerine tabi tutulması önerilmektedir.

2.5.1.5. SWGIT "Ceza Adalet Sisteminde Görüntüleme Teknolojilerinde Eğitim için Yönergeler ve Öneriler" (2010c)

Yukarıda açıklanan SWGDE ve SWGIT (2010)'dan farklı olarak bu belge, görüntü veya video analizi yapmayan disiplinlerdeki kişiler (örneğin; avukat, hakim, yönetici vb.) personel veya laboratuvarlar için görüntüleme teknolojileri eğitimi konusunda rehberlik etmektedir.

Ceza adalet sistemindeki bu teknolojilerin personel ve farklı kullanıcı grupları tarafından güvenilir kullanımı amacıyla, çeşitli eğitim kategorileri için öneriler ve yönergeler tanımlamayı amaçlamaktadır. Ayrıca kuruluşların, eğitimden beklenenin yeterli olduğunu belgelemek kaydıyla, kendilerinin seçtiği farklı türde eğitimler vermeyi tercih edebileceğini de belirtmektedir.

Teknik eğitim, süreç eğitimi, mahkemeye sunumdaki tanık ifadesi, vaka eğitimi ve süreklilik temelli ek ve güncel eğitimler SWGDE ve SWGIT (2010) ile aynı yolu izlemektedir.

2.5.1.6. SWGDE "Adli Ses için Temel Yetkinlikler" (2011)

Bu belge, ses kanıtı toplaması, ses laboratuvarı konfigürasyonu ve adli ses işlevlerini yürütmek için gerekli yasal standartları takip ederek raporlamaya kadar tüm adli ses süreci için temel yetkinlikleri tanımlamakta ve ayrıca adli sesle ilgili yetkinlik ve yeterlilik için ihtiyaç duyulan eğitim ve sertifika programları için temel oluşturmaktadır.

2.5.1.7. SWGDE "Cep Telefonu Adli Bilişimi İçin Temel Yetkinlikler" (2013b)

İlk müdahale ekipleri ve laboratuvar personeli için her seviyede gerekli olan temel beceriler için gerekli eğitim, sertifika ve test programlarını belirleyerek, cep telefonlarının analizi, kullanımı ve adli olarak işlenmesi için gerekli temel yetkinlikleri tanımlamaktadır.

2.5.2. Sertifikasyon ve Eğitim Programları

Yukarıda gözden geçirilen en iyi uygulama rehberleri ile standartlara ek olarak, adli bilişim analizlerinde yaygın olarak kullanılan yazılımları üreten şirketlerin, analizlerin başarıyla yürütülmesini sağlamak amacıyla gerçekleştirdiği birçok eğitim ve sertifika programı bulunmaktadır. Örneğin, en yaygın yazılımlardan Forensic Toolkit (FTK)'nın üreticisi AccessData Group Inc. tarafından "***AccessData BootCamp*", "*AccessData Certified Examiner* (ACE)", *"AccessData Certified Examiner for Enterprise (ACEE)"* ve *"AccessData eDiscovery Certified Administrator (eDCA)"* eğitimlerinden başka, adli soruşturmacı, Mac adli bilişim uzmanı, kötü amaçlı yazılım araştırmacısı olmaya yönelik çeşitli sertifika programları da vardır. Diğer bir yaygın yazılım olan EnCase Forensics'in üreticisi Guidance Software, Inc. ise "*EnCE Certified Examiner", "Certified eDiscovery Practitioner* (EnCEP)" gibi programlar yürütmektedir.

Polislik Koleji (CoP - *College of Policing*) tarafından devralınan Ulusal Polisliği İyileştirme Ajansı (NPIA - *National Policing Improvement Agency*) tarafından verilen eğitimlerden, "**NPIA / CoP Çekirdek Becerileri** *(Core Skills)"* eğitim kursları Birleşik Krallık kolluk kuvvetlerinin en temel kursları arasındadır (Li ve ark., 2015, s:84). "**Veri Kurtarma ve Analizde Temel Beceriler** (*Core Skills in Data Recovery and Analysis*)" programı gibi adli bilişim uzmanlarına yetenek ve beceri kazandırma hedefi güden kolluk kuvvetleri tarafından yürütülen programlar da bulunmaktadır (College of Policing, 2021). Yine aynı kurumun "**Cep Telefonu Adli Tıp Temel Becerileri"** (*Core Skills in Mobile Phone Forensics*); cep telefonundan ve SIM kartlarından veri alması gereken personel için uygun araçlar ve prosedürler eşliğinde uygulama eğitimlerini, ilgili İngiltere ve Galler mevzuatı arasındaki ilişkiyi, bu mevzuatların etkisini ve bir avukatın telefonla ilgili kanıtlara bakış açısını öğretmeyi temel almıştır (College of Policing Mobile, 2021).

Multimedya kanıtları ve adli bilişimi için LEVA International, Inc tarafından sunulan LEVA Sertifikasyon Programı bulunmakta olup, LEVA, adli video analistleri için "**Sertifikalı Adli Video Analisti (CFVA** - *Certified Forensic Video Analyst*)**"** ve **"Sertifikalı Adli Video Teknisyeni (CFVT** - *Certified Forensic Video Technician*)**"** olmak üzere iki düzeyde sertifika sunmaktadır. Minimum bir yıl boyunca video kanıtı işleyen ancak tam analiz gerçekleştirmeyen ve üç yıllık bir süre içinde Seviye 1 ve Seviye 2 temel kurslarını başarıyla tamamlayanlar CFVT; en az iki yıl boyunca hareketsiz görüntü ve video kanıtlarını işleyerek, Seviye 1'i başarıyla tamamlayanlar CFVA unvanı almaya hak kazanmaktadır (LEVA Inc., 2021).

Birleşik Krallık kanun uygulayıcıları için, ACPO En İyi Uygulama Rehberi'nin 7.1. bölümünde "E-Suç Soruşturmaları Yöneticileri için ACPO İyi Uygulama ve Tavsiye Kılavuzu" şu konuları düzenlemektedir (ACPO, 2012);

- Dijital araştırmaların normal polislik eğitiminden farklı olduğunu,
- Teknolojinin hızlı gelişimine ayak uydurmak için sürekli ve güncel eğitim gerekliliğini,

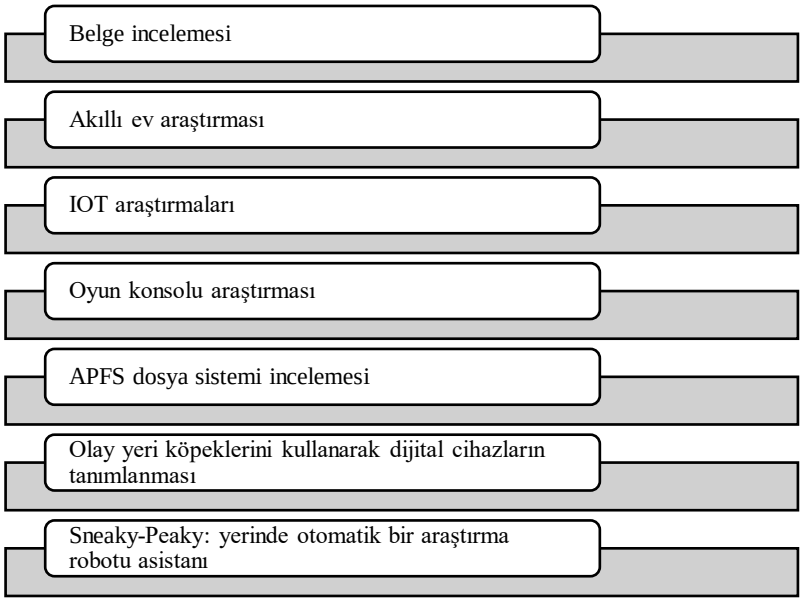
- Bunun için sertifika programları, konferanslar ve teknik atölyelere katılım ve bağımsız araştırmalar gibi mesleki gelişim fırsatlarının değerlendirilmesini,
- POLKA (Polis Çevrimiçi Bilgi Alanı - *Police On-Line Knowledge Area*) gibi adli bilişim topluluklarından ve bazı ilgili belgelerin bulunduğu platformlardan yararlanmak gerektiği.

Yöneticilere, personellerini eğitmelerine yardımcı olması için ürün odaklı eğitimler, genel nitelikli kurslar ve yüksek öğrenim derecesinde programlar dahil olmak üzere adli bilişimle ilgili birçok kurs sunulmaktadır (Li ve ark., 2015, s:84).

Avrupa Siber Suçlar Eğitim ve Öğretim Grubu (ECTEG - *European Cybercrime Training and Education Group*) tarafından, kolluk kuvvetleri için ücretsiz nitelikte eğitimler verilmektedir. Bunlar, konunun uzmanlarından oluşan bir ekip tarafından, uluslararası izleyici kitlesine yönelik, en az bir pilot eğitimle yürütülen kursları içermektedir (ECTEG Course, 2021).

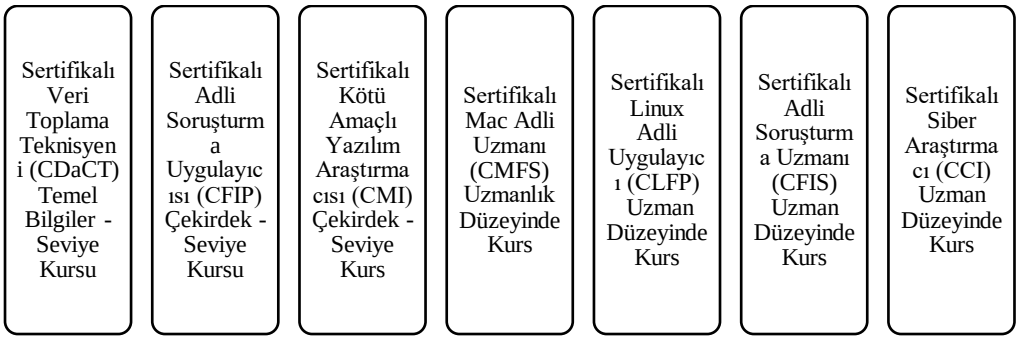
Bunların haricinde örneğin, birçok ülkenin polis bürosu işbirliğiyle yürütülen "İlk Müdahale Ekipleri İçin e-Öğrenme Paketi" (ECTEG E-Learning, 2021), "Senaryo Projesi" (ECTEG Scenario, 2021), "Küresel Siber Suç Sertifikasyon Projesi" (ECTEG Certification, 2021) ve "Temel Ağlar Adli Bilişimi" (ECTEG Network, 2021) eğitimleri bulunmaktadır.

Cranfield Üniversitesi Adli Bilişim Merkezi (CFFC - *Centre for Forensic Computing*), "senaryoya dayalı vaka çalışmaları ve araştırmaya yönelik pratik eğitimleri eğlenceli bir tarzla" sunmayı hedeflemektedir. Merkez, şifrelenmiş veya gizlenmiş veriler, silinmiş ve parçalanmış dosyalar, işletim sistemlerinin dahili çalışmaları, yıkıcı ve tahribatsız edinim teknikleri dahil, karmaşıklık açısından değişen tüm dijital araştırma alanlarında çalışmaktadır (Cranfield University 2021). Merkezin verdiği burslar ise Şekil 2.33.'de gösterilmektedir:



Şekil 2.33. CFFC'nin İlgililerine Verdiği Burslar

2001 yılında Cambridge'de PA Consulting tarafından kurulan "7Safe", siber geliştirme merkezinde 22 üniversite ve endüstri tarafından akredite edilmiş kurslardan oluşan sertifikalı adli bilişim kurslarını, kanun uygulayıcılarına, hukuk uzmanlarına ve endüstri sektöründeki özel şirketlere vermektedir. Siber Teknoloji Yüksek Lisans eğitiminde, bilgi güvenliği yeterliliği sağlamak için De Montfort Üniversitesi (DMU) ile ortak çalışmaktadır. Bu eğitim sekiz üniversite modülünden ve yedi kurstan oluşmaktadır (Şekil 2.34.):



Şekil 2.34. Üniversite Tabanlı Adli Bilişim Kursları

- **Sertifikalı Veri Toplama Teknisyeni** (CDaCT - *Certified Data Collection Technician*) **Temel Bilgiler - Seviye Kursu:** veri işlemede, kopyalamada, aktarımda ve toplamada yetkinlik kazandırarak, dijital delil bütünlüğünün korunmasını sağlamak için beceriler kazandırmak için üç günlük bir kurstur (CDaCT, 2021).

- **Sertifikalı Adli Soruşturma Uygulayıcısı** (CFIP - *Certified Forensic Investigation Practitioner*) **Çekirdek - Seviye Kursu:** adli bilişimin tüm aşamalarının kavranması, ilkelerin ve yönergelerin öğrenilmesi, verilerin elektronik ortamda nasıl depolandığı ve temel adli araştırma araçlarıyla nasıl çalışılacağı gibi bilgilerin edinilmesine yönelik teknik ve uygulamalı eğitim vermektedir (CFIP, 2021).

- **Sertifikalı Kötü Amaçlı Yazılım Araştırmacısı** (CMI - *Certified Malware Investigator*) **Çekirdek - Seviye Kurs:** kötü amaçlı yazılım türlerini tanımlama, analiz etme ve yorumlama ve kötü amaçlı yazılım bulaşmasıyla ilişkili bilgisayar ve ağ etkinliğini araştırma becerileri kazandırmaya yönelik teknik bir eğitimdir (CMI, 2021).

- **Sertifikalı Mac Adli Uzmanı** (CMFS - *Certified Mac Forensics Specialist*) **Uzmanlık Düzeyinde Kurs:** bir Apple ve MAC cihazında depolanan verilerin nasıl bulunacağı, toplanacağı, işleneceği ve şifrelerinin nasıl çözebileceği ile çeşitli adli olaylara etkili bir şekilde nasıl yanıt verileceğine yönelik uygulamalı üç günlük bir eğitimdir (CMFS, 2021).

- **Sertifikalı Linux Adli Uygulayıcı** (CLFP - *Certified Linux Forensic Practitioner*) **Uzman Düzeyinde Kurs:** Linux tabanlı sistemlerin temel sistem bilgilerini öğrenmek, verileri tanımlamak, toplamak ve analiz etmek için bilgi ve beceriler edinmek isteyen deneyimli adli araştırmacılar için eğitim vermektedir (CLFP, 2021).

- **Sertifikalı Adli Soruşturma Uzmanı** (CFIS - *Certified Forensic Investigation Specialist*) **Uzman Düzeyinde Kurs:** canlı sistemler ile uzak ve sanallaştırılmış sistemlerden geçici ve depolanmış verileri yakalamayı ve analiz etmeyi, mevcut Windows işletim sistemlerindeki en son yönergeleri ve eserleri tanıtmayı sağlamaktadır. 7safe, bir dizi adli araç, komut dosyası ve teknik kullanan gerçekçi bir veri / IP hırsızlığı senaryosunu kullanarak yeni becerileri geliştirmeyi sağladıklarını belirtmektedir (CFIS, 2021).

- **Sertifikalı Siber Araştırmacı** (CCI - *Certified Cyber Investigator*) **Uzman Düzeyinde Kurs:** canlı sistemlerden veri yakalama ve analiz etmeye yönelik yeni teknikler oluşturmak, sağlam bir siber soruşturma yürütmek için bir dizi metodoloji geliştirmek ve bir siber olay sırasında veya sonrasında canlı bir ağ ortamında doğru verileri tanımlamak için gereken kritik becerileri öğrenmek, araştırmanın başarısız olmasına veya araştırma sonunda ortaya çıkan kanıtların mahkemede kabul edilemez olmasına neden olabilecek hayati ipuçlarını kavramak için geliştirilen uygulamalı ileri düzey eğitimdir (CCI, 2021).

Bunların haricinde, bağımsız adli bilişim sertifikalarının, kuruluşları ile birlikte listesi Çizelge 2.2.'de gösterilmektedir (Rahman, 2015):

Çizelge 2.2. Adli Bilişim Sertifikaları ve Bağlı Oldukları Kuruluşlar

KURULUŞ	**SERTİFİKA**
AccessData	AccessData Sertifikalı Denetçi (ACE – *AccessData Certified Examiner*)
Guidance Software Inc. (GSI)	EnCase Sertifikalı Denetçi (EnCE)
Brainbench	Brainbench Adli Bilişim (U.S) (BCF – *Brainbench Computer Forensics*)
Anonim Siber Uygulama Kaynakları (CERI - *Cyber Enforcement Resources Incorporated*)	- Bilgisayar Adli İnceleme (CFE - *Computer Forensic Examination*) - Gelişmiş Bilgisayar Adli İncelemesi (ACFE - *Advanced Computer Forensic Examination*)
Siber Güvenlik Enstitüsü (CSI - *Cyber Security Institute*)	Siber Güvenlik Adli Analisti (CSFA - *Cyber Security Forensic Analyst)*

Adli Bilişim Sertifikasyon Kurulu (DFCB - *Digital Forensic Certification Board*)	Dijital Kanıt Uygulayıcısı (DEP - *Digital Evidence Practitioner*)
E-İş Süreç Çözümleri (E-BPS - *E-Business Process Solutions*)	Sertifikalı Siber Suç Uzmanı (C3E - *Certified Cyber-Crime Expert*)
Küresel Bilgi Güvencesi Sertifikası (GIAC - *Global Information Assurance Certification*) SANS	- GIAC Sertifikalı Adli Analist Gümüş - GIAC Sertifikalı Adli Analist Altın (*GCFA - GIAC Certified Forensics Analyst Silver /Gold*)
Uluslararası Endüstriyel Güvenlik İçin Amerikan Topluluğu (ASIS - *American Society for Industrial Security International*)	Profesyonel Sertifikalı Araştırmacı (PCI - *Professional Certified Investigator*)
Yüksek Teknolojili Suç Enstitüsü (HTCI – *High Tech Crime Institute*)	- Bilgisayar Olay Yeri Teknisyeni (CCST - *Computer Crime Scene Technician*) - Sertifikalı Bilgisayar Ağı Araştırmacısı (CCNI - *Certified Computer Network Investigator*) - Sertifikalı Adli Bilişim Teknisyeni (CCFT - *Certified Computer Forensic Technician*) - Adli İşletim Sistemi Uzmanı (FOSS - *Forensic Operating System Specialist*)
Yüksek Teknolojili Suç Ağı (HTCN – *High Tech Crime Network*)	- Temel Sertifikalı Bilgisayar Suçları Araştırmacısı - Gelişmiş Sertifikalı Bilgisayar Suçları Araştırmacısı (*CCCI – Basic/Advanced Certified Computer Crime Investigator*) - Temel Sertifikalı Bilgisayar Adli Bilişim Teknisyeni - Gelişmiş Sertifikalı Bilgisayar Adli Bilişim Teknisyeni (*CCFT – Basic/Advanced Basic Certified Computer Forensics Technician*)
Uluslararası Bilgisayar Araştırma Uzmanları Birliği (IACIS - *The International Association of Computer Investigative Specialists*)	- Sertifikalı Adli Bilgisayar Denetçisi (CFCE - *Certified Forensic Computer Examiner*) - Sertifikalı Elektronik Kanıt Toplama Uzmanı (CEECS - *Certified Electronic Evidence Collection Specialist)*
Uluslararası Elektronik Ticaret Danışmanları Konseyi *(EC-Council, The International Council of Electronic Commerce Consultants*)	Bilgisayar Korsanlığı Adli Araştırmacısı (CHFI - *Computer Hacking Forensic Investigator*)
Uluslararası Bilgi ve İletişim Teknolojileri Konseyi (IICTC - *International Information and Communication Technology Council*)	Adli Bilişim Araştırmacısı (CIFI - *Computer Information Forensics Investigator*)

Uluslararası Bilgi Sistemleri Adli Bilişim Derneği (IISFA - *International Information Systems Forensics Association*)	Sertifikalı Adli Bilişim Araştırmacısı (CIFI - *Certified Information Forensics Investigator*)
Uluslararası Adli Bilişim Denetçileri Topluluğu (ISFCE - *The International Society of Forensics Computer Examiners*)	Sertifikalı Bilgisayar Denetçisi (CCE - *Certified Computer Examiner*)
Paraben Corporation	Paraben Sertifikalı Mobil Cihaz Denetçisi (PCME – *Paraben Certified Mobile Examiner*)
Bilgi Güvencesi Sertifikasyon İnceleme Kurulu (IACRB - *Information Assurance Certification Review Board*)	Sertifikalı Adli Bilişim Denetçisi (CCFE - *Certified Computer Forensics Examiner*)
Sertifikalı E-Keşif Uzmanları Derneği (ACEDS - *Association of Certified E-Discovery Specialists*)	Sertifikalı E-Keşif Uzmanı (CEDS - *Certified E-Discovery Specialist*)
Mile2	Sertifikalı Adli Bilişim Denetçisi (CDFE - *Certified Digital Forensics Examiner*)

2.6. Hukuki Düzenlemeler

Suç niteliği taşıyan eylemlerin cezalandırılması fikriyle ortaya çıkan ceza kanunları, döneminin yaygın fiilleriyle ilgili hükümler içermektedir. Dünya çapında yaygınlaşıp genişleyen bilişim suçlarının ortaya çıkışıyla birlikte, bu suç tipiyle ilgili kanuni düzenlemeler yapma zorunluluğu da doğunca ülkeler ilgili hükümleri mevcut ceza kanunları içine yerleştirmek veya bağımsız bir kanun yapmak arasında bir tercih yapmak durumunda kalmışlardır. Anglo-Sakson hukuk sistemine sahip Amerika, İngiltere, Portekiz, İrlanda, Kanada gibi ülkeler ayrı bir kanunla düzenleme yapmayı seçerken, Almanya, Fransa, Hollanda gibi Kıta Avrupası hukuk sistemini benimsemiş ülkeler ilgili maddeleri ceza kanunlarında bulundurmayı tercih etmiştir (Yazıcıoğlu, 1997). Türkiye de Kıta Avrupası sistemini benimsemiş bir ülke olarak ilgili hükümleri mevcut ceza kanununa dahil etmiştir. Ancak bu sistem ayrı bir kanunla geniş düzenlemeler yapabilme durumunu elbette ki engellememektedir.

