

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



**ULUSLARARASI HUKUK VE TEKNİK STANDARTLARINA
UYUMLU ADLİ BİLİŞİM SÜREÇLERİNİN GELİŞTİRİLMESİ**

Mustafa PEKDEMİR

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

OCAK 2025

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

ULUSLARARASI HUKUK VE TEKNİK STANDARTLARINA UYUMLU
ADLI BİLİŞİM SÜREÇLERİNİN GELİŞTİRİLMESİ

Tez Yazarı
Mustafa PEKDEMİR

Danışman
Doç. Dr. Fatih ERTAM

OCAK 2025
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Uluslararası Hukuk Ve Teknik Standartlarına Uyumlu Adli Bilişim Süreçlerinin Geliştirilmesi
Yazarı:	Mustafa PEKDEMİR
İlk Teslim Tarihi:	23.12.2024
Savunma Tarihi:	24.01.2025

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

İmza

Danışman: Doç. Dr. Fatih ERTAM

Fırat Üniversitesi, Teknoloji Fakültesi

Onayladım

Başkan: Dr. Öğr. Üyesi Başak Ozan ÖZPARLAK

Özyeğin Üniversitesi, Hukuk Fakültesi

Onayladım

Üye: Dr. Öğr. Üyesi İlhan Fırat KILINÇER

Fırat Üniversitesi, Teknoloji Fakültesi

Onayladım

Bu tez, Enstitü Yönetim Kurulunun/...../20.....tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Burhan ERGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım “Uluslararası Hukuk Ve Teknik Standartlarına Uyumlu Adli Bilişim Süreçlerinin Geliştirilmesi ” Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

24.01.2025

Mustafa PEKDEMİR



ÖNSÖZ

Bu tez çalışmasında uluslararası hukuk ve teknik standartlara uyumlu adli bilişim süreçlerinin geliştirilmesi konusu ele alınmıştır. Teknolojinin hızla gelişmesi ve dijital dünyadaki suçların artması, adli bilişim süreçlerinin daha etkili ve uluslararası standartlarla uyumlu hale getirilmesini zorunlu kılmaktadır. Bu bağlamda, çalışmanın önemi, adli bilişimde küresel düzeyde bir standardizasyonun gerekliliğinden kaynaklanmaktadır. Bu süreç, karmaşık yapısı ve teknik zorlukları nedeniyle derinlemesine bir araştırma ve analiz gerektirmiştir. Ayrıca uluslararası hukuk ve teknik standartların farklılık göstermesi, çalışmanın kapsamını sınırlayan unsurlardan biri olmuştur fakat bu zorluklar, alana duyduğum ilgi ve motivasyonla aşılmış, sürecin başarılı bir şekilde tamamlanmasını sağlamıştır. Bu çalışmanın gerçekleşmesinde doğrudan katkı sağlayan danışmanım Doç. Dr. Fatih Ertam'a, bilgi ve rehberliği için teşekkürlerimi sunarım. Ayrıca, çalışma boyunca manevi desteklerini esirgemeyen aileme ve arkadaşlarıma da teşekkür ederim.