Bilişim suçlarının dünya çapında bir sorun haline gelmesi neticesinde, birçok ülkeyi içine alacak kadar geniş çaplı bir hukuki düzenleme yapılarak bu suçlarla savaşma ihtiyacı doğduğunda, ortaya "Avrupa Siber Suçlar Sözleşmesi (*Convention on Cybercrime*)" çıkmış, Türkiye'nin de dahil olduğu birçok ülke düzenlenen

hükümleri kabul etmiştir. 2001 yılında Budapeşte'de Avrupa Konseyi tarafından sunulan bu sözleşme, başta; bir bilgisayar sistemine haksız ve yasadışı erişim (md.2); kamuya açık olmayan bilgisayar verilerinin iletiminde yasadışı müdahale (md.3); verilerin haksız yere silinmesi, bozulması, değiştirilmesi ve erişilmez kılınması (md.4); bilgisayar sisteminin işleyişini haksız yere engelleme (md.5); yazılım, şifre, kod gibi unsurlar kullanılarak cihazların kötüye kullanımı (md.6) fiillerini ve bilişim sistemlerini araç olarak kullanarak işlenen ceza kanunlarında suç kabul edilen diğer fiilleri düzenlemektedir (CoE, 2001). Sözleşme ayrıca, bilgisayarla ilgili sahtecilik (md.7) ve dolandırıcılık (md.8) suçları ile çocuk pornografisine ilişkin suçlar (md.9)'ı düzenlemekle birlikte, depolanan bilgisayar verilerinin korunması (md.16), aranması ve bunlara el konulması (md.19) ile ilgili hükümler de içermektedir (CoE, 2001). Bilişim suçlarının uluslararası niteliği ile uzantılı olarak sözleşmede, yargı yetkisi (md. 22), uluslararası işbirliği (md.23), suçluların iadesi (md.24) ve karşılıklı yardımlaşma (md.25) konuları suçların soruşturulmasında ve kovuşturulmasında belirsizlikleri ortadan kaldırmak adına sözleşmeye eklenmiştir (CoE, 2001).

Hemen her siber suç, bir sistemi veya içindeki verileri hedef aldığından dolayı uluslararası alanda kabul edilmiş kişisel verilerle ilgili "Genel Veri Koruma Tüzüğü (GDPR - *General Data Protection Regulation*)" de atlanmaması gereken önemli bir mevzuattır. Özetle, 2018'de yürürlüğe giren bu tüzük, küresel anlamda nerede hizmet verdiğine ve faaliyette bulunduğuna bakılmaksızın, GDPR'ın uygulama alanındaki her veri sorumlusu/veri işleyen bakımından bağlayıcı olup, işleme konu her kişisel verinin de hukuki güvencesini sağlamayı amaçlamaktadır (Özkaya ve Samet, 2020b, s:166). Tüzüğün 33. Maddesinde; bir kişisel veri ihlalinin söz konusu olması durumunda, veri sorumlusunun, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde kişisel veri ihlalini yetkin denetim makamına ve gecikmeksizin veri sahibi ilgili kişiye bildirme sorumluluğu bulunmaktadır.

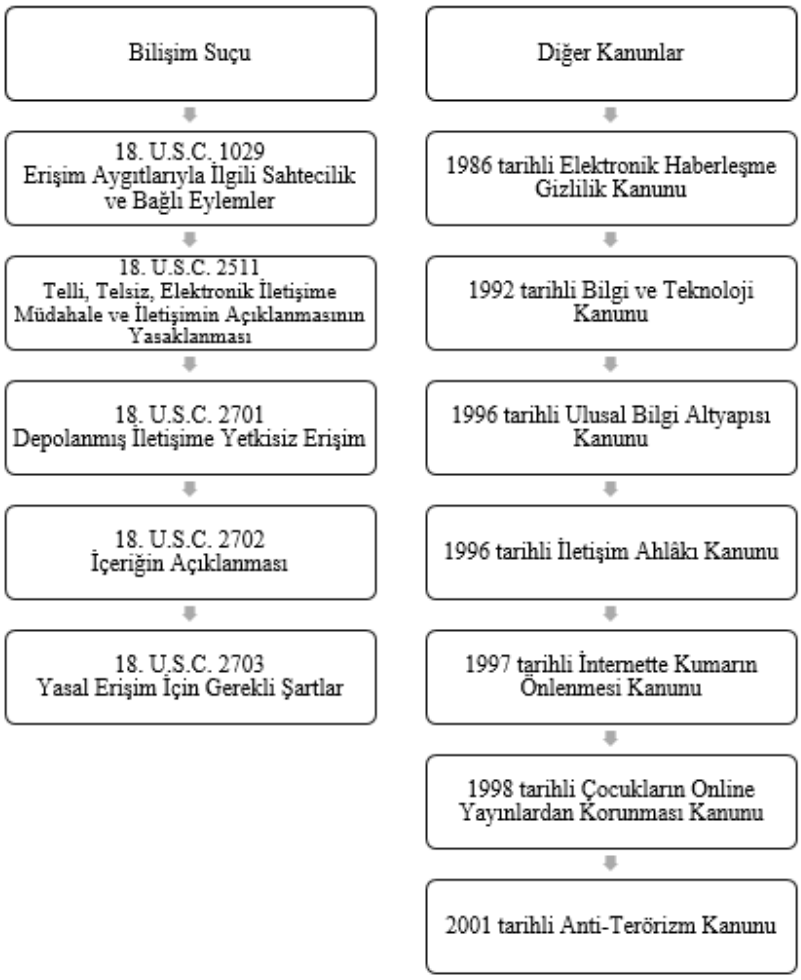
Bu kapsamda, adli bilişim alanında ve bilişim suçlarıyla mücadelede öncü olan ve aktif rol oynayan Amerika ve Birleşik Krallık ile ilgili düzenlemelerden bahsedilerek, sonraki kısımda Türkiye'deki durum hakkında açıklamalarda bulunulacaktır.

2.6.1. Amerika Birleşik Devletleri

Bilişim suçlarının ilk örneklerinin Amerika'da ortaya çıkması, bu alandaki ilk hukuki düzenlemelerin de aynı kıtada oluşmasını beraberinde getirmiştir. Bilişim suçlarıyla ilgili olarak ilk kanun tasarısının 1977 yılında Amerika Birleşik Devletleri Kongresine verildiği kabul edilmektedir. Artan suç faaliyetleri neticesinde mevcut ceza adalet sisteminin değişen teknoloji ile başa çıkabilmesi için yeterli donanıma sahip olmadığı anlaşılınca, 1984 tarihli "Kapsamlı Suç Kontrol Yasası (CCCA - *Comprehensive Crime Control Act*)"ın bir parçası olarak kabul edilen "Erişim Aygıtlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu (*Counterfeit Access Device and Computer Fraud and Abuse Act*)" isimli kanun yürürlüğe girmiş ve 1986' da "*Computer Fraud and Abuse Act* - CFAA" adını almıştır (18. U.S.C. 1030).

Kapsamlı Suç Kontrol Yasası, dolandırıcılık eyleminin tanımını iyileştirmesine ve ceza hükümlerini güçlendirmesine rağmen, aynı zamanda çeşitli sorunlar yarattığı gerekçesi ile Kongre tarafından 1984 yılında, CCCA' nın eksiklikleri düzeltmek amacıyla "Kredi Kartı Sahteciliği Kanunu (*Credit Card Fraud Act*) (18 U.S.C. § 1029) " kabul edilmiştir (Caminer, 1985, s:759).

Şekil 2.35.'de Amerika'da düzenlenen bilişim suçlarıyla doğrudan ve dolaylı olarak ilgili kanunlar gösterilmektedir:



Şekil 2.35. Amerika Birleşik Devletleri İlgili Kanun Maddeleri (Ehliz, 2019)

Suç tiplerine karşılık gelen kanunlar ise Çizelge 2.3.'de gösterilmektedir:

Çizelge 2.3. Doğrudan ve Dolaylı Bilişim Suçlarıyla İlgili ABD Yasaları

YASA DIŞI DAVRANIŞ	YASA
Servis Reddi Saldırıları	18 U.S.C. § 1030 (a)(5)(A) (program, bilgi, kod veya komutun iletilmesi)
	18 U.S.C. § 1362 (devlet iletişim sistemlerine müdahale)
Bir web sitesinin değiştirilmesi veya yönlendirilmesi	18 U.S.C. § 1030 (a)(5)(A) (i)
	18 U.S.C. § 1030 (a)(5)(A) (ii) (iii) (bir bilgisayara yetkisiz erişim)
Yanıltıcı Alan Adının Kullanımı	18 U.S.C. § 2252 B (bir kişiyi veya çocuğu müstehcen materyalleri görmesi için kandırmak amacıyla)
Gasp	18 U.S.C. § 1030 (a) (7) (zarara neden olma tehdidi içeren iletişimi iletmek)
	18 U.S.C. § 875 (b), (d) (zorla ve kasten, bir kişiyi kaçırmak veya zarar vermek ya da kşinin mülküne veya itibarına zarar verme tehdidi-Hobbs Act)
	18 U.S.C. § 1951 (ticarete gasp, soygun, tehdit veya şiddet nedeniyle müdahale
İnternet Sahtekarlığı (örn; kimlik avı)	18 U.S.C. § 1030 (a)(4) (dolandırmak veya bir şey elde etmek amacıyla bir bilgisayara erişim)
	18 U.S.C. § 1028 (kimlik belgeleri ve kimlik doğrulama özellikleriyle bağlantılı dolandırıcılık)
	18 U.S.C. § 1028A (ağırlaştırılmış kimlik hırsızlığı)
	18 U.S.C. § 1343 (tel sahtekarlığı)
	18 U.S.C. § 1956, 1957 (kara para aklama)
	18 U.S.C. § 1001 (hükümetin yetkisi dahilindeki herhangi bir konuda yanlış beyanda bulunmak)
	18 U.S.C. § 45 (haksız veya aldatıcı ticaret uygulamaları)
	18 U.S.C. § 6821 (finansal bilgilere hileli erişim)

2.6.1.1. Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası (CFAA - 18 U.S.C. § 1030)

CFAA, Kapsamlı Suçlarla Mücadele Kanunu'na dahil edilmiş olan, mevcut bilgisayar sahtekarlık yasasında bir değişiklik olarak 1986'da yürürlüğe giren bir ABD siber güvenlik yasasıdır ve başlık 18, bölüm 1030 (18 U.S.C. § 1030) olarak kodlanmıştır (DoJ, 2015, s:1).

Kanun, hükümete ait ulusal bilgiler ile finansal kurumların mali kayıtlarının bulunduğu veya eyaletler arası veya yabancı ticarette kullanılan ya da bunları etkileyen herhangi bir bilgisayara yani "korunan bilgisayarlar"a bilerek, kasten ve yetkisiz şekilde yapılan girişleri cezalandırmaktadır. Bu bilgisayarlara kuruluş içinden veya dışından yapılan her türlü saldırıyı kapsayacak şekilde, ticari sırların, finans ve bankacılık bilgilerinin, fikri mülkiyet konularının, müşterilerin ve çalışanların kişisel verilerinin ve diğer hassas ve gizli bilgilerin korunması amaçlanmaktadır (Jesteadt ve Sutton, 2020).

2.6.1.2. CAN-SPAM Yasası - 18 U.S.C. § 1037

Spam e-postalarının kötüye kullanımını engellemek amacıyla, "CAN-SPAM Act" olarak bilinen, 2003 yılında "Pornografi ve Pazarlama Saldırısının Kontrol Edilmesi Kanunu (*Controlling the Assault of Non-Solicited Pornography and Marketings Act of 2003*)" kabul edildi. Bu kanun da korunan bilgisayarlara yetkisiz ve kasten yapılan müdahaleleri cezalandırmakta, kişileri e-posta aracılığıyla yanlış yönlendirmeyi ve kandırmayı suç kapsamına almaktadır. Kanun kapsamındaki suç sayılan fiiller; mesaj iletilerinin kökenini gizlemek, başlık bilgilerini önemli ölçüde değiştirmek, çevrimiçi kullanıcı hesabı veya alan adı için gerçek tescil ettirenin kimliğini önemli ölçüde tahrif eden bilgileri kullanarak kaydolmak şeklinde düzenlenmektedir (DoJ, 2015, s:106; U.S. ve Kilbride, 2007).

Kurum veya şirketlerin mevcut müşterileri ile ürün/hizmetleri ile ilgili olarak iletişime geçtikleri potansiyel müşterilerine attıkları e-postalar "ilişki mesajı" olarak adlandırılmakta ve kanun kapsamı dışında tutulmaktadır, ancak mesajın yanlış veya yanıltıcı başlık bilgisi bulunması kanunen suç kapsamında kabul edilmektedir. Eğer gönderilen mesaj ticari ise, kanunun tüm gerekliliklerine uyum zorunluluğu bulunmaktadır (Dollar, 2004).

2.6.1.3. WIRETAP Yasası (18 U.S.C. § 2511)

Telli, telsiz, sözlü veya elektronik haberleşmenin yetkisiz olarak engellenmesini, ifşa edilmesini ve kullanılmasını yasaklayan kanunda şu maddeler düzenlenmiştir:

- Herhangi bir telli, sözlü veya elektronik iletişimi kasten engellemek veya engellemeye çalışmak,
- Kasıtlı olarak herhangi bir sözlü iletişimi durdurmak için herhangi bir elektronik, mekanik veya başka bir cihazı kullanmak veya başkasını kullanması veya satın alması için teşvik etmek,
- Bir telli, sözlü veya elektronik iletişimin kesilmesiyle elde edildiğini bilmek veya bilebilecek durumda olmak ve herhangi bir telli, sözlü veya elektronik iletişimin içeriğini kasıtlı olarak kullanmak veya kullanmaya çalışmak veya herhangi bir kişiye kasıtlı olarak ifşa etmek veya ifşa etmeye çalışmak.

Wiretap Yasası, özel bir konuşmanın tarafı olmayan ve konuşmanın içeriğini duymaması gereken kişilerin bu özel iletişimi "elektronik, mekanik veya başka bir cihaz" kullanarak dinlemesi, ele geçirmesi ve kesmesini yasaklamaktadır. Örneğin; kapalı mekandaki bir konuşmayı yakalamak için odaya dinleme cihazı yerleştirilmesi, bir telefon konuşmasının dinlenmesi ve anlık mesajları yakalayan "sniffer" yazılımının yüklenmesi gibi… Bunun bir istisnası, mahkeme kararıyla müdahaleye izin verilmesidir.

2.6.1.4. Elektronik İletişim Gizlilik Yasası (ECPA - 18 ABD § 2701 vd)

ECPA (*Electronic Communications Privacy Act*), "elektronik iletişim hizmetinin sağlandığı bir tesise kasten izinsiz olarak veya yetkinin kasıtlı olarak aşılması suretiyle erişim ve bu işlemin bir sonucu olarak bir kablolu veya elektronik iletişime erişim elde etmek, iletişimi değiştirmek veya engellemek" eylemlerini cezalandırmaktadır (DoJ 18 U.S.C. § 2701 ve LII 18 U.S.C. § 2701, 2021).

İletişim hizmet sağlayıcıları abonelerine ve müşterilerine ait kayıtları tutmakta ve dosyaları depolamaktadır. Suça konu bir olay meydana geldiğinde kolluk kuvvetleri bu kayıtları vermesi için hizmet sağlayıcıları ile iletişime geçebilmektedir. Hizmet sağlayıcının türüne bağlı olarak (internet servis sağlayıcısı veya cep telefonu sağlayıcısı vb.) ECPA, bu türden olaylarda belirli türdeki abone ve müşteri bilgilerini kolluk kuvvetlerine verme konusundaki yasal süreci şekillendirmektedir.

Bir iletişimin alıcıya iletilmesinden önce veya sonra mesajın bir kopyası saklanırsa, saklanan elektronik iletişimin gizliliğini korumak için 18 U.S.C. §2701 ila 2710 hükümleri düzenlenmiştir. Bu hükümler, mesajların kopyalarının saklandığı e-posta ve bilgisayar iletimleri gibi teknolojilere odaklanmaktadır (DoJ 18 U.S.C. § 2701, 2021).

2.6.1.5. Gizlilik Koruma Yasası (PPA - 42 U.S.C. § 2000AA vd.)

PPA (*The Privacy Protection Act*), cezai suçların soruşturulması veya kovuşturulmasıyla bağlantılı olarak hükümet görevlileri ve çalışanları tarafından yapılan aramalar ve el koymalardan bahsetmekte ve kolluk kuvvetlerinin bu işlemleri gerçekleştirmek için arama emri kullanmasını sınırlamaktadır. Korunan malzemeler ya "iş ürünleri (kaçak mallar, bir suçtan elde edilenler, başka bir şekilde cezai olarak sahip olunanlar, kullanılmak üzere tasarlananlar ya da kullanılan veya kullanılanlar dışındaki malzemeler)" ya da "belgesel malzemeler (bilgilerin kaydedildiği yazılı veya basılı materyaller ile fotoğraflar, sinema filmlerini, negatifleri, video kasetlerini,

ses bantlarını ve diğer mekanik materyalleri içeren materyaller)" olabilmektedir (LII 42 U.S. Code § 2000aa–7, 2021).

PPA'nın, bilgisayarların suç işlemek veya suç işlemeyi kolaylaştırmak için kullanıldığı durumlarda genellikle kanun yaptırımı için önemli sorunlar yarattığı söylenmektedir. Örneğin, materyalleri dağıtan veya internet üzerinden dağıtım için materyal hazırlayan kişiler korumalı halka açık iletişimciler kategorisine girebilir ve bu materyale el konulması, emrin konusu olsun veya olmasın, hükümetin kesin hukuki sorumluluğuna neden olabilir (Keeney, 1969).

2.6.1.6. Örnek Olaylar

- Polis olan sanık, CFAA uyarınca bir polis veri tabanından elde edilen bilgileri sattığı için "bir bilgisayara kasıtlı olarak yetkisiz erişim veya yetkili erişimi aşma" suçunu işlediği gerekçesiyle mahkum edildi. Maddi sıkıntılar nedeniyle borç aldığı kişinin para karşılığında istediği bilgiyi polislik yetkilerini kullanarak elde eden ve karşılığında para alan sanık 18 U.S.C. § 1030 (a) (2) uyarınca 18 ay hapis cezasına çarptırıldı (U.S. ve Van Buren, 2019).

- Sanık Aleynikov, çalıştığı yatırım şirketi Goldman için geliştirdiği kaynak kodunun da içinde olduğu 500.000'den fazla kaynak kodunu şifreledi ve Almanya'daki bir sunucuya yükledi, daha sonra, şifreleme programını ve bilgisayar komutlarının geçmişini sildi. Tutuklanan sanık yapılan adli bilişim araştırmaları sonucunda bazı suçlarla birlikte bilgisayara yetkisiz erişim ve bilgisayar erişimde yetki sınırını aşma (U.S. ve Aleynikov, 2011) suçlarından yargılandı ve 97 ay hapis cezası, ardından üç yıllık denetimli serbest bırakılma cezası aldı ve 12.500 dolar para cezası ödemesi emredildi, 2018'de ise yüksek mahkeme kararıyla beraat etti. (U.S. ve Aleynikov, 2012).

- 2010 yılında Anonymous'un, PayPal'ın sitesini dört gün boyunca aralıklı olarak düşüren "DDoS saldırısı" gerçekleştirmesi neticesinde FBI, 27 arama emriyle

12 eyalette 100'den fazla bilgisayarı ele geçirdi. Bu davadaki 14 sanık, 18 USC § 1030'u ihlal ederek, korunan bir bilgisayara zarar vermek ve korunan bir bilgisayara kasıtlı olarak zarar vermek için yardım ve suç ortaklığı etmek üzere 15 komplo ile suçlandı. "Paypal 14" olarak da bilinen dava sonunda grubun tüm üyeleri PayPal'a toplamda yaklaşık 80,000 $ tutarında ödeme yapmakla cezalandırıldı (U.S. ve Collins, 2013)

- Sanıklar Schaffer ve Kilbride 2003 yılında, bir bilgisayar ağı uzmanından CAN-SPAM Yasasından kaçınmak amacıyla Amsterdam ağını kullanarak e-posta göndermek istediklerini söyleyip anlaşmaya vardılar. Sistem büyük ölçüde otomatikleştirildi ve çok sayıda adrese e-posta göndermek için kullanıldı. Bu e-postalar pornografik görüntüler ve pornografik web sitelerine bağlantılar içeriyordu. Gönderici adı genellikle günlük olarak değiştirilecek ve spam filtreleyicilerden kaçınacak şekilde tasarlandı, böylece e-posta alan kişiler aynı göndericiden geldiğini tespit edemedi (U.S. ve Kilbride, 2007). Operasyonda toplamda yaklaşık 43 milyon civarında e-posta adresi tespit edildi. Nihayetinde mahkeme sanıkları ilgili kanunun birçok hükmünü ihlal ile kara para aklama suçunun da dahil olduğu sekiz suçtan cezalandırdı; Jeffrey Kilbride 78 ay, Robert Schaffer 63 ay hapis cezasına çarptırıldı (U.S. ve Kilbride Appeals, 2009).

2.6.2. Birleşik Krallık

2.6.2.1. Bilgisayarı Kötüye Kullanım Yasası - CMA

CMA (*Computer Misuse Act*) yasası, kuruluşlar tarafından tutulan verileri yetkisiz erişime ve değiştirmeye karşı korumak amacıyla 1990 yılında kabul edilmiş olup, yetkisiz erişim, herhangi bir özel program veya veri; belirli türden bir program veya veri; ya da herhangi bir bilgisayarda tutulan bir program veya veriye erişim şeklinde olabilir. Verilerin ele geçirilmesi eylemine karşı ayrıca veri koruma yasaları ile koruma sağlamak da amaçlanmaktadır (CMA, 1990).

Kanunda; “başka bir suç işlemek niyetiyle sisteme yetkisiz erişimde, sistem içindeki verileri yok etmek veya izinsiz değiştirmek ya da sistemin işleyişini engellemek” fiilleri düzenlenmiş olup ayrıca, kullanılmak üzere eşya yapmak, tedarik etmek veya elde etmek, bir suçun işlenmesi veya işlenmesine yardımcı olmak için kullanılması amaçlanan herhangi bir nesneyi yapmak, uyarlamak, tedarik etmek veya sunmayı teklif etmek fiilleri de suç kapsamındadır. Nesneden kasıt, elektronik ortamda tutulan her türlü program veya verilerdir (CMA, 1990).

Bu maddelerle, sisteme virüs, trojen veya solucan sokmak suretiyle sistemi hackleme, bilgisayar dolandırıcılığı, şantaj, virüs, kişisel veri hırsızlığı gibi suç tiplerinin işlenmesi şeklinde karşılaşılmaktadır ve hapis ile para cezalarına hükmedilmektedir.

Bir fiilin kanundaki tanımına göre suç sayılabilmesi için bilgisayarla herhangi bir şekilde etkileşimde bulunulması gerekir, ancak bu etkileşimin fiili olmasına gerek yoktur, başlat düğmesine basmak bile kanun kapsamında değerlendirilmektedir (Clough, 2015). Ayrıca kanun yetkisiz erişimi yeterli görmekte, belli bir bilgisayarın hedef alınmasını veya failin kötü niyetli olmasını aramamaktadır (Ormerod ve Laird, 2018, s:1048). Benzer şekilde, failin sisteme girmeye çalışıp başarısız olması veya herhangi bir zarar vermemesi durumunda bile ceza söz konusu olmaktadır.

Failin bu kanun kapsamında cezalandırılabilmesi için, amaçlanan erişimin yetkisiz olduğunu bilmesi gerekmektedir (CPS CMA, 1990). Verilen zarar, herhangi bir yerde insan refahına verilen, herhangi bir yere-çevreye verilen, herhangi bir ülkenin ekonomisine verilen veya herhangi bir ülkenin ulusal güvenliğine verilen zarar şeklinde oluşabilir. Eğer eylem insana zarar verici nitelikte ise, insan yaşamına yönelik kayıp; insan hastalığı veya yaralanması; para, yiyecek, su, enerji veya yakıt arzının bozulması; bir iletişim sisteminin veya ulaşım olanaklarının bozulması; ya da sağlıkla ilgili hizmetlerin aksaması biçimlerinde görülebilir.

2.6.2.2. Polis ve Suç Delilleri Yasası – PACE

1984 yılında kabul edilen kanun (*The Police & Criminal Evidence Act*), polisin şüphelilere yönelik muamalesi, bir kişiyi veya mekanı araması, aramalarda eşyalara el koyması ve sonrasında bunların iadesi vb. arama yetkilerini düzenlemektedir.

İşlemlerin usulüne ve hukuka uygun yürütülmesini sağlayan arama emri, polisin eşyalara el koymasını sağlayacak koşullar, el konulan eşyalara erişim ve kopyalamaya ilişkin yetki ile olayla bağlantısız delillerin araştırma dışı bırakılması gibi düzenlemeler içermektedir (PACE, 1984).

2.6.2.3. Soruşturma Yetkilerinin Düzenlenmesi Yasası - RIPA

2000 yılında yürürlüğe giren RIPA (*Regulation of Investigatory Powers Act*), şüpheli bir kişi hakkında özel bilgilerin elde edilmesi amacıyla, kamu yetkilileri tarafından yapılan dijital gözetim ile kişi veya kuruluş tarafından tutulan dijital iletişime erişime ilişkin yetki gereksinimlerini düzenlemektedir. Gözetleme faaliyeti, şüphelinin hareketlerinin, konuşmalarının veya diğer faaliyetlerin ve iletişimin izlenmesini, gözlenmesini veya dinlenmesini içerir (RIPA, 2000).

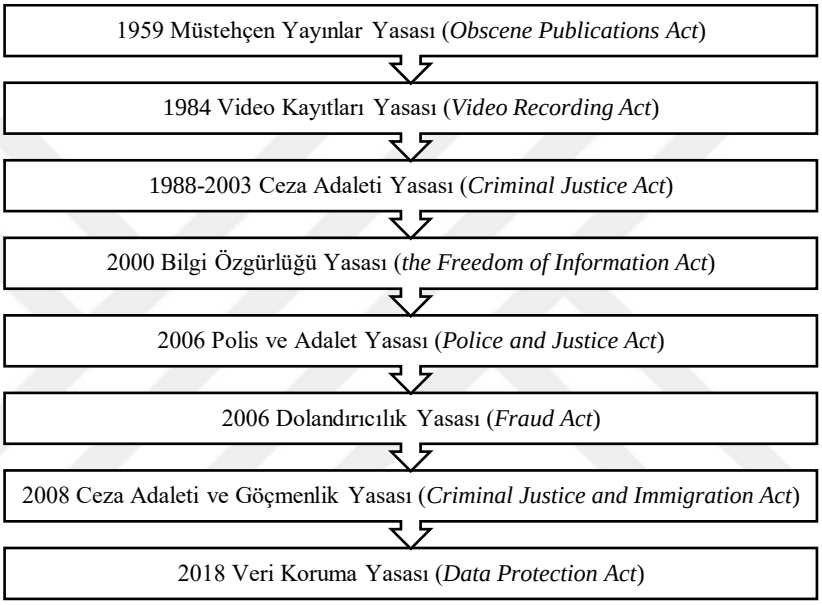
İnternet Servis Sağlayıcıları (ISP'ler - *Internet service providers*), dijital iletişime veya depolanan dijital verilere erişebilen kamu kuruluşları, dijital iletişim ve depolamaya izin veren tesislere sahip işletmeler ve bu işletmelerin bireysel kullanıcıları ve çalışanları kanunun ilgi alanına girmektedir.

2.6.2.4. Ceza Muhakemesi ve Soruşturma Yasası – CPIA

1996 yılında kabul edilen kanun (*Criminal Procedure and Investigations Act*), polis memurlarının bir ceza soruşturmasında elde edilen materyalleri kaydetme, saklama ve yargı makamına sunma kurallarını düzenlemektedir. Elde edilenler

arasında, savcılığın iddialarını zayıflatma veya çürütme özelliği olan, sanık için davayı destekleyen materyaller bulunabilir. Bu tür materyallerin ifşa edilmesinin, adil yargılamanın sağlanması ve adaletin tesis edilmesi noktasındaki önemi kanunun konuları arasındadır (CPIA, 1996).

Birleşik Krallıkta bilişim suçlarıyla dolaylı bağlantıları olan kanunlar Şekil 2.36.'de gösterilmektedir:



Şekil 2.36. Diğer İlgili Kanunlar

2.6.2.5. Örnek Olaylar

- R v Zain Qaiser - Kingston Kraliyet Mahkemesi 8 Nisan 2019

Uluslararası bir organize suç grubunun üyesi olan Qaiser, yasal çevrimiçi reklam ajansları gibi davranmak için sahte kimlikler ve sahte şirketler kullanarak pornografik web sitelerinden kitlesel reklam trafiği satın aldı. Kullanıcıların, reklamlara tıkladıklarında başka bir web sitesine yönlendirilmelerini sağlayan karmaşık kötü amaçlı yazılım türleri ile kullanıcıların tarayıcılarını kilitleyen yazılım kullanmaktaydı. Virüsün bulaştığı cihaz, bir suçun işlendiğini ve mağdurun cihazının

kilidini açmak için 300-1.000 dolar arasında para cezası ödemesi gerektiğini iddia eden kolluk kuvveti veya devlet kurumundan geliyormuş gibi görünen bir mesaj görüntülüyordu. Şantaj mağdurları, fidye talebini önceden belirlenmiş bir sanal para birimi kullanarak ödemeye yönlendirilecek ve bu para daha sonra çeşitli yöntemler ve uluslararası bir yasadışı finansal hizmet sağlayıcı ağı kullanılarak aklanacaktı. Qaiser kendisini durdurmaya çalışanlara DDoS saldırılarıyla karşılık vererek, şirketlerin toplamda en az 500.000 £ kaybetmesine neden oldu. Yakalandığında şantaj, dolandırıcılık, kara para aklama ve bilgisayarın kötüye kullanımı dahil 11 suçu kabul etti ve altı yıl beş ay hapis cezasına çarptırıldı. Bu dava Birleşik Krallık'ın en ciddi siber suç vakası olarak rapor edilmiştir (NCA, 2021).

- R v Daniel Devereux - Norwich Crown Court 16 Haziran 2017

Daniel Devereux, 2015 yılında Norwich havaalanı ile Norfolk ve Norwich hastanesinin web sitelerini hackledi. Havaalanının hack'i, rezervasyonları, varışları ve kalkış panolarını etkiledi, web sitesi üç gün boyunca kapalı kaldı ve ihlalin düzeltilmesi 40.000 sterline mal oldu. Hastane hacklemesi ise klinik prosedürleri etkilemedi. Fail, suç faaliyetleriyle övünen bir video yayınladı ve her iki kuruluştaki personele 'His Royal Gingerness' takma adı altında e-postalar gönderdi. Hem videosundan, hem de web sitelerine erişme girişimlerinden bilgisayarının konumu tespit edildi. Devereux 32 hafta hapis cezasına çarptırıldı (BBC, 2017) ve beş yıl boyunca bir dizi katı kurala uymadıkça ve 150 sterlin ödemeye karar vermedikçe internete bağlı bir cihaza sahip olmasını engelleyen bir Suç Davranışı Emri (CBO) ile cezalandırıldı (Turner, 1992).

2.6.3. Türkiye

Türk hukuk sistemi Kıta Avrupası sistemine dahil olup, Türk Ceza Kanunu (TCK) İtalyan Ceza Kanunu, Ceza Muhakemesi Kanunu (CMK) ise Alman CMK baz alınarak hazırlanmıştır. Bilişim suçları ile ilgili düzenlemelere baktığımızda da diğer birçok Kıta Avrupası hukuk sistemini benimsemiş devletler gibi, ayrı bir kanun

oluşturulmadığı görülmekte, mevcut ceza kanunlarına ilavelerle bir sistem oluşturulmaya çalışıldığı gözlenmektedir.

2004 yılında Resmi Gazete'de yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun "Özel Hükümler – Topluma Karşı Suçlar" başlıklı bölümünde "Bilişim Alanında Suçlar" adı altında bilişim suçları düzenlenmiştir. Bununla birlikte, diğer birçok suç tipinin bilişim sistemleri aracılığıyla işlenmesi halinde verilecek cezalar da ilgili maddelere eklemeler yapılarak tamamlanmıştır. Bilişim suçlarında yürütülecek usul ise, 5271 sayılı Ceza Muhakemeleri Kanunu çatısı altında toplanmıştır.

Kişisel verilerle ilgili hükümler için ise, 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) yürürlüğe girmiş ve GDPR ile uyumlu düzenlemeler yaparak, siber saldırılar sonucu ele geçirilen kişisel verilerle ilgili saldırıya uğrayan bilişim sistemleri sahiplerinin izlemeleri gereken usuller açıklanmıştır. Bununla birlikte, TCK içinde de kişisel veri suçlarına ilişkin cezai yaptırımlar yer almakta, verileri kasten ele geçirme, yayma gibi birçok eylem cezai yaptırıma bağlanmaktadır.

Türkiye'de bilgisayar programları ve yazılımların Telif Hukuku ile korunması, yapılan saldırılar neticesinde bazı telif hakkı ihlallerini de doğurmakta ve "Fikir ve Sanat Eserleri Kanunu" ile düzenlenen hükümleri gündem konusu yapmaktadır. Bunun dışında, elektronik imzaların ve elektronik sertifikaların saldırılara maruz kalmaları da "Elektronik İmza Kanunu"nu devreye sokmaktadır.

2.6.3.1. Türk Ceza Kanunu – TCK

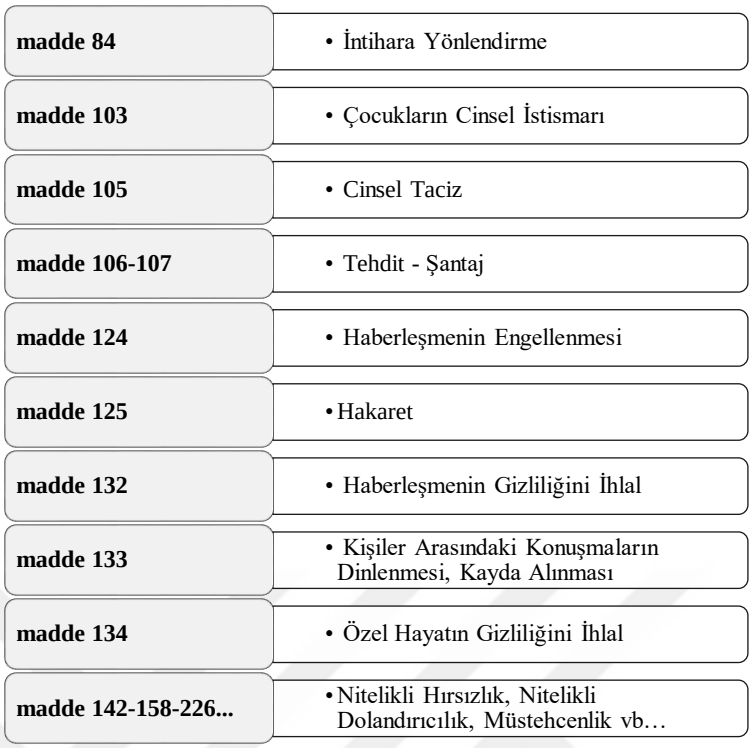
Kanunun "Bilişim Alanında Suçlar" başlıklı bölümünde bilişim sistemlerinin veya verilerin doğrudan hedef alındığı suçlar düzenlenmekte olup, bu suçlara "Doğrudan Bilişim Suçları" denildiğinden önceki bölümlerde bahsedilmişti. Bu

suçlar 243, 244, 245 ve 245A. Maddelerde düzenlenerek yaptırıma bağlanmıştır (Çizelge 2.4.):

Çizelge 2.4. TCK Doğrudan Bilişim Suçları

Madde 243	**Bilişim Sistemine Girme ve Orada Kalmaya Devam Etme Suçu**	– bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek, – bu fiil nedeniyle sistemin içerdiği verileri yok etmek veya değiştirmek, – bir bilişim sisteminin kendi içindeki veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek.
Madde 244	**İşleyişi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**	– bir bilişim sisteminin işleyişini engellemek veya bozmak, – bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek, – bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlemek.
Madde 245	**Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu**	– başkasına ait bir banka veya kredi kartını, ele geçirmek veya elinde bulundurmak, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlamak, – başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek, – sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak.
Madde 245/A	**Yasak Cihaz veya Programlar**	– bir cihazın, bilgisayar programının, şifrenin veya güvenlik kodunun; bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal etmek, ithal etmek, sevk etmek, nakletmek, depolamak, kabul etmek, satmak, almak, başkalarına vermek veya bulundurmak.

Bilişim sistemlerinin başka bir suçu işlemek için aracı olarak kullanıldığı ve "Dolaylı Bilişim Suçu" adıyla bilinen suç tiplerinde ise (Şekil 2.37.), yıllar önce ceza kanunlarında kendine yer bulmuş klasik suç tiplerinin işlenmesinde elektronik cihazlar kullanılmaktadır:



Şekil 2.37. TCK Dolaylı Bilişim Suçları

Bu suçlarda fail kazanç elde etme veya zarar verme amacı gütmektedir. Diğer taraftan bilişim suçlarında temel insan haklarına yapılan müdahaleler de söz konusu olmaktadır. Avrupa Birliği Temel Haklar Bildirgesi'nde (ABTHB, 2007) açıkça belirtilen **"**Özel ve Aile Yaşamına Saygı" ve "Kişisel Bilgilerin Korunması" hakları Türk Anayasası'nda ve Ceza Kanunu'nda da güvence altına alınmıştır.