Mustafa PEKDEMİR

ELAZIĞ, 2025

İÇİNDEKİLER

Sayfa

ÖNSÖZ.....	iv
İÇİNDEKİLER.....	v
ÖZET	vii
ABSTRACT.....	viii
TABLolar LİSTESİ.....	ix
SİMGELER VE KISALTMALAR	x
1. GİRİŞ	1
2. ADLİ BİLİŞİM SÜREÇLERİNİN TANIMI VE ÖNEMİ	4
2.1. Adli Bilişim Nedir?.....	4
2.2. Adli Bilişim Süreçlerinin Aşamaları	5
2.3. Dijital Delillerin Toplanması, İncelenmesi ve Raporlanması	7
3. ULUSLARARASI HUKUK VE TEKNİK STANDARTLAR	9
3.1. Uluslararası Adli Bilişim Standartlarının Tarihçesi	9
3.2. ISO/IEC 27037 ve Diğer İlgili Standartlar	10
3.3. ENFSI (European Network of Forensic Science Institutes) Rehberleri	12
3.4. Budapeşte Sözleşmesi ve Uluslararası Anlaşmalar	14
4. TÜRKİYE’DE UYGULANAN ADLİ BİLİŞİM STANDARTLARI	17
4.1. Türkiye'deki Yasal Düzenlemeler	17
4.2. Türkiye'de Adli Bilişim Alanında Kullanılan Standartlar	21
4.3. Ulusal Yargı Ağı Projesi (UYAP) ve Dijital Delil Yönetimi.....	23
5. ULUSLARARASI STANDARTLAR İLE TÜRKİYE’DE UYGULANAN STANDARTLARIN	
KARŞILAŞTIRILMASI	25
5.1. Ortak Özellikler.....	25
5.1.1. Delillerin Toplanması ve Korunması	26
5.1.2. Raporlama ve Belgelendirme Standartları.....	27
5.1.3. Veri Bütünlüğü ve Güvenliği.....	28
5.2. Farklılıklar.....	30
5.2.1. Mevzuat ve Yasal Çerçeve Farklılıkları	31
5.2.2. Süreçte Uygulama Farklılıkları	32
6. ADLİ BİLİŞİM SÜREÇLERİNDE KARŞILAŞILAN ZORLUKLAR VE ÇÖZÜMLER.....	33
6.1. Teknik Zorluklar	33
6.1.1. Veri Toplama Aşamasında Karşılaşılan Zorluklar	34
6.1.2. Veri Analizi ve Yorumlamada Yaşanan Sorunlar	36
6.2. Hukuki ve Etik Zorluklar	37
6.2.1. Gizlilik ve Veri Güvenliği İkilemleri	38
6.2.2. Yasal Düzenlemelerdeki Sorunlar.....	40
7. ADLİ BİLİŞİMDE TEKNOLOJİK GELİŞMELER VE GELECEK YÖNELİMLERİ.....	42
7.1. Makine Öğrenimi Uygulamaları	42
7.1.1. Delil İnceleme Sistemleri.....	43
7.1.2. Suç Analizinde Veri Madenciliği.....	44

7.2. Blokzincir Teknolojisi ve Dijital Delillerin Güvenliđi	46
7.2.1. Blokzincir Tabanlı Kayıt Sistemleri.....	48
7.3. Bulut Biliřim ve Uzaktan Eriřim Çözümleri	49
7.3.1. Bulutta Veri Depolama ve Adli Analiz	50
7.3.2. Güvenlik ve Eriřim Kontrolü Zorlukları	52
8. MATERYAL VE METOT	54
8.1. Materyal.....	54
8.2. Metot.....	56
9. BULGULAR VE TARTIřMA.....	59
10. SONUÇLAR.....	68
ÖNERİLER.....	70
KAYNAKLAR	72
ÖZGEÇMİř	



ÖZET

Uluslararası Hukuk Ve Teknik Standartlarına Uyumlu Adli Bilişim Süreçlerinin Geliştirilmesi

Mustafa PEKDEMİR

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Ocak 2025, Sayfa: x + 75

Bu çalışma, adli bilişim süreçlerinin uluslararası hukuk ve teknik standartlarla uyumlu bir şekilde geliştirilmesinin önemini ve yöntemlerini incelemektedir. Teknolojinin hızla gelişmesi ve dijital verilerin adli olayların aydınlatılmasında artan önemi, adli bilişim disiplinine duyulan ihtiyacı artırmıştır fakat bu süreçlerin güvenilirliği ve geçerliliği için uluslararası normlara ve teknik standartlara uyum büyük önem taşımaktadır. Çalışma, mevcut adli bilişim süreçlerinde karşılaşılan hukuki ve teknik uyumsuzlukları analiz etmekte ve bu uyumsuzlukların giderilmesine yönelik çözüm önerileri sunmaktadır. Aynı zamanda çeşitli ülkelerdeki yasal düzenlemeler ve adli bilişim standartları karşılaştırılarak, uyumlu bir süreç geliştirilmesi için gereken adımlar ortaya konmaktadır. Bu bağlamda hem hukuki düzenlemeler hem de teknik standartlar incelenmiş ve adli bilişim uzmanlarının bu gereksinimleri karşılayabilmesi için yol haritası önerilmiştir. Bu tez çalışması, adli bilişim alanında daha güvenilir, şeffaf ve uluslararası kabul gören süreçlerin oluşturulmasına katkı sunmayı amaçlamaktadır.