Anayasa Madde 20'e göre; özel hayatın ve aile hayatının gizliliğine dokunulamaz; herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Maddede sayılı haller dışında kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir (T.C. AY, 1982). Anayasanın bu maddesinin TCK bünyesinde düzenlendiği suçlar Çizelge 2.5.'de gösterilmektedir:

Çizelge 2.5. TCK Özel Hayata ve Hayatın Gizli Alanına Karşı Dolaylı Bilişim Suçları

Md 134	**Özel Hayatın Gizliliğini İhlal Suçu**	– kişilerin özel hayatının gizliliğini ihlal etmek, – gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi, – kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etmek.
Md 132	**Haberleşmenin Gizliliğini İhlal Suçu**	– kişiler arasındaki haberleşmenin gizliliğini ihlal etmek, – bu gizlilik ihlalini haberleşme içeriklerinin kaydı suretiyle gerçekleştirmek, – kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etmek, – kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa etmek.
Md 133	**Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması**	– kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinlemek veya bunları bir ses alma cihazı ile kaydetmek, – katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda almak, – kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa etmek.
Md 281	**Suç Delillerini Yok Etme, Gizleme Veya Değiştirme**	– gerçeğin meydana çıkmasını engellemek amacıyla, bir suçun delillerini yok etmek, silmek, gizlemek, değiştirmek veya bozmak.

TCK içinde siber saldırılar sonucu elde edilen kişisel verilerle ilgili de cezalandırıcı hükümlere rastlanmaktadır. Md 135 uyarınca, hukuka aykırı olarak kişisel verileri kaydeden kişiler cezalandırmaktadır. Eğer söz konusu kişisel veriler özel nitelikli kişisel veri (KVKK md.6) kapsamındaysa, verilecek ceza artmaktadır.

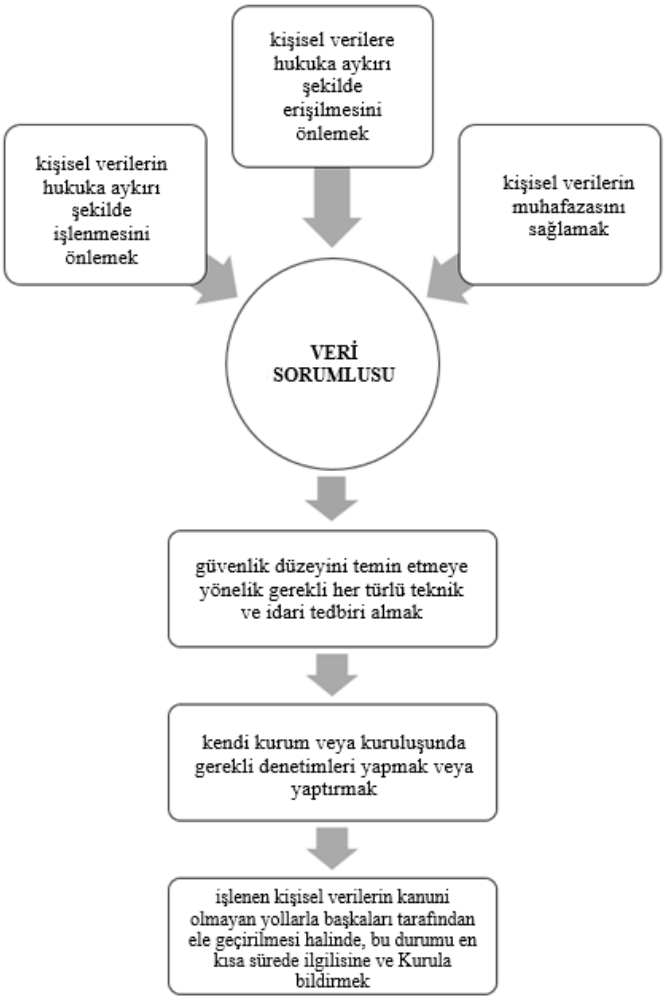
Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçirenler (md 136) ile kanunların belirlediği sürelerin geçmiş olmasına karşın

verileri sistem içinde yok etmekle yükümlü olup görevlerini yerine getirmeyenler de suç kapsamına alınmaktadır (md 138).

2.6.3.2. Kişisel Verileri Koruma Kanunu - KVKK

Türkiye'de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verileri Koruma Kanunu, 95/46/AT sayılı Direktif referans alınarak hazırlanmış olup, temelini Anayasa'nın 20. Maddesi "Temel Hak ve Özgürlükler - Özel Hayatın Gizliliği" nden almaktadır (Özkaya ve Samet, 2020b, s:169).

Bu kanunda, siber saldırılara maruz kalan bilişim sistemlerinden, saldırganlar tarafından ele geçirilen kişisel veriler konusunda sistem sahiplerinin yükümlülükleri düzenlenmektedir. KVKK md. 3/1-ı: **"**kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"yi "Veri Sorumlusu" olarak tanımlamakta ve bu veri sorumlusu md 12 uyarınca Şekil 2.38.'deki sorumlulukları taşımaktadır:



Şekil 2.38. Veri Sorumlusunun Yükümlülükleri (KVKK md.12)

Dolayısıyla, özellikle tüzel kişi konumundaki şirketlerin veya kurumların sistemlerinde herhangi bir güvenlik ihlali olması durumunda bu ihlalin bildirilmesi, tehlikede olan ve kişilerin zararına kullanılacak kişisel veriler açısından zorunluluk arz etmektedir.

Aynı durum adli bilişim soruşturması sırasında toplanan kişisel veriler için de söz konusu olacaktır. Bilişim sistemlerinin araştırılması sırasında, gerek şüpheliyle gerekse üçüncü kişilerle ilgili çok sayıda veri ele geçirilmektedir. Araştırma ve analiz yapan kişiler, uzmanlar ve personel tarafından çokça temas edilen bu veriler, soruşturma ve kovuşturma kapsamı adı altında uzun zaman saklanmaktadır. Bunların haricinde örneğin, CMK md 135'deki iletişimin dinlenmesi ve özellikle kayda

alınmasında kişinin sesi “Biyolojik Biyometrik Veri” olup, özel nitelikli kişisel veri kapsamında kabul edilmektedir. CMK 140. Maddede teknik araçlarla izleme sırasında ise kişi ile ilgili “Davranışsal Biyometrik Veri” dahil çok sayıda veri toplanmaktadır. Bu maddelerde dikkat çeken en önemli husus, maddelerin uygulanmasının sıkı şartlara bağlanmış olmasıdır. Kuvvetli şüphe varlığı, başka türlü delil elde etme imkanının olmaması ve hakim kararı, ilgili maddelerin her durumda kullanılmasını önlemek amacıyla hazırlanmıştır.

Bununla birlikte, yukarıda sayılı maddelere uymadan elde edilecek deliller hukuka aykırı kabul edileceği için ceza yargılamasında kullanılamayacaktır. Burada da hem sanığın haksız yere suçlanması hem de elde edilen kişisel verilerin gizliliğinin sağlanması ve gereksiz yere veri toplanmasının engellenmesi amaçlanmaktadır.

Bu sebeple GDPR ile, tüm devletlerin iç hukuk sistemlerinde bulunması gereken kurallar düzenlenerek yaptırımlara bağlanmıştır. Ceza yargılaması sırasında adli bilişim aşamalarından elde edilen delillerin mahkemelerde kabul edilmesi ve hukuka uygun yargılama yapılabilmesi için kişisel verilerle ilgili düzenlemelere uymak da görüldüğü gibi elzemdir ve artık bir bütünün parçası olmaya çok yaklaşmışlardır.

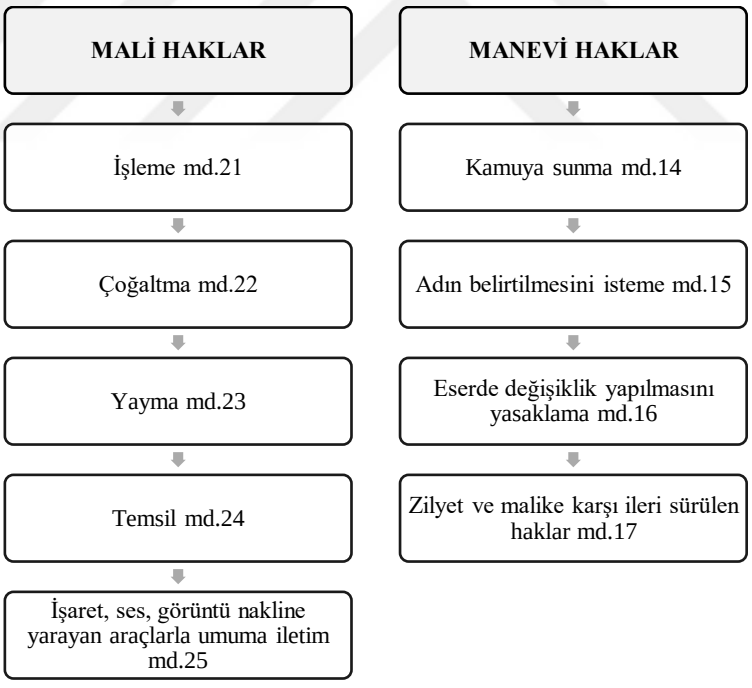
Yukarda da belirtildiği gibi bilişim sitemlerinin diğer ayağını oluşturan programların ve daha geniş anlamıyla yazılımların saldırıya maruz kalması ceza kanunları dışında telif hukukunu da ilgilendiren meseleler olduğundan dolayı Fikir ve Sanat Eserleri Kanunu’ndaki hükümler de önemlidir.

2.6.3.3. Fikir ve Sanat Eserleri Kanunu – FSEK

1951 yılında yürürlüğe giren kanunun 2. Maddesinde bilgisayar programları ve program sonucu doğurması koşuluyla bunların hazırlık tasarımları, İlim ve Edebiyat Eserleri içerinde kabul edilerek koruma altına alınmıştır.

Fikri mülkiyet hukuku olarak bilinen daha geniş yasal düzenlemelerin alt dalı olan telif hakkı, eser sahibinin (bu durumda yazılım sahibinin) çalışmalarını çoğaltma, uyarlama, kamuya açıklama, yayınlama gibi izinsiz kullanımlara karşı korumayı amaçlamaktadır (Özkaya ve Samet, 2020a, s:22).

Eser yani yazılım sahibinin kanun kapsamında mali ve manevi hakları bulunmaktadır (Şekil 2.39.):



Şekil 2.39. FSEK Eser Sahibinin Hakları

Bilgisayar programlarının siber suçlara konu olması telif hakkı hırsızlığı sonucunu doğurarak adli bilişim araştırmasına sebep olabilmektedir. Örneğin, FSEK md. 71'de eser sahibinin rızası dışında gerçekleşecek tecavüz işlemleri, md 72

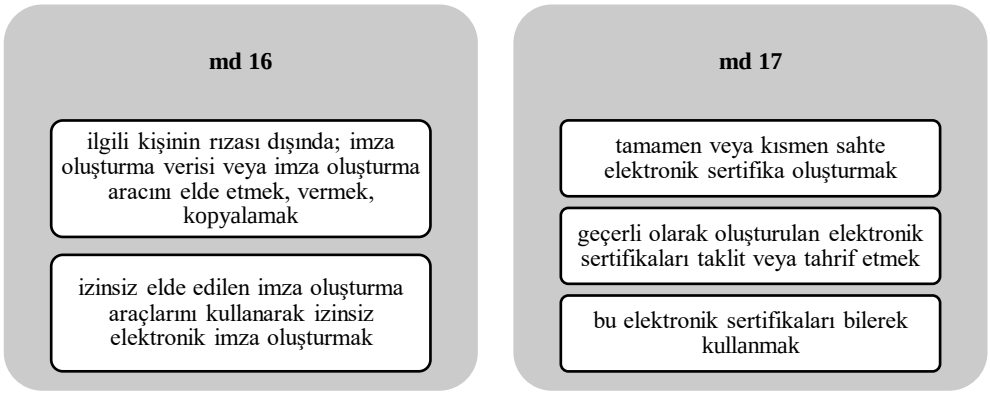
kapsamındaki, bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik faaliyetler ile hackerlar tarafından telif hakkı koruması altında olan bir materyalin internet üzerinden çalınması hallerinde ilgili bilişim sistemlerinin araştırılması ihtimali doğabilmektedir. Diğer taraftan, yazılımcının eser üzerindeki sahipliğini, kriptografi, filigran ve steganografi gibi bilgi gizleme teknikleri (Ablon ve ark. 2014) ve anti-adli bilişim yöntemleri kullanarak sağlamlaştırması ve koruması mümkündür.

2.6.3.4. Elektronik İmza Kanunu - EİK

Bilişim sistemlerinin mevcut olduğu hemen her ortamda siber saldırılar söz konusu olabildiğinden adli bilişimin konusuna giren Elektronik İmza kavramından da burada bahsetmek yerinde olacaktır, çünkü kanuni olarak ıslak imza ile aynı hukuki geçerliliğe sahip olan (EİK md 5) e-imza uygulamasının bir siber saldırıya maruz kalması neticesinde hem özel kişilere, hem de kurumlara ciddi zararlar verilmesine sebep olabilecektir.

2004 tarihinde yürürlüğe giren EİK'in 3. Maddesinde Elektronik İmza; "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmakta, bu imzanın oluşturulması belli donanım ve yazılımlar vasıtası ile söz konusu olurken (md 3-e), doğrulanması için şifre ve kriptografik açık anahtar gibi veriler kullanılmaktadır (md 3-f).

Münhasıran imza sahibine bağlı olan bu güvenli e-imza, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamaktadır. Bu sebeplerle, sahibinin izni olmadan kullanılması veya sertifikalarda sahtekarlık yapılması suç kapsamında kabul edilerek kanunun ilgili maddelerince koruma altına alınmıştır (Şekil 2.40.):



Şekil 2.40. Elektronik İmza Kanununun İlgili Hükümleri

2.6.3.5. Ceza Muhakemesi Kanunu – CMK

Türkiye'de adli bilişimle ilgili kurallar CMK'daki maddeler uyarınca düzenlenmekte olup, bu kurallar uyarınca yargılamanın nasıl yapılacağı mercek altına alınmıştır.

Kanunun 134. Maddesi "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" faaliyetini düzenlemekle birlikte, buradaki "bilgisayar" teriminin içine diğer bilişim sistemlerini dahil etmenin yanlış olmayacağını vurgulamak gerekir. Zira günümüzde bilişim suçları sadece bilgisayarlarla sınırlı olamamakta, içinde delil bulundurma özelliği bulunan pek çok elektronik cihazın suça konu olduğu görülmektedir. Bu açıdan kanunu geniş yorumlamak doğru bir yaklaşım olacaktır. Söz konusu madde uyarınca:

"Bir suç dolayısıyla yapılan soruşturmada,

- somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve
- başka surette delil elde etme imkânının bulunmaması halinde,

- hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından

şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (…) karar verilir.
Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir.
Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
Alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir.” (CMK md 134)

“İletişimin Tespiti, Dinlenmesi ve Kayda Alınması” Suçu ise CMK md.135’de düzenlenmekte ve tıpkı 134.maddedeki gibi somut delillere dayanan kuvvetli şüphenin varlığı ile başka suretle delil elde edilmesi imkânının bulunmaması hali aranmakta ve yine hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararı gerekmektedir. Bu madde kapsamında şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin dinlenebilmesi, kayda alınabilmesi ve sinyal bilgilerinin değerlendirilebilmesi ancak maddede sayılan suçlarla sınırlı olarak uygulanabilmektedir.

Md. 140 “Teknik Araçlarla İzleme” suçunda şüpheli veya sanığın kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenebilmesi ile ses veya görüntü kaydı alınabilmesi, yine aynı şekilde, somut delillere dayanan kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi hâllerinde mümkün

olmakta olup, yine maddede sayılı belirli suçlarla sınırlı olarak ve hâkim, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı kararıyla uygulanabilmektedir.

Hem 135 hem de 140. maddelerde ortak sayılan suçlardan bazıları şunlardır:

- Göçmen kaçakçılığı ve insan ticareti (madde 79, 80), organ veya doku ticareti (madde 91),
- Kasten öldürme (madde 81, 82, 83),
- Nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149) ile nitelikli dolandırıcılık (madde 158)
- Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),
- Parada sahtecilik (madde 197)
- Suç işlemek amacıyla örgüt kurma (madde 220, fıkra üç),
- Fuhuş (madde 227)
- İhaleye fesat karıştırma (madde 235),
- Tefecilik (madde 241),
- Rüşvet (madde 252),
- Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),
- Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302) ,
- Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),
- Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları

Şekil 2.41. CMK md 135 ve md 140'da Düzenlenen Sınırlı Sayılan Ortak Suçlar

2.6.3.6. Örnek Olaylar

- "...@hotmail.com" e-posta adresi ile bağlantılı olan facebook adresinin, sahibinin bilgisi ve rızası olmaksızın değiştirilerek erişilmez kılınması sonucu açılan davada, olaya ilişkin tüm deliller toplanmadan soruşturma ve kovuşturma yürütülmesi ile mahkumiyet kararı verilmesi sonucunda yerel mahkeme kararı Yargıtay tarafından bozulmuştur. İlk derece mahkemesinin, söz konusu e-posta adresinin faal olup olmadığını, katılanın kendi adresine erişim sağlayıp

sağlamadığını tespit etmeden ve e-posta adresine ait şifrenin değiştirilip değiştirilmediğini, değiştirilmişse erişim yapılan IP numarası ile değiştirilme tarihi konusunda internet sağlayıcısından bilgi alınmadan ve bilirkişi görüşü alarak sanığın hukuki durumunu takdir ve tayin etmesi gerekirken, eksik araştırma yaparak hüküm kurmasının kanuna aykırı olması sebebiyle karar bozulmuştur (Yargıtay 8CD, 2014 /19342).

- Clickbus Seyahat Hizmetleri A.Ş. internet sistemlerinde zararlı bir işlem olabileceğine ilişkin aldığı uyarı üzerine adli bilişim uzmanlarının yardımına başvurmuştur. İncelemeler neticesinde, bazı şüpheli faaliyetler yakalanmış, sunucularda bazı zararlı dosyalar ile bazı meşru kaynak kod dosyalarının Clickbus'ın sunucularına uzaktan erişim sağlanmasına izin veren zararlı kodları içerecek şekilde modifiye edildiği tespit edilmiştir. Veri sızıntısının yaklaşık 2 ay sürmesi, bu sızıntıdan yaklaşık 67.519 kişinin etkilenmesi ve farklı kategorilerde ve çok sayıda kişisel verinin ele geçirilmesi sebebiyle Kişisel Verileri Koruma Kurulu ("Kurul"), Şirketin yeterli teknik ve idari tedbirleri almaması, sistemlerinde ciddi bir güvenlik açığı olması ve kanunda belirtilen veri ihlalini bildirme yükümlülüğünü zamanında yerine getirmemesi gerekçeleriyle toplam 550.000 TL idari para cezası uygulanmasına karar vermiştir (KVK Kurulu, 2019/141).

- Bir oyun şirketindeki oyuncu verilerine hackerlar tarafından yasal olmayan yollarla hukuka aykırı erişim gerçekleştirildiğinin, bulut sistemlerine erişimin log kayıtlarından anlaşıldığının, sistemdeki oyuncu giriş bilgilerinin değiştirildiğinin ve ihlalden 39,995 kişinin etkilendiğinin tespit edildiği olayda, Kurul toplam 1.100.000 TL idari para cezası uygulanmasına karar verilmiştir. Bu kararın gerekçesinde; "bulut sistemi bulunan veri tabanına saldırganlar tarafından erişim sağlanmasının yapılan zafiyet testlerinin yetersiz olduğunun ve gerekli önlemlerin alınmadığının ve Veri sorumlusu tarafından ihlal öncesi alınması gereken ancak ihlal sonrası uygulanan teknik ve idari tedbirlerin zamanında alınmadığının göstergesi olduğu" belirtilmiştir. Teknik tedbirler olarak da; "güvenlik ajanının ağ sistemine konuşlandırılması, kötü niyetli IP adreslerinin sistemden engellenmesi, oyuncu hesaplarının yetkisiz erişimlerden korunması için gerekli önlemlerin alınması, hackerlar tarafından

kullanılan mekanizmaların ve IP'lerin gözlenmesi için 7x24 gerçek zamanlı gözetleme sistemini de içeren, geliştirilmiş gözetleme ve alarm sistemlerinin faaliyete geçirilmesi örnek olarak gösterilmiştir" (KVK Kurulu, 2020/286).

3. BULGULAR

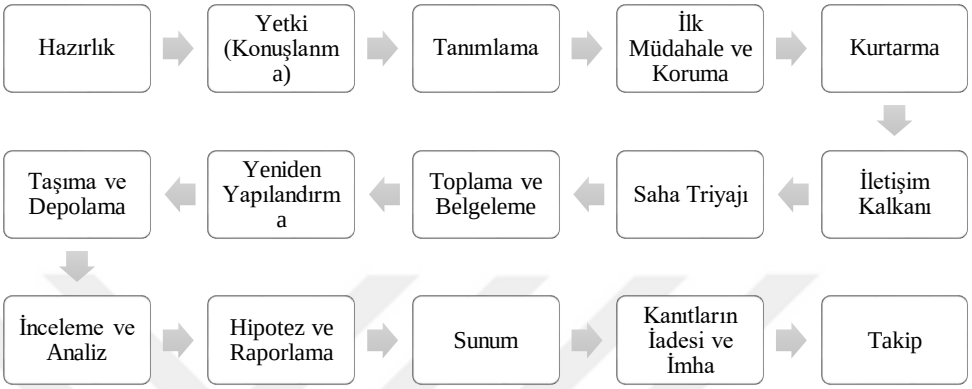
Suça konu bir olay meydana geldiğinde olay yeri araştırmalarının suçun basit veya karmaşık olmasına bakılmaksızın en ince detayına kadar ve eksiksiz şekilde yürütülmesi, soruşturma ve kovuşturma süreçlerinin hukuka uygun şekilde gerçekleştirilerek suçun aydınlatılmasında hayati öneme sahiptir. Bu sebeple, bir önceki bölümde de açıklandığı üzere, adli bilişim alanında çalışan uzmanlar ve araştırmacılar tarafından ortak özellikleri ve farklılıkları bulunan birçok model oluşturulmuştur. Adli bilişim araştırmalarına yol gösteren bu modellerin bazıları aşamaları geniş tutarken, bazıları daha çok basamakla detaylandırmayı tercih etmiştir. Bu amaçla bu tez çalışmasında incelenen modeller referans alınarak bir öneri model sunulmuş, bu modelle araştırma ve analiz yapacak uzman ve personelin görevlerinin belirlenmesinde ve işlemleri gerçekleştirmelerinde eksiksiz hareket etmelerine yardımcı olmak amaçlanmıştır.

3.1. Önerilen Model

Önceki bölümlerde anlatılan modellerin her biri kendi içinde faydalı basamaklar barındırmakta ve yeni yaratılacak modellerin oluşturulmasına ilham verici özellikler taşımaktadır. Her modelin bu değerli basamaklarının harmanlandığı yeni bir model düşüncesinin olgunlaşıp uygulamaya konulması, gelişen teknolojilere ve çeşitlenen suç türlerine uyum sağlaması konusunda önemli bir ihtiyaç haline gelmektedir. Kuşkusuz ki geniş aşamalı ve detaylı işlem yapan bir modelin, araştırmacılar için, hem analizleri şüpheye yer bırakmayacak şekilde şeffaf ve doğru yürütmeleri açısından yol gösterici, hem görev tanımlarını netleştirici hem de davanın tarafları için aydınlatıcı özellikleri olacaktır.

Bu yeni modelin bulut bilişim ve IoT modellerinin dışındaki, yerleşik depolama alanlarının bulunduğu bilişim sistemleri için genel özellik taşıyacak nitelikte oluşturulması, bulut bilişim ve IoT bilişimin araştırma bölümlerinden biri

olan bu alanın faydalı bir şekilde analizini sağlayarak diğer araştırmaların yürütülmesini kolaylaştıracaktır. Bu kapsamda yukarıda anlatılan modellerde kullanışlı olduğu düşünülen basamaklar esas alındığında en kapsamlı modelin çerçevesinin çizilmesi gerekmektedir.



Şekil 3.1. Önerilen Model

Şekil 3.1. üzerinden bakıldığında, en bilinen ve klasikleşmiş adli bilişim aşamaları hariç tutulursa, bir modelde bulunması gereken diğer aşamaların şu şekilde düzenlenmesi gerektiği söylenebilir:

Modellerin çoğunda bulunan "hazırlık" aşaması bir modelde bulunması gereken en temel aşamadır. Kullanılacak yazılım ve donanımlardan, olayla ve ekipmanla ilgili uzmanlaşmış araştırmacılara kadar olay yeri incelemeye yardımcı olacak materyallerin ve kişilerin belirlenmesi bu aşamada gerçekleştirilmelidir.

IDIP ve EIDIP modellerindeki konuşlanma aşaması "yetki"aşaması olarak, yasal izin ve onaylar bakımından hukuka uygun uygulamalarda olmazsa olmaz koşuldur.

Sistematik modelin "iletişim kalkanı" aşaması incelenen sistemlerin diğer cihazlarla olan iletişimlerinin kesilerek delil bütünlüğünün korunması açısından önemli bir aşamadır.

Saha Triyaj modelindeki "triyaj" aşaması, laboratuvara götürülmeden olay yerinde sistemlerin analizine ve yorumlanmasına fırsat verdiği için işlemleri oldukça hızlandırıp kolaylaştırabilecek bir adım olacaktır. Özellikle uçucu verilerin canlı ediniminde faydalanılmalıdır.

IDIP ve EIDIP aşamalarınada karşımıza çıkan ancak Lee (2001), Casey (2000 ve 2004), Cohen (2010) ve Kohn (2013) tarafından da irdelenen "Yeniden yapılandırma" aşaması; adli bilişim sürecinde elde edilen çıktıları ve diğer ilgili bilgileri bir araya getirerek, olayların meydana gelişini ve suçun oluşumunu yeniden sahnelemek ve sonucun nasıl elde edildiğini kanıtlamak için gereklidir.

"Kanıtların iadesi ve imha"; incelenmek üzere alınan materyallerin gerekli işlemler sonlandıktan sonra sahibine iadesini ve araştırmayla ilgisi olmayan elde edilmiş verilerin imhasını içermektedir. Veri koruma kanunlarında özellikle vurgulanan kişisel verilerin gizliliği hususunun uzantısı olan bu basamağın mutlaka dikkate alınması gerekmektedir.

IR modelinin "takip" aşaması ise araştırma sırasında tespit edilen yanlışların, eksiklerin ve sorunların düzeltilerek uzun vadeli çözüm bulunması için kullanışlı olacaktır.

Bölüm başında da belirtildiği gibi, adli bilişimin ilk ortaya çıkışından günümüze kadar çok sayıda model geliştirilerek, sistem üzerindeki eksiklikler giderilmeye, yapılan hatalar düzeltilmeye çalışılmıştır. Pratiklik, maliyet düşüklüğü, şeffaflık ve hukuka uygunluk gibi amaçlarla, tespit edilen ihtiyaçlar doğrultusunda hareket edilmiştir. Modellerin çoğu ortak aşamalar içermekle birlikte, bazen aynı isimdeki süreçlerin içinde farklılıklar taşıdığı görülmüş, bazı modeller aşamaların sayısını azaltıp birleştirirken, bazı modeller aşama sayısını genişletip detaylandırmıştır.

Modellerle ilgili bölümde de açıklandığı gibi, bu tez çalışmasında, birbirine benzer aşamaları taşıyan modellerden en kapsamlı olanlar ile bu alanda en çok faydalanılan ve temel alınan modeller seçilerek gelişme süreci anlatılmaya, genel bir çerçeve çizilerek adli bilişim biliminin şu anki sınırları gösterilerek, gelecekte, bu sınırların ne kadar genişleyebileceğine ilişkin fikir verilmeye çalışılmıştır. Sonraki bölüm, modelleri toplu halde görebilmek ve benzerliklerle farklılıkları kolay tespit edebilmek için model karşılaştırmalarına ayrılmıştır ve karşılaştırmalar tezde açıklanan modellerle sınırlı tutulmuştur.

3.2. Modellerin Karşılaştırılması

Bilişim suçlarının araştırılması ve soruşturulmasının önem kazanmaya başladığı yıllardan, yakın tarihe kadar geliştirilen en bilinen ve en temel modeller Çizelge 3.1.'de gösterilmektedir. Suç konusu olay meydana geldiğinde, adli bilişim sürecinin devreye girmesiyle birlikte soruşturma üç bölüme ayrılarak, her bölüme karşılık gelen süreçler ve her uzman/uzman grubunun hangi aşamayı modellerine dahil ettiği işaretlerle gösterilmiştir.

Çizelge 3.1. Adli Bilişim Modellerinin Karşılaştırılması (Zulkipli ve ark., 2017, s:321)

MODELLER	HAZIRLIK	ELDE ETME	DEĞERLENDİRME	TANIMLAMA	TOPLAMA	KORUMA	İNCELEME	ANALİZ	SUNUM	RAPORLAMA	BELGELEME	YAYGINLAŞTIRMA	GERİ BİLDİRİM
Önerilen Model	●			●	●	●	●	●	●	●	●		
DFRWS				●	●	●	●	●	●				
IR	●	●		●	●	●	●	●	●	●			
Soyut Model	●			●	●	●	●	●	●				
IDIP	●			●	●	●	●		●		●		
EIDIP	●				●	●		●			●		
Genişletilmiş Siber Suç Araştırma Modeli				●	●	●	●	●	●			●	
Ortak Model – CM		●			●			●		●			
Malezya Modeli	●			●	●	●	●	●	●				
Sistematik Araştırma Modeli	●			●	●	●	●	●	●				
Bulut Bilişim İçin Çerçeve				●	●	●	●	●	●	●			
Veri Azaltma ve Veri Madenciliği Çerçevesi	●			●	●	●	●	●	●				
	SORUŞTURMA ÖNCESİ AŞAMALAR			SORUŞTURMA AŞAMALARI						SORUŞTURMA SONRASI AŞAMALAR			

Tabloda dikkat çeken hususlardan biri, modellerin soruşturma aşamasına ağırlık vererek, öncesinde ve sonrasındaki süreçlere yeterli dikkati vermedikleridir. Örneğin hazırlık aşamasının uzantısı olan değerlendirme aşaması hiçbir modelde bulunmuyorken, raporlama aşaması beklenilenin aksine modellerin çoğunda bulunmamaktadır. Her ne kadar tabloda bulunmasa da, belirlenen prosedürler ile gerçekleştirilen fiillerin amaca hizmet edip etmediği noktasında bilgilendirme açısından faydalı olan geribildirim aşamasının önemi ise en son geliştirilen modeller tarafından yeni fark edilmeye başlanmıştır.

Ciardhuáin'nin "Genişletilmiş Siber Suç Araştırması Modeli" süreçleri en detaylı ayıran modellerden biridir. Bu sebeple, aynı/benzer aşamalar taşıyan diğer modellerle karşılaştırılması Çizelge 3.2.'de gösterilmektedir:

Çizelge 3.2. Genişletilmiş Siber Suç Araştırması Modeli'nin Karşılaştırılması (Ciardhuáin, 2004, s:10-11).

GENİŞLETİLMİŞ (Ciardhuáin, 2004)	**DFRWS** (Palmer, 2001)	**SOYUT** (Reith, 2002)	**IDIP** (Carrier, 2003)	**EIDIP** (Baryamureeba, 2004)	**MALEZYA** (Perumal, 2009)	**SİSTEMATİK** (Agarwal, 2011)	**VERİ MADENCİLİĞİ** (Quick ve Choo, 2014)	**ÖNERİLEN MODEL** (Özkaya, 2021)
Farkındalık		✓						
Yetki			Konuşlanma	Konuşlanma	✓			✓
Planlama		Hazırlık	Hazırlık	Hazırlık	✓	Hazırlık	Hazırlık	Hazırlık
Bildirim			✓	✓				
Arama Tanımlama	✓	✓	✓		✓	✓	✓	✓
Toplama	✓	✓	✓		✓	✓	✓	✓
Taşıma					✓			✓
Depolama					✓		✓	✓
İnceleme	✓	✓	✓			✓		✓
Hipotez	Analiz	Analiz	Analiz		Analiz	Analiz	Delil Analizi	✓
Sunum	✓	✓	✓	✓	Sonuç	✓	✓	✓
Kanıt Savunma	Karar				✓			
Yayılma								

Modeller arasında araştırma süreçleri içerik olarak birbirine benzese de, süreçleri tanımlamak için kullanılan terimlerde farklılıklar göze çarpmaktadır. Hatta bazı modeller bir aşama adı altında birkaç süreci birden yürütebilmektedir. Karşılaştırmalarda sadece terime odaklanmak yerine içeriğini baz alarak karşılaştırma yapmak bu açıdan daha mantıklı görünmektedir. Çizelge 3.2.'de aynı isimli aşamalar "✓ " sembolüyle gösterilirken, aynı/benzer özellik gösteren aşamaların ilgili yerlerine, o modelde tanımlanan terimler eklenmiştir.

"Koruma" aşaması, DFRWS, Soyut Adli Bilişim Modeli, IDIP, Sistematik Adli Bilişim Modeli ve Veri Madenciliği modellerinde bulunurken, "Gözden Geçirme" aşaması, IDIP, EIDIP ve Veri Madenciliği modellerinde yer almaktadır. Diğer taraftan "Veri azaltma ve Veri Madenciliği" basamaklarının, Veri Madenciliği Modelinde yer alması özelliği itibariyle şaşırtıcı olmamakla birlikte, adli bilişimin ilk dönemlerinde öncü konumundaki DFRWS konferansında konu edilmesi, öngörüsel ve amaçsal bakımdan önemlidir.

4. TARTIŞMA

Modellerin adli bilişim alanında açtığı yol, gerçekleşen suç konusu olaylarda yapılan araştırmaların ve soruşturmaların paralel bir düzene oturtulması gereğinin önemini göstermiştir. Birbiriyle benzer ve birbirinden farklı model çalışmaları, kamu ve özel sektör kuruluşların prosedürler oluşturmasını beraberinde getirmiş ve tavsiye niteliğindeki "En İyi Uygulama" rehberlerinin ortaya çıkmasını sağlamıştır. Birçok ülke kendi yasal mevzuatlarıyla da uyumlu, genel içerikli veya özel hususlar barındıran bu rehberleri esas alarak çalışmalarını sürdürmektedir.

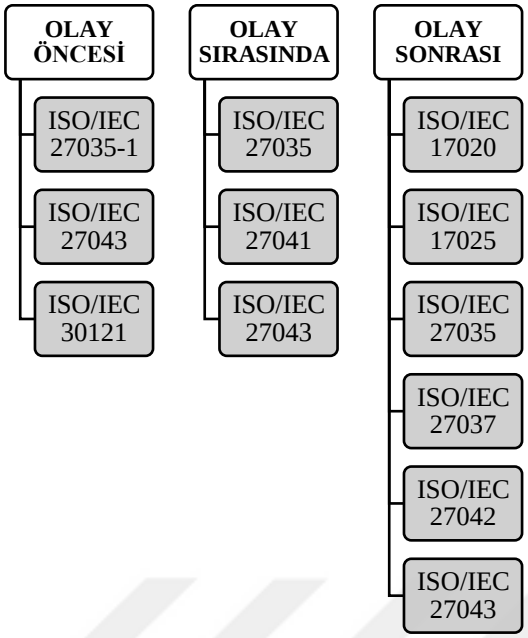
En iyi uygulama rehberleri başta bilgisayarlar olmak üzere üzerinde veri depolama üniteleri olan bilişim sistemlerini esas alan düzenlemeler yaparak, gerek ilk müdahalecilere, gerek kolluk kuvvetlerine gerekse diğer uygulayıcılara yol göstermeyi hedeflemektedir. Bahsi geçen ilkeler uygulanması zorunlu kurallar olmayıp tavsiye niteliği taşımaktadır ancak modellerle şekillenen adli bilişim süreçleri içinde yer alan basamaklar için düzenlenmiş kurallar olmaları bakımından resmiyet kazandığı rahatlıkla söylenebilir. Nasıl ki modeller adli bilişim süreçlerinin bel kemiğini oluşturmuşsa, en iyi uygulamalar da bu basamakların her birine uygulanacak temel kurallar haline gelmiştir.

Tez kapsamında önerilen model dahilinde, anlatılan en iyi uygulama rehberlerinin uygulanabilirlik durumları örnek olarak gösterilebilir. Şöyle ki; NIJ'in 'ilk müdahaleciler rehberi' önerilen modelin birçok aşamasını karşılamaktadır. Olay yerine giden ilk müdahalecilerin gerekli müdahaleleri yapmadan önce gerçekleştireceği hazırlık faaliyetlerini, almaları zorunlu yasal izinleri, olay yerinde buldukları materyaller, cihazlar ve potansiyel delillerin tanımlanması ve belgelenmesi faaliyetlerini, bu delillerin kaybolmasını ve bozulmasını önlemek adına gerek olay yerinde gerekse taşıma esnasındaki koruma altına alma faaliyetlerini düzenleyerek örnek modelin sınırlarını göstermektedir. Benzer şekilde 'NIJ kanun uygulama kılavuzu' da hazırlık ve ilk müdahaleden sonraki süreçlerde kolluk kuvvetleri için kanıtların değerlendirilmesi, edinilmesi, incelenmesi, belgelenmesi ve

raporlanması konularında yol göstericidir. Yine NIJ'in 'cihazlar, araçlar ve teknikler rehberi', araştırmada kullanılacak yazılımların, donanımların, cihazların ve tekniklerin, delillerin değişmeden elde edilmesi, incelenmesi, korunması ve taşınması hususlarındaki önemi bakımından önemli bir kılavuzdur. SWGDE'nin 'canlı sistemlerin yakalanması rehberi' örnek modelin "triyaj" aşamasını ve uçucu verilerin canlı edinimini konu almaktadır.

Gerek gerçek kişiler, gerekse kurum ve kuruluşlar, bilişim sistemleri ve elektronik cihazlarla çok sayıda veri üretmekte ve bu veriler davaya konu olduğunda dijital delillere dönüşmektedir. Bu verilerin işlenmesi, saklanması ve yönetimi konusunda kuruluşların politikalarının olması zorunludur. Bu politikalar yasal otoriteden alınacak izinlerden, delillerin bütünlüğünün sağlanmasına, faaliyetlerin belgelenmesinden kalite yönetimine kadar geniş bir yelpazeyi oluşturmaktadır ve ilgili kuruluşlarca verilen standartlarla sahiplik ispatlanmaktadır.

Bahsi geçen standartların temsilcisi olarak, en temel ve yaygın standartlardan ISO referans alınırsa, adli bilişime konu bir olay meydana geldiğinde, olayın gelişimine göre ISO'nun farklı standartları uygulama alanına girmektedir (Şekil 4.1.):



Şekil 4.1. Adli Bilişim Aşamaları İçin Önerilen Standartlar (Grobler, 2012, s:7)

Uluslararası arenada uygulanabilirlik yetkinliği olan ISO'nun bahsi geçen standartlarından bazılarını örnek olarak önerilen modele uyarlamak gerekirse; ISO 27037 Standardı, olay yerine ilk müdahale edenler, dijital delilleri inceleyenler ve laboratuvar yöneticileri için hazırlanmış bir standart olarak, delillerin tanınması, taşınması, analizi ve korunması hususlarını düzenleyerek örnek model için uygulanabilirlik özelliği taşımaktadır. ISO/IEC 27035 ise, aşamalardaki politikaların belirlenmesi, olay müdahale ekibi kurulması, güvenlik operasyonlarının hazırlanması gibi düzenlemelerle, hazırlık aşamasından sunum aşamasına kadar olan tüm süreçler için bilgi güvenliği olay yönetimi sistemini benimsemiştir. Örnek model bazında zorunlu bir standart olduğu açıktır.

Adli bilişim araştırmaları sonucunda elde edilen verilerin analiz edilerek adli makamlara sunulacak niteliğe kavuşturulmalarında görevli olan laboratuvarlar, yeterliliklerini ve yetkinliklerini akredite edilmeleriyle kazanmaktadır. İhtiyaçların, faydaların ve mevcut durum analizinin yapılması, politika ve prosedürlerin belirlenmesiyle başlayan akreditasyon süreci, ilgili bağımsız kurumun gerekli denetimleri yapması ve karar vermesiyle tamamlanmaktadır. Kullanılacak bilişim sistemlerinin, verilerin ve delillerin güvenliğinden binaların fiziki güvenliğine,

personelin teknik eğitiminden, adli bilişim süreci konusunda bilinçlendirilmesine kadar birçok faktörde kendilerini ispatlamaları beklenmektedir.