Anahtar Kelimeler: Adli Bilişim, Hukuk, Bilişim Hukuku, Adli Bilişim Standartları

ABSTRACT

Development of Forensic Computer Processes Compliant with International Legal and Technical Standards

Mustafa PEKDEMİR

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences
Department of Digital Forensic Engineering
January 2025, Pages: x + 75

This study examines the importance and methods of developing digital forensic processes in accordance with international law and technical standards. The rapid development of technology and the increasing importance of digital data in the elucidation of forensic events have increased the need for digital forensic discipline, but compliance with international norms and technical standards is of great importance for the reliability and validity of these processes. The study analyzes the legal and technical incompatibilities encountered in current digital forensic processes and offers solutions to eliminate these incompatibilities. At the same time, the legal regulations and digital forensic standards in various countries are compared and the necessary steps for developing a compatible process are presented. In this context, both legal regulations and technical standards are examined and a roadmap is proposed for digital forensic experts to meet these requirements. This study aims to contribute to the creation of more reliable, transparent and internationally accepted processes in the field of digital forensic.

Keywords: Digital Forensics, Law, Informatics Law, Computer Forensics Standards

TABLÖLAR LİSTESİ

	Sayfa
Tablo 9.1. Uluslararası Standartlar ve Türkiye Mevzuatı Karşılaştırılması	65
Tablo 9.2. Adli Bilişim Çalışmalarında Ulusal Standartlara Uyumun Getireceği Olası Avantaj ve Dezavantajlar.....	66
Tablo 9.3. Adli Bilişim Çalışmalarında Uluslararası Standartlara Uyumun Getireceği Olası Avantaj ve Dezavantajlar.....	66



SİMGELER VE KISALTMALAR

Kısaltmalar

AB	: Avrupa Birliği
ENFSI	: European Network of Forensic Science Institutes (Avrupa Adli Bilimler Enstitüleri Ağı)
GDPR	: General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
IEC	: International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
ISO	: International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
KVKK	: Kişisel Verilerin Korunması Kanunu
NIST	: National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü, ABD)
TCK	: Türk Ceza Kanunu
TS	: Türk Standartları
UYAP	: Ulusal Yargı Ağı Projesi
CMK	: Ceza Muhakemesi Kanunu

1. GİRİŞ

Günümüzde dijital teknolojilerin hızla yaygınlaşması ve hayatın her alanında kullanılmaya başlaması, bilgi ve veri güvenliğine dair yeni zorlukları beraberinde getirmiştir. Bu durum, adli bilişim bilimini hem bireylerin hem de kurumların haklarını koruma noktasında vazgeçilmez bir disiplin haline getirmiştir. Adli bilişim, dijital delillerin tespit edilmesi, toplanması, incelenmesi ve mahkemelerde kullanılmasına kadar olan süreçleri kapsayan bir bilim dalıdır. Dijital delillerin adil yargulamalarda kullanılması ise hem yerel hem de uluslararası hukukun belirlediği standartlara uygunluk gerektirmektedir. Bunun yanı sıra adli bilişim süreçlerinin teknik standartlara uygun şekilde gerçekleştirilmesi, delillerin bütünlüğünün ve güvenilirliğinin sağlanmasında kritik bir rol oynamaktadır. Yusuf [1], adli bilişim sürecinde karşılaşılan sorunları ve bu sorunlara yönelik çözüm önerilerini ele almaktadır. Çalışmada, adli bilişim uzmanlarının karşılaştığı teknik, hukuki ve operasyonel zorluklar detaylı bir şekilde incelenmiştir. Özellikle dijital delillerin toplanması, muhafazası ve incelenmesi sırasında ortaya çıkan sorunlara odaklanılmıştır. Ayrıca, uluslararası standartlar ve yasal düzenlemelerle uyumlu adli bilişim süreçlerinin nasıl daha etkin hale getirilebileceği tartışılmıştır [17].

Bu tez çalışmasında adli bilişim süreçlerinin uluslararası hukuk normları ve teknik standartlarla nasıl uyumlu hale getirilebileceği ele alınmıştır. Özellikle sınır ötesi bilişim suçlarının artışı, uluslararası işbirliğini ve ortak standartların uygulanmasını zorunlu kılmaktadır. Bu bağlamda farklı ülkelerdeki adli bilişim yaklaşımlarını ve teknik standartları incelemek, sürecin küresel bir çerçevede nasıl geliştirilebileceği konusunda önemli ipuçları sunmaktadır. Çalışmanın amacı, mevcut adli bilişim uygulamalarını değerlendirmek ve uluslararası hukuk ve teknik standartlarla uyumlu, daha etkin bir süreç geliştirmek için öneriler sunmaktır. Ayrıca uluslararası düzenlemelerin yanı sıra, adli bilişim alanında kullanılan ISO standartları gibi teknik normlar da detaylı olarak analiz edilecektir. Bu bağlamda, adli bilişim uzmanlarının uluslararası kabul gören prosedürlere nasıl adapte olabileceği ve daha güvenilir sonuçlar elde edebileceği üzerine odaklanılmıştır. Ve adli bilişim süreçlerinin mevcut durumu ve temel kavramlar ele alınmıştır. Ayrıca adli bilişimin dijital delillerin toplanması, incelenmesi ve mahkemelerde kullanılmasına yönelik süreçleri detaylandırılmıştır. Buna ek olarak uluslararası hukuk normları ve adli bilişimdeki teknik standartlar detaylı bir şekilde analiz edilecektir. Özellikle Avrupa Birliği (AB) Genel Veri Koruma Tüzüğü (GDPR), Budapeşte Siber Suçlar Sözleşmesi, ISO/IEC 27037, ISO/IEC 27042 gibi önemli hukuki düzenlemeler ve teknik standartlar üzerinde durulmuştur. Bu normların adli bilişim süreçlerine etkileri ve sınır ötesi veri transferi, veri güvenliği ve dijital delil yönetimi konularındaki gereklilikleri değerlendirilecektir.

Adli biliřim srelerinin uluslararası hukuka ve teknik standartlara nasıl uyumlu hale getirilebileceğine dair öneriler verilecektir. Bu kapsamda adli biliřim uzmanları için geliştirilmesi gereken yeni prosedrler ve en iyi uygulama örnekleri ele alınmıştır.

Genel olarak dijital dünyada işlenen suçların artması, adli biliřimin önemini daha da artırmaktadır. Özellikle sınır ötesi suçların çzlmesinde dijital delillerin geçerliliğı ve btnlğ büyük önem taşımaktadır. Bu noktada dijital delillerin adil yargı srelerinde kanıt olarak kabul edilebilir olması için uluslararası hukuk normları ve teknik standartlarla uyumlu hale getirilmesi gerekmektedir. Adli biliřim sreleri, yalnızca yerel yasal düzenlemelere değıl, aynı zamanda küresel ölçekte kabul edilen düzenlemelere de uygun olmalıdır. Bu, farklı lkeler arasında bilgi paylaşımını ve işbirliğini kolaylařtırmakta ve sınır ötesi suçların çzmnde etkinliğı artırmaktadır. Örneğın Avrupa Birliğı'nın Genel Veri Koruma Tzğ (GDPR) gibi düzenlemeler, kiřisel verilerin korunmasını ve bu verilerin güvenli bir şekilde işlenmesini zorunlu kılmaktadır. Bu durum, adli biliřim srecinde toplanan verilerin korunması için belirli standartların uygulanmasını gerektirmektedir. Bunun yanı sıra Budapeřte Siber Sular Szleşmesi gibi uluslararası düzenlemeler de siber sularla mcadelede ortak standartların oluřturulmasına katkıda bulunmaktadır. Bu tr düzenlemeler, adli biliřim uzmanlarına rehberlik etmekte ve veri güvenliğı, dijital delil ynetimi ve sınır ötesi veri transferi gibi konularda yol gsterici standartlar sunmaktadır. Bu standartlar, delillerin toplanması, muhafazası, analiz edilmesi ve mahkemelerde kullanılabilir hale getirilmesi sırasında takip edilmesi gereken prosedrleri kapsamaktadır. Çalıřmada ayrıca adli biliřim alanında güvenilir ve geçerli sonular elde edebilmek için uygulanması gereken en iyi prosedrler ve örnekler de ele alınmaktadır. Bu bağlamda dijital delillerin güvenilirliğı, delil btnlğnn korunması ve bu srecin yasalara uygun şekilde ynetilmesi için öneriler sunulmaktadır. Adli biliřim srelerinin uluslararası hukuk normları ve teknik standartlarla uyumlu hale getirilmesi, dijital delillerin geçerliliğı ve güvenilirliğı açısından kritik bir öneme sahiptir. Bu çerevede uluslararası kabul grmř standartlar ve yasal düzenlemeler, adli biliřim uzmanlarına rehberlik etmekte ve srelerin etkinliğini ve doėruluėunu artırmaktadır.