Akreditasyonun sağlanmasında temel belirleyiciler, uluslararası alanda kabul görmüş standartların laboratuvar koşullarının hazırlanmasında belirleyici olmasıdır. Bu alanda yine en bilinen standartların ISO tarafından oluşturulduğu görülmektedir. Bu standartlar tez kapsamında önerilen model için uygulama alanı bulabilecek niteliklere sahiptir. Şöyle ki; ürün, mal ve hizmet kalitesi, sistem ve tesis güvenliği ile adli bilişim laboratuvarlarının süreç ve prosedürleri için ISO 17020; ekipman, test ve kalibrasyonlar, laboratuvar yönetimi, çalışan personel ile ilgili süreç ve görev tanımlamaları için ISO 17025; bilgi güvenliği ve gizliliği için ISO 27001 ve 27002, kalite planlaması ve güvencesi ile kalite kontrol işlemleri için ISO 9001 dikkate alınması gereken standartlar olacaktır.

Bilişim sistemleri ve üzerinde depolama üniteleri bulunan elektronik cihazlardan elde edilen verilerin davalarda delil olarak kullanılmaya başlamasından itibaren, bu sistemlerin içeriğinin analizi için çeşitli donanım ve yazılımlar üretilmeye başlandı. Bunlardan en iyi verimin alınması için bu aygıtların geliştirilmesi, güncellenmesi ve kullanımı noktasında nitelikli ve eğitimli iş gücünün olmazsa olmaz koşul olduğu farkedildi. Bu kapsamda, adli bilişimde lider konumda olan adli bilişim araç üreticileri, ürettikleri araçların kullanılması konusunda tanıtımlar yaparken, kullanıcılar için çeşitli eğitimler oluşturdu. Adli bilişim bir bilim dalı olarak kabul edildikten sonra, bu alanla ilgili kamu ve özel sektör kurumlar, araştırma kuruluşları ve üniversiteler de bu alanda çalışmalar yapmaya başladı.

Her cihaza hakim konumda olmaya çalışan uzmanlardan ziyade, her bir sistem için ayrı ve bağımsız olarak uzmanlaşmış kişilerin bu bilim içerisinde daha faydalı ve verimli olacağının anlaşılmasıyla verilen eğitimler de kendi içinde alanlara ayrılmaya başladı; bilgisayar, mobil cihazlar, ağ, multimedya, ses analizi, görüntüleme sistemleri, malware analizi, akıllı ev, IoT, oyun konsolu araştırmaları vb..

Teknolojideki durdurulamaz gelişim tüm hızıyla devam ederken, yeni dijital cihazların ve depolama alanlarının üretilmesine devam edilmekte ve geçmişte hazırlanan eğitim müfredatının ve sistem analizlerinin bugünkü birçok sistemde karşılığının olmadığı görülmektedir. Adli bilişim uzmanlarının ve araştırmacıların kendilerini yeni gelişen teknolojilere göre güncellemesi ve geliştirmesi gerekmektedir. Teorik eğitimin bel kemiğini oluşturan lisans ve lisansüstü eğitimler, sertifika programları, kurslar ve konferanslar ile pratik eğitimi oluşturan suç senaryosu, olay yeri inceleme stajı veya laboratuvar analiz uygulamaları gibi yöntemlerle gerekli yetkinliğin sağlanmasına çalışılmalıdır. Uzmanlığı ispatlayıcı nitelikteki sertifikaların geçerlilikleri belirli sürelerle sınırlandırılıp güncellikleri teorik ve pratik eğitimlerle sağlanarak, sınav metoduyla sabitlenmelidir.

Elbetteki bu eğitimlerin sadece bilişim sitemlerini kullanan teknik kısımla sınırlı kalmaması, bu alanda çalışan hukukçuların da sisteme dahi edilmesi önemlidir, çünkü adli bilişim, içinde çok sayıda hukuki kuralın bulunduğu bir alandır ve her araştırmanın sonucu mahkeme salonunda sonlanmaktadır. Adli bilişim uzmanı olacak kişilerin her iki disiplinde de hakim konumda olması yargılamanın başarısı için hayati önem taşımaktadır.

Tez kapsamında önerilen modelde öngörülen aşamalarda görev alacak personel ve uzmanlar, basamaklara denk gelen konularda önceki bölümlerde bahsi geçen temel eğitimlerden ve uzmanlık eğitimlerinden alıp, sınavları başarıyla geçtikleri takdirde modelden beklenen faydaya önemli katkılar sağlayabilirler. Ülkemiz açısından, açıklanan bu en iyi uygulamalar, standartlar ve eğitimler, yerel kurumlar ve üniversiteler açısından hazırlanacak eğitim müfredatları ve sertifika programları açısından ilham verici kabul edilerek, geliştirilmeye müsait konulardır.

5. SONUÇ VE ÖNERİLER

Adli bilişim nispeten yeni bir alan olmakla birlikte, gelişimi hızla artan bir ivmeye sahiptir. Teknolojinin gelişen tüm imkanlarından faydalanan siber suçlular, adli bilişimin de evrimleşmesinin yolunu açıyor olsa da, alanın hala birçok eksiğe sahip olduğu da bir gerçektir. Uzmanlar ve araştırmacılar tarafından oluşturulan modellerle şekillenen alan, sonrasında en iyi uygulamalar ve standartlarla bir zemine oturtulmaya çalışılmıştır. Alanın temel direklerinden biri olan hukuk bilimi ise, gerek bilişim suçları gerekse adli bilişim kurallarının yasal prosedürleri açısından gelişmenin gerisinde kalarak ayak uydurmakta zorlanmaktadır.

Adli Bilişimin bu multidisipliner alan olma özelliği, kurallar ile teknik ve yasal hususları birlikte barındırmaktadır. Yapılacak herhangi bir işlemin hukuka aykırı olması, sonradan çok sayıda problemi beraberinde getirmektedir. Türkiye'de bilişim suçları ve adli bilişim prosedürleri Türk Ceza Kanunu ve Ceza Muhakemeleri Kanunu içerisine birkaç madde eklenmesi suretiyle düzenlenmiştir ve bu düzenlemeler oldukça yetersiz olup yeni gelişmelere uyum sağlayamamaktadır. Bu sebeple ilgili teknik hususların da yer aldığı, çerçevesi iyi çizilmiş, detaylı şekilde hazırlanmış ve hızlı gelişmelere hazır düzenlenmeler yapılması elzemdir. Sınırötesi özelliği olan bilişim suçları için yapılacak bu düzenlemelerin, tüm ülkelerle paralel hükümler içermesi ve uygulamaların da aynı sistem üzerinden yürütülmesi zorunludur. Bu sebeplerle Türkiye'de bağımsız, detaylı ve güncel bir kanuna olan ihtiyaç her geçen gün artmaktadır ve bahsedilen paralelliğin sağlanması için ülkelerin bu alanda ortak bir çalışma yürütmesi gerekmektedir.

Benzer şekilde, uluslararası düzenlemelere uygun en iyi uygulama rehberlerinin de hazırlanması kanunları ve uygulamaları desteklemesi bakımından önemlidir. Türkiye'de bu alanda yapılmış herhangi bir resmi düzenleme olmadığı görülmektedir. Mevcut kurallar da özetler halinde ve yetersiz içeriktedir.

Her olay ve her duruma uygun, belirlenmiş standartlar çerçevesinde gerçekleştirilen uygulamalar, dünya çapında kabul görme, coğrafi ve yasal sınırlar arasında uyum sağlama ve ortak metodoloji oluşturma açısından bir gerekliliktir. Uluslararası kabul görmüş bir standarda sahip olmak, uluslararası arenada konunun uzmanı birçok kişinin güvenilir referansını da almak demektir (Grobler, 2010, s:262) ve standartlar, karşılıklı güvenin ve iş disiplininin oluşması bakımından gereklidir. Adli olaylarda farklı araştırmacıların tüm aşamaları ele alırken standartlaştırılmış bir süreci uygulaması, araştırmaların şeffaf ve eşit yürütülmesi açısından büyük öneme sahiptir (Grobler, 2012, s:4). Özelikle uluslararası nitelikli standartların küresel bazda iş yapan işletmeler veya sınır ötesi niteliği olan bilişim suçları ile ilgili davaların delillerinin analizini yapan laboratuvarlar bakımından ayrı bir özelliği bulunmaktadır (AIAC, 1998).

Diğer laboratuvarlarda olduğu gibi adli bilişim analizi için kurulacak laboratuvarlarda da yapılan işlemlerin doğruluğunu ve güvenirliğini etkileyen pek çok faktör bulunmaktadır. Metodlar, yazılımlar, donanımlar ve diğer cihazlar ilk etapta baş etkenler gibi görülse de, bu materyalleri çalıştıracak ve kullanacak insan faktörünün gerekli bilgi, beceri ve yeterlilikte olup olmaması, yasalardan, tekniklerden ve risklerden haberdar olup olmaması, oluşabilecek herhangi bir fiziki veya siber saldırıya karşı hazırlıklı olup olmamasının daha önemli bir faktör olduğu söylenebilir, çünkü kullanılacak yazılım, donanım ve cihazların kullanım, bakım, onarım, güvenlik ve güncelleme işlemlerini yürütecek olan yine insandır ve bu noktada en önemli yatırımın insana yapılması, diğer faktörlerin başarısını da etkileyecektir.

Adli bilişim uzmanları ve araştırmacıları açısından ise Türkiye'de eğitim konularında ayrı boşluklar bulunmaktadır. Yazılım araçlarının yabancı kaynaklı olması ve yerli araçların kullanılmaması, yazılımlar üzerindeki yetkinlik için yine yabancı şirketlerle muhatap olma zorunluluğuna neden olmaktadır. Türkiye'de özellikle kolluk mensupları tarafından gerçekleştirilen adli bilişim uygulamalarının, kamu ve özel sektör açısından da uygulanabilir olması hem suçla mücadelede farklı alanlardan gelen kişilerin de bu alana dahil edilerek katkı sunması, hem de

akademide bilimsel çalışmaların geliştirilmesi açısından önemlidir. Bireysel araştırmacılar için gerek yazılımlara sahiplik, gerekse eğitimlerin yüksek maliyetli olması bahsedilen gelişimi oldukça sınırlayan bir durumdur. Lisans, yüksek lisans ve doktora programlarının etkin şekilde çoğaltılması, hali hazırda sadece teorik eğitim bulunan bu kurumlara pratik ve saha eğitiminin eklenmesi, bu amaçla laboratuvar kurulumuna finansal destek verilmesi bu alanın nitelikli bir hal almasına sebep olacaktır.

Diğer taraftan, bazı kurumlarca düzenlenen bir veya iki günlük yine sadece teorik bilgiyle sınırlı sertifika programlarının yeterli olmadığı açık olmakla birlikte, bu sertifikaların sınavın ve uygulamanın olmadığı bir eğitim sonunda verilmesi de büyük bir eksikliktir. Birçok ülkede, teorik ve pratiğin harmanlandığı bir eğitim uygulaması sonucunda yapılan birkaç eğitimde başarı sağlayan adaylara sertifika verildiği ve birkaç yılda bir yine eğitim ve sınavlar sonucunda bu sertifikaların yenilendiği görülmektedir. Bilginin güncel ve taze tutulması, yenilikler ve ihtiyaçlar doğrultusunda yetişmiş elemanların ve uzmanların sahada olması artık bir seçenek değil zorunluluk halini almaktadır.

Elbette konunun sadece teknik hususları bilen uzmanlardan ibaret olmadığı, analizlerin sonucunun raporlaştırılarak delil mahiyetinde yasal organlara sunumuyla ispatlanmaktadır. Bu sebeple araştırmaların, teknik ve hukuki alanda yetişmiş, gerekli eğitimleri alarak aranan becerileri kazanmış uzmanlarca yürütülmesi, gerekli hallerde de, araştırmalar sırasında, adli bilişim, bilişim hukuku ve kişisel veri alanlarına hakim hukuk uzmanlarına danışılması, hem delillerin kabul edilebilirliğini güvence altına almakta, hem de işlemi gerçekleştiren personelin veya uzmanın zan altında kalmasını engellemektedir.

Ülkelerin standartlaşmayla birlikte gelişen kanunlaşma ihtiyacı, uluslararası nitelikli kanunları ve sözleşmeleri beraberinde getirmiştir. Ülkelerin yaptıkları kanuni düzenlemeler arasında benzer metinlerin kabul edildiği görülebiliyorken, uygulamaya koyma noktasında kurallara ne derece uyulduğu noktası ise tartışmaya

açıktır. Bilişim suçlarının sınır üstü özellikleri dikkate alındığında, metinlerin benzer olması doğal bir durumdur hatta tercih edilen bir yöntem olmalıdır çünkü eylem, yer, zaman ve zarar faktörleri göz önüne alındığında birkaç ülkeyi de içine alan bir araştırma ve yargılama zinciri oluşmaktadır.

Yukarıda bahsi geçen tüm bu sebepler dahilinde, adli bilişimin tarihçesiyle ve özellikleriyle başlayan bu tez çalışması, temeli oluşturan modellerin teknolojik gelişmelere ve uzmanların bakış açısına göre şekillenişini özetlemekte, bu modellerde yer alan her bir aşamanın doğurduğu en iyi uygulama rehberleri ve standartlara işaret etmektedir. Standartlar, akreditasyon formuna bürünerek, dijital delillerin incelenip analiz edildiği laboratuvarlara ve delilleri toplayan, inceleyen, analiz eden ve raporlaştırarak mahkemeye sunan uzman ve personellerin eğitim ve yetkinlik sertifikalarına etki etmiştir. Bu sebeplerle bu tez çalışmasında, bilişim suçlarının ilk ortaya çıktığı, geliştiği ve adli bilişime yön verdiği en önemli ve etkili iki ülke olan Amerika Birleşik Devletleri ile Birleşik Krallık'ta en yaygın kullanılan en iyi uygulamalar, standartlar, akreditasyonlar, sertifikasyonlar ve eğitimler anlatılmış, her iki ülkedeki ve Türkiye'deki hukuki düzenlemeler örnek olaylarla somutlaştırılarak tez sonuçlandırılmıştır.

Adli bilişimin başlangıcından günümüze kadar süren, araştırmacılar ve uzmanlar tarafından geliştirilen modeller üzerinde yapılan araştırmada, her bir modelde faydalı işlev gören aşamalar bulunmakla birlikte, bu aşamaların hepsinin bir arada bulunduğu bir model tespit edilememiştir. Bu sebeple, bahsi geçen modellerle sınırlı tutulan bir "Öneri Model" sunulmuş ve bu modelin araştırılacak bilişim sistemleri ile dijital cihazların özelliklerine uyum sağlaması açısından geniş ve detaylı şekilde oluşturulması hedeflenmiştir. Ayrıca, açıklanan en iyi uygulamalar ile standartların hangilerinin, öneri modelin basamaklarına uyarlanabileceği konusunda değerlendirmelerde bulunulmuştur. Modelin aşamaları belirlenirken hem mevcut bilişim sistemleri nezdinde en iyi verimin alınabileceği bir kapsam belirlenmeye çalışılmış, hem de gelecekte daha da yaygınlaşacağı şimdiden belli olan yeni teknolojilere, uzak sunuculara ve otonom sistemlere uyum sağlayabilecek nitelikte esnek ve uyum sağlama potansiyeli güçlü basamaklar hazırlanması amaçlanmıştır.

Modellerin uygulanabilirliği ve tercih edilebilirliği, gelecekte hazırlanacak yeni rehberler ve standartlar kadar, belirlenecek prosedürler ve hukuki düzenlemeler açısından da yol gösterici olacaktır. Hukuka uygun, şeffaf ve adil yargılanma kurallarına uygun yargılamaların temelini oluşturan adli bilişim araştırmaları için bu sınırların belirlenmesi hem bir zorunluluk, hem de uygulayıcılar için kolaylık sağlayacaktır.

ÖZET

Adli Bilişimde Standardizasyon, Sertifikasyon, Akreditasyon ve En İyi Uygulamalar

Elektronik cihazlar ile internetin suç faaliyetlerinde kullanımının yaygınlaşması neticesinde bilişim sistemlerinin suçun hedefi olduğu kadar aracı konumunda olmasının çocuk pornografisinden kişisel verilerin çalınmasına, fikri mülkiyetin tahrip edilmesinden dolandırıcılık ve hırsızlık gibi daha pek çok suçun işlenmesinde kullanılmasına sebep olmaktadır. Bu suçlar ceza hukukunun klasik suçlarından farklı olarak mekandan bağımsız ve soruşturulması ile kovuşturulması noktasında da çok sayıda tutarsızlık ve belirsizlik içermektedir.

Uluslararası nitelik kazanan adli olaylarda, ülkeler arasında düzenlenmiş adli bilişim süreçleri, metotları ve yasal mevzuatları arasındaki farklılığın yaratacağı olumsuz sonuçları ortadan kaldırmak için, adına "best practices" denilen en iyi uygulama rehberleri hazırlanarak, standardizasyon, akreditasyon ve sertifikasyonlar düzenlenmiş, hukuki zemini sağlamlaştırmak için de uluslararası nitelikli kanunlar ve sözleşmeler kabul edilmiştir.

Son yıllarda yapay zeka sistemlerinin gelişmesi, bulut bilişim ve nesnelerin interneti teknolojilerinin oluşumu, adli bilişimin yerleşik depolama cihazlarından daha farklı özellikli sistemlerin incelenmesini zorunlu kılmaya başladı. Henüz uluslararası platformda klasik adli bilişimin en iyi versiyonuna ulaşılamamışken, daha belirsiz bir alan olan bulut ve IoT için daha çok çalışmak gerektiği ortadadır.

Çalışmanın oluşturulma amacı da geçmişteki ve günümüzdeki yöntemlerden yola çıkarak, gelecek teknolojilere uyumlu bir model ve modele uygun yeni teknik ve hukuki kurallar ihtiyacıdır. Bu çalışma, bu ihtiyacın çerçevesini çizen bir metodoloji izleyerek yol gösterici bir sistem benimsemiştir. Adli Bilişim aşamalarının geniş ve detaylı şekilde düzenlenerek, bulut bilişim, IoT ve yapay zeka sistemlerine entegre edilebilecek esneklikte bir model oluşturulması, rehberlerin, standartların ve hukuki düzenlemelerin model basamaklarına uygun şekilde güncellenmesi gerekliliğidir.

Anahtar Sözcükler: Adli Bilişim, Akreditasyon, En İyi Uygulama, Sertifikasyon, Standardizasyon.

SUMMARY

Standardization, Certification, Accreditation and Best Practices in Digital Forensics

As a result of the widespread use of electronic devices and the internet in criminal activities, the fact that information systems are in the position of an intermediary as well as the target of the crime causes them to be used in many crimes such as child pornography, theft of personal data, the destruction of intellectual property, fraud and theft. Unlike the classical crimes of the criminal law, these crimes are independent from the place and contain many inconsistencies and uncertainties in terms of investigation and prosecution.

In order to eliminate the negative consequences of the difference between forensic informatics processes, methods and legal regulations regulated between countries in international forensic cases, best practice guides have been prepared, standardizations, accreditations and certifications have been regulated and international laws and conventions have been adopted to strengthen the legal basis.

In recent years, the development of artificial intelligence systems, the appearance of cloud computing and internet of things technologies have made it necessary to examine systems with different features than the built-in storage devices of forensic computing. While the best version of classical forensics has not yet been reached in the international platform, it is clear that more work is needed for the cloud and IoT, which is a more uncertain area.

The purpose of the thesis study is the need for new technical and legal rules that are suitable for a model and model compatible with future technologies, based on the methods of the past and present. This study adopts a guiding system by following a methodology that outlines this need. It is the necessity of arranging the stages of Digital Forensics in a wide and detailed way, creating a flexible model that can be integrated into cloud computing, IoT and artificial intelligence systems, and updating the guidelines, standards and legal regulations in accordance with the model steps.

Keywords: Digital Forensics, Accreditation, Best Practices, Certification, Standardization.

KAYNAKLAR

AB Avrupa Birliği Temel Haklar Bildirgesi. (2007). Erişim Adresi: [https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708] Erişim Tarihi: 01.05.2021

ABLON L, LIBICKI MC, GOLAY AA. (2014). Markets for Cybercrime Tools and Stolen Data. Hackers' Bazaar. *Rand Corporation National Security Research Division*.

ACPO The Association of Chief Police Officers. (2008). Managers Guide Good Practice and Advice Guide for Managers of e-Crime Investigation. *By Janet William. Metropolitan Police Service.* **Version V0.1.4**. Erişim Adresi: [https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf] Erişim Tarihi: 30.04.2021

ACPO The Association of Chief Police Officers. (2012). Good Practice Guide for Digital Evidence. *By Janet William. Metropolitan Police Service*. **Version 5**. Erişim Adresi: [https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf] Erişim Tarihi: 30.04.2021

AGARWAL A, GUPTA M, GUPTA S, GUPTA SC. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS),* **Volume (5)** : Issue (1). Erişim Adresi: [https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume5/Issue1/IJCSS-438.pdf] Erişim Tarihi: 01.05.2021

AIAC Accreditation International Association for Certifying Bodies (1998). Guidance on the Application of ISO/IEC 17020. Erişim Adresi: [http://www.aiacacc.org/downloads/IBCB-04%20Guidelines.pdf] Erişim Tarihi: 01.05.2021

AKYÜREK G. (2012). Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu. *Türkiye Barolar Birliği Dergisi*, Sayı: 101. ss.:61-82.

ANAB ANSI National Accreditation Board. Erişim Adresi: [https://anab.ansi.org/en/forensic-accreditation/iso-iec-17020-forensic-accreditation-process] Erişim Tarihi: 13.04.2021

APAC Asia Pacific Accreditation Cooperation. Erişim Adresi: [https://www.apac-accreditation.org/] Erişim tarihi: 17.04.2021

APAC NAC. (2019). Asia Pacific Accreditation Cooperation, National Accreditation Center. Erişim Adresi: [http://nationalaccreditationcenter.org/wp-content/uploads/2019/10/ingilizce.jpg] Erişim Tarihi: 30.04.2021

AQUILINA JM, CASEY E, MALIN C. (2008). Malware Forensics: Investigating and Analyzing Malicious Code. Syngress; 1st edition. p:592.

ASCLD American Society Of Crime Laboratory Directors. Erişim Adresi: [https://www.ascld.org/our-history/] Erişim Tarihi: 25.04.2021

ASTM Internatıonal. Erişim Adresi: [https://www.eifl.net/publisher/astm-international] Erişim Tarihi:13.04.2021

ASTM E2678-09. (2009). Standard Guide For Education and Training in Computer Forensics. *ASTM International*. Erişim Adresi: [http://www.astm.org/Standards/E2678.htm] Erişim Tarihi: 01.05.2021

ASTM E2763 - 10 Standard Practice for Computer Forensics. Erişim Adresi: [https://www.astm.org/Standards/E2763.htm] Erişim Tarihi: 01.05.2021

ASTM E2825 – 19 Standard Guide for Forensic Digital Image Processing. Erişim Adresi: [https://www.astm.org/Standards/E2825.htm] Erişim Tarihi: 01.05.2021.

ATAMANIUK M. (2020). A Brief History of Computer Viruses. Erişim Adresi: [https://clario.co/blog/history-of-computer-viruses/] Erişim Tarihi: 25.04.2021

BARBARA JJ. (2006). A Standard Level of Acceptability for Computer Forensics. *ASTM International Standards Worldwide*. Erişim Adresi: [https://www.astm.org/SNEWS/FEBRUARY_2006/barbara_feb06.html] Erişim Tarihi: 01.05.2021

BARYAMUREEBA V, TUSHABE F. (2004). The Enhanced Digital Investigation Process Model. *The Digital Forensic Research Conference.* DFRWS. Erişim Adresi: [https://dfrws.org/wp-content/uploads/2019/06/2004_USA_paper-the_enhanced_digital_investigation_process_model.pdf] Erişim Tarihi: 01.05.2021.

BBC News. (2017). Norwich Airport and Hospital Cyber-hacker 'His Royal Gingerness' Jailed. Erişim Adresi: [https://www.bbc.com/news/uk-england-norfolk-40307003] Erişim Tarihi: 01.05.2021

BELCİC I. (2020). What is a Sniffer and How Can I Protect Against Sniffing? *Avast Academy*. Erişim Adresi: [https://www.avast.com/c-sniffer] Erişim Tarihi: 29.04.2020

BEVERLY R, GARFINKEL SL, CARDWELL G. (2011). Forensic Carving of Network Packets and Associated Data Structures. *Digital Investigation* **Volume 8,** Supplement, pp:78–89 DOI:10.1016/j.diin.2011.05.010

BSI BIP 0008. (1996). British Code for Legal Admissibility and Record Retention. Erişim Adresi: [https://www.efilecabinet.com/bip-0008-british-code-legal-admissibility-record-retention/] Erişim Tarihi: 01.05.2021.

BSI BS 10008. (2008). *The British Standard Institute*. *BCS The Chartered Institute for IT*. Erişim Adresi: [https://www.bcs.org/content-hub/bs-10008-a-new-standard-for-legally-admissible-electronic-information/] Erişim Tarihi: 01.05.2021

BSI BS 10008 (2020). Evidential Weight and Legal Admissibility of Electronic Information. *BSI The British Standard Institute.* Erişim Adresi: [https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/] Erişim Tarihi: 01.05.2021

CAMINER BF. (1985). Credit Card Fraud: The Neglected Crime. *The Journal of Crimınal Law & Criminology* **Volume. 76**, No. 3. Northwestern University, School of Law Printed. pp:746-763

CARRIER B, SPAFFORD EH. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence.* Fall. **Volume 2**, Issue 2.

CASEY E. (2004). Investigative Process. *Digital Evidence and Computer Crime*. 2nd Ed. Academic Press, p:688

CCI Certified Cyber Investigator. Digital Forensics Specialist. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cci-network-forensic-investigation] Erişim Tarihi: 02.05.2021

CDaCT Certified Data Collection Technician. Digital Forensics. Fundamentals. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cdact-certified-data-collection-technician] Erişim Tarihi: 02.05.2021

CFIP Certified Forensic Investigation Practitioner. Digital Forensics. Core. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cfip-forensic-investigation] Erişim Tarihi: 02.05.2021

CFIS Certified Forensic Investigation Specialist. Digital Forensics Specialist. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cfis-advanced-forensic-investigation] Erişim Tarihi: 02.05.2021

CLFP Certified Linux Forensic Practitioner. Digital Forensics Specialist. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/clfp-linux-forensic-investigation] Erişim Tarihi: 02.05.2021

CMFS Certified Mac Forensics Specialist. Digital Forensics. Specialist. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cmfs-apple-mac-forensics] Erişim Tarihi: 02.05.2021

CMI Certified Malware Investigator. Digital Forensics. Core. 7safe. Erişim Adresi: [https://www.7safe.com/our-courses/certified-digital-forensics-courses/details/cmi-malware-investigation-training] Erişim Tarihi: 02.05.2021

CENTEL N, ZAFER H. (2015). Ceza Muhakemesi Hukuku, 12. Baskı, Beta Yayınevi.

CHOO KKR, QUICK D. (2014). Impacts of İncreasing Volume of Digital Forensic Data: A Survey and Future Research Challenges. *Digital Investigation.* **Volume 11**, Issue 4, pp:273-294. DOI: 10.1016/j.diin.2014.09.002

CIARDHUÁIN SÓ. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence.* Summer, **Volume 3**, Issue 1. p:22. Erişim Adresi: [https://www.researchgate.net/publication/220542517_An_Extended_Model_of_Cybercrime_Investigations] Erişim Tarihi: 02.05.2021

CLOUGH J. (2015). Principles of Cybercrime. *Cambridge University Press*, Second Edition. Erişim Adresi: [https://doi.org/10.1017/CBO9781139540803] Erişim Tarihi: 02.05.2021

CMA Computer Misuse Act (1990). *UK Legislaton.* Erişim Adresi: [https://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences] Erişim Tarihi: 01.05.2021.

CoE Council of Europe. (2001). Convention on Cybercrime Budapest, Erişim Adresi: [https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561] Erişim Tarihi: 01.05.2021

CoE Council of Europe. (2014). Electronic Evidence Guide A Basic Guide For Police Officers, Prosecutors and Judges. **Version 2.0.** Erişim Adresi: [https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf] Erişim Tarihi: 13.04.2021

CoE Council of Europe. (2017). Digital Forensics A Basic Guide For The Management and Procedures of A Digital Forensics Laboratory. **Version 1.1.** Erişim Adresi: [https://www.coe.int/documents/9252320/19022082/GLACY+DFL+Guide+version+June+2017+v6.pdf/d10b6d08-2baf-0f43-0ac5-23309ec58f2e] Erişim Tarihi: 25.04.2021

COHEN F. (2010). Toward a Science of Digital Forensic Evidence Examination. *IFIP International Conference on Digital Forensics. Information and Communication Technology*. *Conference: Advances in Digital Forensics* VI - Sixth IFIP WG 11.9. pp:17-35. DOI:10.1007/978-3-642-15506-2_2

College of Policing. (2021). Core Skills in Data Recovery and Analysis. Erişim Adresi: [https://www.college.police.uk/career-learning/learning/courses/core-skills-data-recovery-and-analysis] Erişim Tarihi: 01.05.2021

College of Policing. (2021). Core Skills in Mobile Phone Forensics. Erişim Adresi: [https://www.college.police.uk/career-learning/learning/courses/core-skills-mobile-phone-forensics] Erişim Tarihi: 14.04.2021

CONNOLLY K. (2020). Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel. Erişim Adresi: [https://www.theguardian.com/world/2020/may/13/russian-hacking-attack-on-bundestag-damaged-trust-says-merkel] Erişim Tarihi: 25.04.2021

CPIA Criminal Procedure and Investigations Act (1996). *UK Legislaton.* Erişim Adresi: [https://www.legislation.gov.uk/ukpga/1996/25/contents] Erişim Tarihi: 01.05.2021.

CPS CMA Computer Misuse Act (1990). *The Crown Prosecution Service.* Erişim Adresi: [https://www.cps.gov.uk/legal-guidance/computer-misuse-act] Erişim Tarihi: 01.05.2021.

CRANFIELD UNIVERSITY. (2021). Centre for Electronic Warfare Information and Cyber. *Digital Investigation Unit.* Erişim Adresi: [https://www.cranfield.ac.uk/centres/centre-for-electronic-warfare-information-and-cyber/digital-investigation-unit] Erişim Tarihi: 14.04.2021

DFRWS. (2001). A Road Map For Digital Forensic Research. Technıcal Report. DTR - T001-01. Erişim Adresi: [https://www.scribd.com/document/439280751/A-Road-Map-for-Digital-Forensic-Research] Erişim Tarihi: 25.04.2021

DoD Department of Defense, Cyber Crime Center (DC3). (2019). History of DC3 Chronological History Last. Erişim Adresi:

[https://www.dc3.mil/Portals/100/Documents/DC3/DC3_Home/About_History/History%20of%20DC3.pdf?ver=2020-02-19-114119-117] Erişim Tarihi: 25.04.2021

DoJ Department of Justice. (2015). Prosecuting Computer Crimes. *Computer Crime and Intellectual Property Section Criminal Division. Office of Legal Education Executive Office for United States Attorneys*. p:207. Erişim Adresi: [https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf] Erişim Tarihi: 03.05.2021.

DoJ 18 U.S.C. § 2701. Unlawful Access To Stored Communıcatıons. *U.S. Department of Justice.* Erişim Adresi:[https://www.justice.gov/archives/jm/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701] Erişim Tarihi: 14.04.2021

DU X, LE-KHAC NA, SCANLON M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *Computer Science and Network Security*, **9**,. Conference: 16th European Conference on Cyber Warfare and Security (ECCWS) Erişim Adresi: [https://www.markscanlon.co/papers/ProcessModelsDFaaS.pdf] Erişim Tarihi: 03.05.2021

DUCKLIN P. (2018). Forget VPNfilter – Here's Backlash, a Networking Hack From Way, Way Back. Erişim Adresi: [https://nakedsecurity.sophos.com/2018/05/31/forget-vpnfilter-heres-backlash-a-networking-hack-from-way-way-back/] Erişim Tarihi: 25.04.2021

ECTEG Course Packages. *European Cybercrime Training and Education Group Centre*. CEPOL EUROPOL EC3 Erişim Adresi: [https://www.ecteg.eu/course-packages/] Erişim tarihi: 14.04.2021

ECTEG E-First: First Responders E-Learning Package. *European Cybercrime Training and Education Group Centre*. CEPOL EUROPOL EC3. Erişim Adresi: [https://www.ecteg.eu/running/first-responders/] Erişim Tarihi: 14.04.2021

ECTEG Scenario Project. *European Cybercrime Training and Education Group Centre*. CEPOL EUROPOL EC3. Erişim Adresi: [https://www.ecteg.eu/running/project-scenario/] Erişim Tarihi: 14.04.2021

ECTEG Global Cybercrime Certification Project. *European Cybercrime Training and Education Group Centre*. CEPOL EUROPOL EC3. Erişim Adresi: [https://www.ecteg.eu/running/gcc/] Erişim Tarihi: 14.04.2021

ECTEG Basic Networks Forensics. *European Cybercrime Training and Education Group Centre*. CEPOL EUROPOL EC3. Erişim Adresi: [https://www.ecteg.eu/running/ecteg-basic-networks-forensics/] Erişim Tarihi: 14.04.2021

EHLİZ H. (2019). Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi. *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı Yüksek Lisans Tez*i. İstanbul

EMEKCİ A, KUĞU E, TEMİZTÜRK M. (2016). Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* **Cilt:2,** No:1, **ss:** 8-14.

ETAHER N, WEIR GRS, ALAZAB M. (2015). From ZeuS to Zitmo: Trends in Banking Malware. *TrustCom. The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp: 1386-1391.

FARNAN JE. (2003). Testimony. The FBI Cyber Division. Erişim Adresi: [https://archives.fbi.gov/archives/news/testimony/the-fbi-cyber-division] Erişim Tarihi: 29.04.2021.

FARWELL JP, ROHOZINSKI R. (2011). Stuxnet and The Future of Cyber War. *Survival* **Volume 53,** No.1, pp:23-40 Erişim Adresi: [https://doi.org/10.1080/00396338.2011.555586] Erişim Tarihi: 03.05.2021.

FBI Federal Bureau of Investigation. (2016). Ten Years After: The FBI Since 9/11-Cyber. Erişim Adresi: [https://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber] Erişim Tarihi: 29.04.2021.

Flashback Data. (2013). Erişim Adresi: [https://www.flashbackdata.com/news-press-releases/pr-ascld-accreditation/] Erişim Tarihi: 01.05.2021

FREILING FC, SCHWITTAY B. (2007). A Common Process Model for Incident Response and Computer Forensics. *Conference: IT-Incidents Management & IT-Forensics - IMF 2007, Conference Proceedings*.

GINGERICH D. (2017) The First Hack. Erişim Adresi: [https://sciencenonfiction.org/2017/04/06/the-first-hack/] Erişim Tarihi: 29.04.2021

GROBLER M. (2010). Digital Forensic Standards: International Progress. *Proceedings of the South African Information Security Multi-Conference*. SAISMC. pp:261-271.

GROBLER M. (2012). The Need for Digital Evidence Standardisation. *International Journal of Digital Crime and Forensics,* 4(2), 1-12.

HARÁN JM. (2018). Malware of The 90s: Remembering The Michelangelo and Melissa Viruses. Erişim Adresi: [https://www.welivesecurity.com/2018/11/12/malware-90s-michelangelo-melissa-viruses/] Erişim Tarihi: 30.04.2021

HARDING L. (2016). Top Democrat's Emails Hacked By Russia After Aide Made Typo, Investigation Finds. Erişim Adresi: [https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds] Erişim Tarihi: 30.04.2021

HAYES DR. (2014). A Practical Guide to Computer Forensics Investigations. *Pearson IT Certification*. 1st edition

HEGARTY RC, LAMB DJ, ATTWOOD A. (2014). Digital Evidence Challenges in the Internet of Things. *Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis*. Chapter 2 – WDFIA. pp:163-172.

HENKOĞLU T. (2014). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi. *Pusula Yayıncılık.* 2. Baskı. **s.:**290.

HOSMER C. (2002). Proving the Integrity of Digital Evidence with Time. *International Journal of Digital Evidence,* Spring. **Volume 1**, Issue 1.

IASIELLO E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. 5th International Conference on Cyber Conflict. *NATO CCD COE Publications.*

ILAC (2002). ILAC-G19:2002 The International Laboratory Accreditation Cooperation. Guidelines for Forensic Science Laboratories. Erişim Adresi: [http://www.sadcmet.org/SADCWaterLab/Archived_Reports/2006%20Reports%20and%20Docs/Ilac-g19.pdf] Erişim Tarihi: 02.05.2021

ILAC (2014). ILAC-G19:08/2014. Modules in a Forensic Science Process. *International Laboratory Accreditation Cooperation.* Erişim Adresi: [https://ilac.org/?ddownload=805] Erişim Tarihi: 02.05.2021.

IMTIAZ F. (2006). Enterprise Computer Forensics: A Defensive and Offensive Strategy to Fight Computer Crime. *4th Australian Digital Forensics Conference. School of Computer and Information Science, Edith Cowan University,*

IOCE (2000). G8 Proposed Principles for the Procedures Relating to Digital Evidence. *International Organization on Computer Evidence.*

IOCE 2002b Training Standards and Knowledge Skills and Abilities, *International Organization on Computer Evidence.* Draft **V1.0.**

IORLIAM A. (2018). History of Forensic Science. *Fundamental Computing Forensics for Africa* pp:3-16.

IPAC (2019). Guıde For ISO/IEC 17020 Application OGC006. *Instituto Português De Acreditação Portuguese Accreditation Institute.* Erişim Adresi: [http://www.ipac.pt/docs/publicdocs/requisitos/OGC006_GuiaAplicacao17020_v20160113_En_20190906.pdf] Erişim Tarihi: 02.05.2021

ISO International Organization for Standardization. Erişim Adresi: [www.iso.org] Erişim Tarihi:13.04.2021

ISO 17025 Nedir? Erişim Adresi: [http://iso17025.gen.tr/iso-17025-nedir] Erişim Tarihi:13.04.2021

ISO 9001:2015. How To Use It. *International Organization for Standardization.* Erişim Adresi: [https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100373.pdf] Erişim Tarihi: 02.05.2021.

ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of Practice For Information Security Controls. Erişim Adresi: [https://www.iso.org/standard/54533.html] Erişim Tarihi: 14.04.2021

ISO/IEC 27035-1:2016 Information Technology - Security Techniques - Information Security Incident Management - Part 1: Principles of Incident Management. Erişim Adresi: [https://www.iso.org/standard/60803.html] Erişim Tarihi:13.04.2021

ISO/IEC 27035-2:2016 Information Technology - Security Techniques - Information Security Incident Management - Part 2: Guidelines to Plan and Prepare for Incident Response. Erişim Adresi: [https://www.iso.org/standard/62071.html] Erişim Tarihi:13.04.2021

ISO/IEC 27035-3:2020 Information Technology - Information Security Incident Management - Part 3: Guidelines for ICT Incident Response Operations. Erişim Adresi: [https://www.iso.org/standard/74033.html] Erişim Tarihi:13.04.2021

ISO/IEC 27041:2015 Information Technology - Security Techniques - Guidance on Assuring Suitability and Adequacy of Incident Investigative Method. Erişim Adresi: [https://www.iso.org/standard/44405.html] Erişim Tarihi:13.04.2021

ISO/IEC 27042:2015 Information Technology - Security Techniques - Guidelines For The Analysis and Interpretation of Digital Evidence. Erişim Adresi: [https://www.iso.org/standard/44406.html] Erişim Tarihi:13.04.2021

ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes. Erişim Adresi: [https://www.iso.org/standard/44407.html] Erişim Tarihi:13.04.2021

ISO/IEC 30121:2015 Information Technology - Governance of Digital Forensic Risk Framework. Erişim Adresi: [https://www.iso.org/standard/53241.html] Erişim Tarihi:13.04.2021

JESTEADT AR, SUTTON SK. (2020). U.S. Supreme Court to Weigh in on Computer Fraud and Abuse Act (CFAA) for the First Time. *Carlton Fields.* Erişim Adresi: [https://www.carltonfields.com/insights/publications/2020/us-supreme-court-computer-fraud-abuse-act#:~:text=The%20CFAA%2C%20enacted%20in%201986,financial%20institutions%20and%20the%20U.S.] Erişim Tarihi: 02.05.2021.