Dijital delillerin toplanması, saklanması ve analiz edilmesi srelerinde, uluslararası hukuk normları ve düzenlemeler önemli bir rol oynamaktadır. Özellikle sınır ötesi biliřim sularının artışı, lkeler arası iş birliğini ve ortak standartların uygulanmasını zorunlu kılmaktadır. Bu kapsamda, Avrupa Birliğı'nın Genel Veri Koruma Tzğ (General Data Protection Regulation, GDPR) ve Budapeřte Siber Sular Szleşmesi gibi düzenlemeler, adli biliřim srelerine yn veren temel yasal çerevelerdir. Avrupa Birliğı tarafından 2018 yılında yrrlėe giren GDPR, kiřisel verilerin korunması ve işlenmesi konusunda sıkı kurallar getirmektedir. Adli biliřim srelerinde, kiřisel verilerin toplanması ve işlenmesi sırasında GDPR hkmlerine uyulması gerekmektedir. Bu, dijital delillerin elde edilmesi ve kullanılması srelerinde veri sahiplerinin haklarının korunmasını

sağlamaktadır. 2001 yılında imzalanan ve Türkiye'nin de taraf olduğu Budapeşte Siber Suçlar Sözleşmesi ise siber suçlarla mücadelede uluslararası iş birliğini teşvik etmektedir.

Sözleşme, dijital delillerin toplanması ve paylaşılması konusunda ortak prosedürler ve standartlar belirleyerek, adli bilişim süreçlerinin uluslararası uyumunu sağlamaktadır. Adli bilişim süreçlerinin teknik boyutunda Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından yayımlanan standartlar, süreçlerin etkinliği ve güvenilirliği açısından rehberlik etmektedir. Bu standartlar, dijital delillerin işlenmesi sırasında izlenmesi gereken prosedürleri ve en iyi uygulamaları tanımlamaktadır. Bununla beraber ISO/IEC 27037 standardı dijital delillerin tanımlanması, toplanması, elde edilmesi ve muhafaza edilmesi konusunda kılavuzluk sağlamaktadır. Adli bilişim uzmanlarının, delillerin bütünlüğünü ve güvenilirliğini koruyarak, uygun yöntemlerle elde edilmesini sağlamaktadır. ISO/IEC 27042 standardı ise dijital delillerin analizi ve yorumlanması süreçlerine yönelik rehberlik sunmakta olup delillerin geçerliliği, tekrarlanabilirliği ve doğrulanabilirliği konularında en iyi uygulamaları tanımlamaktadır. Bu sayede, adli bilişim uzmanları, delillerin mahkemelerde kabul edilebilirliğini artırmaktadır. ISO/IEC 27043 standardı da olay inceleme ilkeleri ve süreçleri hakkında kılavuzluk sağlamaktadır. Dijital olayların incelenmesi sırasında izlenmesi gereken adımları ve prosedürleri tanımlayarak, adli bilişim süreçlerinin standardizasyonunu desteklemektedir. Tüm bunlarla beraber adli bilişim uzmanlarının, uluslararası standartlar ve yasal düzenlemeler konusunda düzenli eğitim almaları ve farkındalıklarının artırılması gerekmektedir. Bu sayede, süreçlerin doğru ve etkin bir şekilde yürütülmesi sağlanmaktadır. Bu çerçevede /IEC 27037, ISO/IEC 27042 ve ISO/IEC 27043 gibi standartların, adli bilişim süreçlerinde aktif olarak uygulanması ve bu standartlara uygun prosedürlerin geliştirilmesi önemlidir. Bu kapsamda sınır ötesi bilişim suçlarıyla mücadelede, ülkeler arası iş birliğinin artırılması ve ortak standartların benimsenmesi gerekmektedir. Bu, dijital delillerin paylaşımı ve kullanımı süreçlerinde etkinliği artırmaktadır. Ayrıca adli bilişim süreçlerinde kullanılan teknolojik araçların ve yazılımların, uluslararası standartlara uygun ve güncel olması sağlanmalıdır. Bu, delillerin güvenilirliğini ve bütünlüğünü korumaktadır. Bu bağlamda adli bilişim süreçlerinin uluslararası hukuk normları ve teknik standartlarla uyumlu hale getirilmesi, dijital delillerin geçerliliği ve güvenilirliği açısından hayati bir öneme sahiptir. Bu uyumun sağlanması, adil yargılamaların gerçekleştirilmesi ve siber suçlarla etkin mücadele için gereklidir.