KEENEY JC. (1969). Recent Amendments to the Federal Child Pornography and Abuse Statutes, 18 U.S.C. 2252. Criminal Resource Manual 1969; JM 9-75.001. *U.S. Department of Justice.* updated 1998. Erişim Adresi: [https://www.justice.gov/archives/jm/criminal-resource-manual-2467-keeney-memorandum-recent-amendments-federal-child-pornography-and] Erişim Tarihi: 02.05.2021.

KEHOE BP. (1992). Chapter 8: Things You'll Hear About. Zen and the Art of the Internet. A Beginner's Guide to the Internet. *PTR Prentice Hall, INc.* First Edition. p.:98. Erişim Adresi: [http://www.tugurium.com/docs/ZenAndTheArtOfTheInternet.pdf] Erişim Tarihi: 29.04.2021

KELTY C. (2011). The Morris Worm. *eScholarship, Open Access Publications from the University of California. Limn UCLA.* Erişim Adresi: [https://escholarship.org/uc/item/8t12q5bj] Erişim Tarihi: 30.04.2021

KENT K, CHEVALIER S, GRANCE T, DANG H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory*. Special Publication 800-86 p.:121.

KESSLER GC, HOSMER C. (2011).. Chapter 2 - An Overview of Steganography. *Advances in Computers.* **Volume 83**, pp: 51-107. Erişim Adresi: [https://doi.org/10.1016/B978-0-12-385510-7.00002-3] Erişim Tarihi: 03.05.2021

KIZZA JM. (2007). Ethical and Social Issues in the Information Age. Editors David Gries Fred B. Schneider. 3rd Ed, *Springer.*

KOHN MD, ELOFF MM, ELOFF KHP. (2013). Integrated Digital Forensic Process Model. *Computers & Security*. pp:103-115 DOI:10.1016/j.cose.2013.05.001

KOLTUKSUZ A. (2007). Adli Bilişime Giriş. *Adli Bilişim Kursu, İzmir İleri teknoloji Enstitüsü*.

KRAKOFF S. (2021). What's the Difference Between Cybersecurity and Computer Forensics? Erişim Adresi: [https://online.champlain.edu/blog/difference-between-cybersecurity-and-computer-forensics] Erişim Tarihi: 30.04.2021

KVK Kurulu 2019/141. Kişisel Verileri Koruma Kurulu. Karar Tarihi: 16.05.2019.

KVK Kurulu 2020/286. Kişisel Verileri Koruma Kurulu. Karar Tarihi: 16.04.2020.

LEE, HC, PALMBACH, T, MİLLER, MT. (2001). Henry Lee's Crime Scene Handbook, *Academic Press.* 1st ed.

LEVA (2021). Law Enforcement & Emergency Services Video Association International. *LEVA Certification Program*. Erişim Adresi: [https://www.leva.org/certification/] Erişim Tarihi 14.04.2021.

LII 18 U.S.C. § 2701. *Legal Information Institute.* Erişim Adresi: [https://www.law.cornell.edu/uscode/text/18/2701] Erişim tarihi 14.04.2021

LII 42 U.S. Code § 2000aa–7. *Legal Information Institute. Cornell Law School – Definitions.* Erişim Adresi: [https://www.law.cornell.edu/uscode/text/42/2000aa-7] Erişim Tarihi: 14.04.2021

LI S, DHAMI MK, HO ATS. (2015). Standards and Best Practices in Digital and Multimedia Forensics. Handbook of Digital Forensics of Multimedia Data and Devices, Surrey Centre for Cyber Security (SCCS), University of Surrey, First Edition. UK. pp:38-93

LIN H. (2012). Cyber Conflict and İnternational Humanitarian Law. *International Review of the Red Cross*, **Volume.94,** No.886, pp:515-531.

LOEBENBERGER D, WIELPUTZ R. (2007). Evolution! From Creeper to Storm. Presentation for the Seminar on "Malware". Bonn-Aachen International Center for Information Technology.

LYLE JR, WHITE DR, AYERS RP. (2008). Software Diagnostics and Conformance Testing. *Digital Forensics at the National Institute of Standards and Technology.* NISTIR 7490.

MANDIA K, PROSISE C, PEPE M. (2003). Incident Response&Computer Forensics. *McGrawHill Osborne Media.* 2nd Ed. p.:507.

MARTINI B, CHOO KKR. (2012). An Integrated Conceptual Digital Forensic Framework For Cloud Computing. *Digital Investigation* **Volume 9,** Issue 2, pp:71-80.

MILLER MT. (2009). Crime Scene Investigation. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. Editors James S, Nordby J. Editors. CRC Press. 3rd Edition. pp:167-192.

MRDOVİC S. (2021). IoT Forensics. Security of Ubiquitous Computing Systems. *Springer*. pp:215-229.

Dollar D. (2004). Controlling the Assault of Non-Solicited Pornography and Marketing Act. *National Credit Union Administration. 04-RA-07.* Erişim Adresi: [https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/controlling-assault-non-solicited-pornography-and-marketing-act] Erişim Tarihi: 02.05.2021.

NCA National Crime Agency. Hacker From Russian Crime Group Jailed For Multi-Million Pound Global Blackmail Conspiracy. Erişim Adresi: [https://www.nationalcrimeagency.gov.uk/news/hacker-from-russian-crime-group-jailed-for-multi-million-pound-global-blackmail-conspiracy] Erişim Tarihi: 14.04.2021

NIJ National Institute of Justice. Erişim Adresi: [https://nij.ojp.gov/about-nij] Erişim Tarihi: 30.04.2021

NIJ National Institute Of Justice. (1999). Forensic Examination Of Digital Evidence: A Guide For Law Enforcement. *U.S. Department Of Justice Office Of Justice Programs*. **Apr. 04.**

NIJ National Institute Of Justice. (2001). Electronic Crime Scene Investigation: A Guide For First Responders. *U.S. Department Of Justice Office Of Justice Programs*. Second Edition **APR. 08.**

NIJ National Institute of Justice. (2002). Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ.

NIJ National Institute of Justice. (2003). Investigative Uses of Technology: Devices,Tools, and Techniques. *U.S. Department of Justice Office of Justice Programs.* **OCT. 07**

NIST National Institute of Standards and Technology (1901). Timeline, Erişim Adresi: [https://www.nist.gov/timeline#event-774226] Erişim Tarihi: 02.05.2021.

NIST National Institute of Standards and Technology (2018). Digital Forensics Programs. Erişim Adresi: [https://www.nist.gov/programs-projects/digital-forensics] Erişim Tarihi: 02.05.2021.

NIST National Institute of Standards and Technology (2019). The CFReDS Project. Information Technology Laboratory. Erişim Adresi: [https://www.cfreds.nist.gov/] Erişim Tarihi: 02.05.2021

NPCC The National Police Chiefs' Council. History and Background. Erişim Adresi: [https://www.npcc.police.uk/About/History.aspx] Erişim Tarihi:13.04.2021

ORMEROD D, LAIRD K. (2018). Smith, Hogan, & Ormerod's Criminal Law. Oxford. E-book. Fifteenth Edition p.:1216.

ÖĞÜN MN, KAYA A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Security Strategies Journal*, **Cilt 9**, Sayı 18. ss:145-181.

ÖZKAYA P, SAMET R. (2020a). Yazılım Ürünlerinin Telif Hukuku Kapsamında Korunması. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, **c. 6**, sayı. 1. p.17-34

ÖZKAYA P, SAMET R. (2020b). Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik. Siber Güvenlik ve Savunma - Biyometrik ve Kriptografik Uygulamalar. *Nobel Yayıncılık.* 1. Basım. 4.Bölüm ss: 121-180

PACE Police and Criminal Evidence Act 1984. *UK Legislaton.* Erişim Adresi: [https://www.legislation.gov.uk/ukpga/1984/60/contents] Erişim Tarihi: 02.05.2021.

PALMER G. (2001). DFRWS Technical Report: A Road Map for Digital Forensic Research. *Digital Forensic Research Workshop. DFRWS*. p.:42

PALMER D. (2018). Thanatos Ransomware: Free Decryption Tool Released For Destructive File-Locking Malware. Erişim Adresi: [https://www.zdnet.com/article/thanatos-ransomware-free-decryption-tool-released-for-destructive-file-locking-malware/] Erişim Tarihi: 01.05.2021

PARASRAM SWN. (2017). Digital Forensics with Kali Linux. *Publisher: Packt*. p.:334.

PERUMAL S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. *IJCSNS International Journal of Computer Science and Network Security*, **Volume .9** No.8 pp:38-44.

POLLITT M. (2010). A History of Digital Forensics. *IFIP International Conference on Digital Forensics Advances in Digital Forensics* VI. pp:3-15.

PONCIANO E. (2021). Calibration Awareness. Elements in Implementing an Internal Calibration Laboratory. Erişim Adresi: [https://calibrationawareness.com/iso-iec-170252017-requirements-list-of-documents-outline-and-summary] Erişim Tarihi:13.04.2021.

Purdue University Department of Computer Science .2014.Information Security CS 526 Topic 10: Malwares.ErişimAdresi:[https://www.cs.purdue.edu/homes/ninghui/courses/526_Fall14/handouts/14_526_topic10.ppt] Erişim Tarihi: 02.05.2021.

QUİCK D, CHOO KKR. (2014). Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive. *Trends & Issues in Crime and Criminal Justice. Australian Institute of Criminology.* no: 480.

RADER M, RAHMAN S. (2013). Exploring Historical And Emerging Phishing Techniques and Mitigating The Associated Security Risks. *International Journal Of Network Security & Its Applications (IJNSA*), **Volume 5**, No.4. pp.:23-41.

RAHMAN T. (2015). Computer Forensic. Erişim Adresi: [https://www.slideshare.net/invisible381/digial-forensic-52885398] Erişim Tarihi: 02.05.2021.

RCFL National Program Office, Regional Computer Forensics Laboratory, Erişim Adresi: [https://www.rcfl.gov/] Erişim Tarihi: 02.05.2021.

REITH M, CARR C, GUNSCH G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, **Volume 1**, Issue 3. pp.:1-12.

RIPA Regulation of Investigatory Powers Act 2000 *UK Legislaton.* Erişim Adresi: [https://www.legislation.gov.uk/ukpga/2000/23/contents] Erişim Tarihi: 02.05.2021.

ROGERS MK, GOLDMAN J, MISLAN R, WEDGE T, DEBROTA S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law*: **Volume. 1** , Article 2. pp:19-28.

RUDIN N, INMAN K. (2002) Principles and Practice of Forensic Science: The Profession of Forensic Science .Forensic Science Timeline. Erişim Adresi: [http://plaza.ufl.edu/jhefner/forensic_Timeline.pdf] Erişim Tarihi: 02.05.2021.

SAMMONS J. (2012). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. *Syngress*. p:208.

SERBU M. (2016). What is a Trojan Horse? Erişim Adresi: [https://www.centurylinkquote.com/resources/what-is-a-trojan-horse/] Erişim Tarihi: 02.05.2021.

SERVIDA F, CASEY E. (2019). IoT Forensic Challenges And Opportunities For Digital Traces. *Digital Investigation* **Volume 28,** Supplement, **S**22-S29.

SCHWITTAY B. (2006). Towards Automating Analysis in Computer Forensics. *RWTH Aachen University Department of Computer Science Dependable Distributed Systems Group.* Diploma Thesis in Computer Science.

SMITH C. (2014). How I learned to Stop Worrying and Love The Bombe: Machine Research and Development and Bletchley Park. *History of Science*, **Volumel 52,** no. 2, pp. 200-222.

SPECHT J. (2020). The Origins and Evolution of DC3. Official United States Air Force. Erişim Adresi: [https://www.osi.af.mil/News/Features/Display/Article/2088965/the-origins-and-evolution-of-dc3/] Erişim Tarihi: 02.05.2021

STOYANOVA M, NIKOLOUDAKIS Y, PANAGIOTAKIS S, PALLIS E, MARKAKIS EK. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communıcatıons Surveys & Tutorıals*, **Volume. 22**, No.2. pp.:1191 – 1221.

SWGDE (1999). Scientific Working Group on Digital Evidence. International Organization on Digital Evidence (IOCE). Digital Evidence: Standards and Principles. Forensic Science Communications. **Volume 2.** No.2. October.

SWGDE (2011). Scientific Working Group on Digital Evidence. Core Competencies for Forensic Audio. **Version 1.0.**

SWGDE (2013a). Scientific Working Group on Digital Evidence. Best Practices for Mobile Phone Forensics **Version: 2.0**. February.

SWGDE (2013b). Scientific Working Group on Digital Evidence. Core Competencies for Mobile Phone Forensics.**Version 1.0**

SWGDE (2014a). Scientific Working Group on Digital Evidence. Best Practices for Computer Forensics **Version: 3.1.** September.

SWGDE (2014b). Scientific Working Group on Digital Evidence. Capture of Live Systems **Version: 2.0.** September.

SWGDE (2017a). Scientific Working Group on Digital Evidence. Overview of the Accreditation Process for Digital and Multimedia Forensic Labs. **Version: 1.0.** February.

SWGDE (2017b). Scientific Working Group on Digital Evidence. Myths and Facts about Accreditation for Digital and Multimedia Evidence Labs. **Version: 1.0.** February.

SWGDE (2017c). Scientific Working Group on Digital Evidence. Best Practices for Maintaining the Integrity of Imagery. **Version 1.0**. July.

SWGDE (2018a). Scientific Working Group on Digital Evidence. Best Practices for Computer Forensic Acquisitions. **Version: 1.0.** April.

SWGDE (2018b). Scientific Working Group on Digital Evidence. Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage **Version: 1.0.** April.

SWGDE (2020a) Scientific Working Group on Digital Evidence. International Organization on Digital Evidence (IOCE) . Forensic Science Communications. **Volume 2**. No. 2. April.

SWGDE (2020b). Scientific Working Group on Digital Evidence. Best Practices for Mobile Device Forensic Analysis **Version: 1.0.** September.

SWGDE (2020c). Scientific Working Group on Digital Evidence. Best Practices for Digital Evidence Acquisition from Cloud Service Providers **Version: 1.0**. September.

SWGIT (2010c). Scientific Working Group on Imaging Technology. Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice. System. **Version 1.3.** Document Section 6.

SWGDE/SWGIT (2006). Proficiency Test Program Guidelines. **Version 1.1.**

SWGDE/SWGIT (2010). Guidelines & Recommendations for Training in Digital & Multimedia Evidence **Version: 2.0.** January.

The Open University, A Brief History of Digital Forensics. Scotland. Erişim Adresi: [https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2] Erişim Tarihi: 02.05.2021.

TS EN ISO 9001:2015 Kalite Yönetim Sistemi Belgelendirmesi. Türk Standartlar Enstitüsü. Erişim Adresi: [https://www.tse.org.tr/Icerik/DuyuruDetay?DuyuruID=4288] . Erişim Tarihi: 02.05.2021.

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. Türk Standartlar Enstitüsü. Erişim Adresi: [https://www.tse.org.tr/IcerikDetay?ID=2311] Erişim Tarihi: 14.04.2021

TURNER MJL. (1992). Computer Misuse Act 1990 Cases. Erişim Tarihi: 02.05.2021. [https://www.computerevidence.co.uk/Cases/CMA.htm]

U.S. & Aleynikov. (2011). United States District Court, S.D. New York. No. 10 Cr. 96(DLC). 785 F. Supp. 2d 46 (S.D.N.Y. 2011). March 16th, 2011

U.S. & Aleynikov. (2012). United States Court of Appeals, Second Circuit. 676 F.3d 71 (2d Cir. 2012) 102 U.S.P.Q.2d 1458. Apr 11, 2012

U.S. & Collins. (2013). United States District Court Northern District of California San Jose Division. Case No.: 11-CR-00471-DLJ (PSG). N.D. Cal. Mar. 15, 2013.

U.S. & Kilbride. (2007). United States District Court, D. Arizona. Case No: CR 05-870-PHX-DGC (D. Ariz. Jun. 4, 2007).

U.S. &. Kilbride. (2009). United States Court of Appeals, Ninth Circuit. Nos. 07-10528, 07-10534. Decided: October 28, 2009.

U.S. & Van Buren. United States Court of Appeals For The Eleventh Circuit. 940 F.3d 1192 (11th Cir. 2019). Date published: Oct 10, 2019.

Utica College. (2002). Cyber-Forensic Research Experimentation and Test Environment (Create). *Air Force Research Laboratory Information Directorate Rome Research Site*. Final Technical Report. AFRL-IF-RS-TR-2002-269. p.:107

VEBER, J., KLÍMA, T. (2014). Influence of Standards ISO 27000 Family on Digital Evidence Analysis. *22st Interdisciplinary. Information Management Talks (IDIMT)*, PodĢbrady, pp 103-114

VEBER J, SMUTNY Z. (2015). Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic. *Conference: 14th European Conference on Cyber Warfare & Security***.** pp.:294-299

VOLONINO L, ANZALDUA R, GODWIN J. (2006). Computer Forensics: Principles and Practices. *Pearson*. 1st edition

WHITCOMB CM. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence Spring*. **Volume 1**, Issue 1. .

Williams H. (2015). The Hacker Who Inspired Apple: John 'Captain Crunch' Draper. Erişim Adresi: [https://www.lifehacker.com.au/2015/11/the-hacker-who-inspired-apple-john-captain-crunch-draper/] Erişim Tarihi: 02.05.2021

Yargıtay 8. Ceza Dairesi Esas: 2014/19342 Karar: 2015/2322 Tarih: 03.02.2015

YAZICIOĞLU Y. (1997). Bilgisayar Suçlar, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle. *Alfa Yayıncılık.*

ZAWOAD S, HASAN R. (2015). FAIoT: Towards building a forensics aware eco system for the internet of things. *IEEE International Conference on Services Computing,*

ZULKIPLI NHN, ALENEZI A, WILLS GB. (2017). IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. *Conference: 2nd International Conference on Internet of Things, Big Data and Security.* pp:315-324

18 U.S.C. §2705 (b) 4) 18 U.S. Code § 2705(b) – Preclusion of Notice to Subject of Governmental Access. Erişim Adresi: [https://www.law.cornell.edu/uscode/text/18/2705] Erişim Tarihi:13.04.2021

ÖZGEÇMİŞ

I. Bireysel Bilgileri

Adı : Pelin

Soyadı : ÖZKAYA

II- Eğitimi

2011 – 2015 Kırıkkale Üniversitesi Hukuk Fakültesi

2018 – 2021 Ankara Üniversitesi Adli Bilişim Yüksek Lisans

III- Ünvanları ve Mesleki Deneyimi:

2016 Avukat - Ankara Barosu

IV – Bilimsel İlgi Alanları:

Adli Bilişim, Bilişim Suçları, Kişisel Veri, Yapay Zeka, Nesnelerin İnterneti, Siber Güvenlik, Fikri Mülkiyet Hukuku

V- Bilimsel Yayınları:

Haziran 2020 - Yazılım Ürünlerinin Telif Hukuku Kapsamında Korunması. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi.

Aralık 2020 - Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik. Siber Güvenlik ve Savunma - Biyometrik ve Kriptografik Uygulamalar Kitabı

VI- Alanla İlgili Kurslar:

2020 Autopsy Basic – Basis Technology

2021 Intro to Cybersecurity – Cisco Networking Academy

2021 Cybersecurity Essentials - Cisco Networking Academy

2021 Data Protection and Privacy Rights – Council of Europe