2. ADLİ BİLİŞİM SÜREÇLERİNİN TANIMI VE ÖNEMİ

Bu bölümde, adli bilişim süreçlerinin genel bir tanımına yer verilmesi, adli soruşturmalarda delil niteliğindeki dijital verilerin toplanması, saklanması, analiz edilmesi ve raporlanması gibi temel adımların açıklanması hedeflenmektedir. Adli bilişimin suç soruşturma süreçlerindeki önemine, özellikle dijital delillerin güvenilir ve yasal geçerliliğe sahip olmasının sağlanmasındaki rolüne dikkat çekilecektir.

2.1. Adli Bilişim Nedir?

Adli bilişim, dijital cihazlar ve sistemler üzerinde bulunan elektronik verilerin toplanması, saklanması, analiz edilmesi ve adli süreçlerde delil olarak sunulmasıyla ilgilenen bir bilim dalıdır. Bilgisayar, cep telefonu, sunucu gibi dijital cihazlardan elde edilen verilerin yanı sıra ağ trafiği, e-postalar ve bulut sistemlerindeki veriler de adli bilişimin inceleme alanına girmektedir. Adli bilişim, dijital verilerin bir suçun aydınlatılmasında veya bir davada kanıt olarak kullanılmasını sağlayarak dijital dünyanın adalet sistemine entegrasyonunu mümkün kılmaktadır. Bu disiplinin temel amacı, suç şüphesi bulunan bir olayda dijital delilleri adli sürecin gereksinimlerine uygun şekilde toplamak ve analiz etmektir. Bu süreçler, dijital verilerin güvenli bir şekilde muhafaza edilmesi ve manipülasyonlardan korunmasını sağlayacak şekilde yürütülmek zorundadır [1]. Bu bağlamda adli bilişim uzmanlarının hem teknik bilgiye hem de hukuki bilgiye sahip olması gerekmektedir. Delillerin kabul edilebilirliği, doğruluğu ve bütünlüğü, dijital delillerin incelenme ve sunulma biçimine bağlıdır. Bu bağlamda adli bilişim süreci; olay yeri incelemesi, veri toplama, veri analizi ve raporlama aşamalarını içermektedir. Genel olarak ilk aşama olan olay yeri incelemesinde dijital cihazlardan güvenli bir şekilde veri toplanmaktadır. Bu aşamada verilerin bütünlüğünü bozmadan ve delilleri değiştirmeden alınması kritik önemdedir. İkinci aşama olan veri toplamada elde edilen dijital deliller adli inceleme için saklanır ve kopyalanmaktadır. Üçüncü aşamada ise uzmanlar bu verileri analiz etmekte, delillerin ilişkilerini incelemekte ve suçun aydınlatılmasına yönelik veriler elde etmektedir. Tüm bunlarla beraber son olarak elde edilen bulgular raporlanmakta ve adli mercilere sunulmaktadır [2].

Adli bilişim, yalnızca suç soruşturmalarında değil, aynı zamanda iç soruşturmalar, fıkri mülkiyet davaları, siber güvenlik olayları ve veri sızıntıları gibi durumlarda da kullanılır. Teknolojik gelişmelerin hızla ilerlemesiyle birlikte, adli bilişim alanı da sürekli evrim geçirmekte ve yeni veri türleri ile sistemlerin incelenmesi gereksinimi ortaya çıkmaktadır. Adli bilişim, özellikle siber suçların araştırılmasında kilit bir role sahiptir. Dolandırıcılık, kimlik hırsızlığı, veri hırsızlığı ve fidye yazılımı gibi suçlar, genellikle dijital cihazlar ve ağlar üzerinden gerçekleştirilir.

Yüksel [1] çalışmasında bilişim hukukunun bağımsız bir hukuk dalı olarak incelenmesinin gerekliliğine dikkat çekmektedir. Bilişim hukukunun, hızla gelişen teknoloji ile birlikte, kendine özgü dinamikleri olan bir alan haline geldiği vurgulanmaktadır. Bu kapsamda kişisel verilerin korunması, siber suçlar ve bilişim sistemlerinin hukuki sorumluluğu gibi konuların önem kazandığı belirtilmektedir. Bu bağlamda bilişim hukukunun uluslararası düzenlemeler ve teknik standartlarla uyum içinde olması gerektiği ifade edilmektedir [1]. Bu nedenle adli bilişim uzmanlarının bu tür olayları çözmek için teknolojik bilgilerini sürekli güncel tutmaları ve dijital suçlar konusunda kapsamlı bilgiye sahip olmaları gerekmektedir. Bu süreçlerin güvenilirliği, yalnızca teknik becerilere değil, aynı zamanda ulusal ve uluslararası hukuk normlarına uygun hareket edilmesine de bağlıdır. Adli bilişim süreçlerinin yasal dayanakları, dijital delillerin mahkemelerde geçerli olabilmesi ve tarafsız bir şekilde değerlendirilebilmesi açısından hayati öneme sahiptir.

Adli bilişim, yalnızca teknik süreçlerle sınırlı olmayıp aynı zamanda hukuk sistemine sıkı sıkıya bağlı bir alandır. Dijital delillerin mahkemelerde kabul edilebilmesi için bu delillerin elde edilmesi, saklanması ve analiz edilmesi süreçlerinin ulusal ve uluslararası yasalara uygun olması gerekmektedir [3]. Bu bağlamda, adli bilişim uzmanlarının çalışmaları, delillerin zincirleme bir şekilde güvenilirliğini sağlayacak prosedürlerle gerçekleştirilmelidir. Delillerin güvenilirliğini korumak için kullanılan en yaygın yöntemlerden biri, delil zincirinin titizlikle takip edilmesidir. Delil zinciri, dijital bir delilin ilk elde edildiği andan itibaren kimler tarafından nasıl muhafaza edildiği ve hangi işlemlerden geçtiği gibi bilgileri içeren bir kayıt sistemidir. Bu sistem, dijital delillerin herhangi bir manipülasyona uğramadan incelendiğini ispatlamada kritik öneme sahiptir. Buna ek olarak adli bilişim süreçlerinde kullanılan yazılımların ve donanımların da belirli standartlara uygun olması gerekmektedir. Dijital delillerin analiz edilmesinde kullanılan araçlar, hatasız ve güvenilir sonuçlar vermelidir. Bu noktada uluslararası teknik standartlar, adli bilişim araçlarının doğruluğunu ve geçerliliğini garanti altına almak amacıyla belirlenmiştir [4]. ISO/IEC 27037, ISO/IEC 27042 ve ISO/IEC 27043 gibi uluslararası standartlar, adli bilişim süreçlerinde izlenmesi gereken adımları, yöntemleri ve araçları tanımlamaktadır. Adli bilişimin bu kadar önemli hale gelmesinin bir diğer nedeni de siber suçların giderek karmaşıklaşmasıdır. Özellikle uluslararası boyutta gerçekleşen siber saldırılar, farklı ülkelerdeki hukuk sistemleri arasında işbirliğini ve ortak standartların uygulanmasını gerektirmektedir. Bu da adli bilişimin sadece bir ülke içinde değil, uluslararası düzeyde de uyumlu bir şekilde yürütülmesi gerektiğini göstermektedir.

2.2. Adli Bilişim Süreçlerinin Aşamaları

Adli bilişim süreçleri, dijital delillerin toplanması, incelenmesi, analiz edilmesi ve adli makamlar önünde kanıt olarak sunulmasını kapsayan bir dizi aşamadan oluşmaktadır. Bu süreçlerin her bir aşaması, delillerin güvenilirliği ve yasal geçerliliği açısından kritik öneme sahiptir.

Herhangi bir adımda yapılan hata, delilin mahkemede kabul edilmemesine veya manipölasyon şüphesi ile reddedilmesine yol açabilmektedir. Bu nedenle adli bilişim süreçlerinin dikkatlice yürütölmesi, teknik ve hukuki standartlara tam uyum sağlanması gerekmektedir. Genel olarak adli bilişim süreçleri dört ana aşamada gerçekleşmektedir. Bunlar olay yeri incelemesi, veri toplama, veri analizi ve raporlama şeklindedir. Adli bilişim süreçlerinin ilk aşaması olan olay yeri incelemesi, suçun işlendiği dijital cihazlar ve sistemlerdeki verilerin tespit edilmesiyle başlamaktadır [5]. Olay yeri fiziksel bir ortam olabileceği gibi, uzaktan erişim sağlanan bir ağ veya bulut ortamı da olabilmektedir. Bu aşamada dijital delillerin tespit edilmesi ve toplanması süreci son derece önemlidir. Delillerin bozulmadan toplanması, manipölasyona uğramaması ve olay yerindeki diğer unsurların da kayıt altına alınması gerekmektedir. Bu çerçevede dijital delillerin toplanmasında kullanılan en önemli prensiplerden biri, delil bütönlüğünü korumaktır. Olay yeri incelemesinde dijital cihazların yetkisiz kişiler tarafından kullanılmaması ve verilerin değiştirilememesi için gerekli güvenlik önlemleri alınmaktadır. Bu aşamada dijital cihazların kapatılması ancak bu süreçte var olan prosedüre uyulmalı, direk kapatılmamalı, gerekli kontrol yapılarak açık uygulamalar ve uçucu bilgiler konusunda dikkatli olunmalıdır. Veya ağ bağlantısının kesilmesi gibi önlemler, veri bütönlüğünü korumak adına yaygın olarak kullanılan yöntemlerdir [6]. Tüm bunlarla beraber veri toplama aşaması, dijital delillerin fiziksel veya dijital bir ortamdan güvenli bir şekilde elde edilmesini kapsamaktadır. Bu süreçte dijital verilerin orijinal hali bozulmadan kopyalanması ve analiz edilmek üzere saklanması gerekmektedir. Veri toplama sürecinde kullanılan yazılım ve donanımların uluslararası standartlara uygun olması ve toplanan verilerin doğruluğunu garanti altına alması zorunludur. Adli bilişimde yaygın olarak kullanılan bir yöntem, dijital verilerin kopyalanması ve orijinal veriler üzerinde herhangi bir değişiklik yapılmadan incelemelerin bu kopya üzerinden gerçekleştirilmesidir.

Adli bilişim sürecinin ilk aşaması, olay yeri incelemesidir. Bu aşamada suçun işlendiği dijital cihazlar veya sistemlerdeki veriler tespit edilir ve olay yeri detaylı bir şekilde incelenmektedir. Olay yeri, fiziksel bir ortamda olabileceği gibi, dijital ağlar veya bulut sistemleri gibi sanal ortamlarda da bulunabilmektedir. Olay yeri incelemesinin temel amacı, dijital delillerin güvenli bir şekilde toplanmasını sağlamaktır. Bu aşamada cihazların yetkisiz kişiler tarafından kullanılmasının engellenmesi ve verilerin değiştirilmeden muhafaza edilmesi büyük önem taşımaktadır. Olay yerindeki delillerin güvenli bir şekilde muhafaza edilmesi ve manipölasyona uğramaması için gerekli önlemler alınmaktadır [7]. Dijital cihazların kapatılması veya ağ bağlantılarının kesilmesi gibi yöntemler, veri bütönlüğünü korumak amacıyla sıkça uygulanmaktadır. Tüm bunlarla beraber toplanan verilerin analiz edilmesi süreci, adli bilişimin en kritik aşamalarından biridir. Bu aşamada toplanan dijital delillerin incelenmesi, olayla ilgili bağlantıların ve ipuçlarının ortaya çıkarılması hedeflenmektedir. Analiz sürecinde uzmanlar verilerin içeriğini inceler, zaman çizelgeleri oluşturur ve suçun nasıl işlendiğine dair teknik detayları ortaya koymaktadır.

Analiz sürecinde kullanılan yazılımlar ve araçlar, elde edilen sonuçların doğruluğunu ve güvenilirliğini garanti etmelidir. Bu nedenle adli bilişim uzmanlarının kullandığı araçların uluslararası standartlarla uyumlu olması ve doğruluk testlerinden geçirilmiş olması son derece önemlidir [8]. Tüm bunlarla beraber adli bilişim sürecinin son aşaması, raporlama ve delillerin adli mercilere sunulmasıdır. Analiz sonucunda elde edilen bulgular, adli merciler için anlaşılır bir formatta rapor haline getirilmektedir. Raporlama aşamasında delillerin nasıl toplandığı, hangi yöntemlerin kullanıldığı ve analiz sürecinde elde edilen bulgular ayrıntılı bir şekilde açıklanmaktadır. Ayrıca, delillerin doğruluğu ve güvenilirliği ile ilgili tüm teknik detaylar raporda yer almalıdır. Bu raporlar, mahkemelerde dijital delillerin kullanılabilirliği açısından büyük önem taşır ve delillerin kabul edilebilirliğini sağlamaktadır. Mahkemeler, bu raporlar doğrultusunda dijital delillerin geçerliliğini değerlendirir ve kararlarını bu deliller ışığında oluşturmaktadır. Bu kapsamda veri analizi aşaması, adli bilişim sürecinin en önemli ve karmaşık bölümlerinden biridir [9].

Bu aşamada, olay yerinde toplanan dijital veriler, adli bilişim uzmanları tarafından incelenir ve analiz edilmektedir. Amaç, olayla ilgili önemli ipuçlarını bulmak, suçun nasıl işlendiğini ortaya çıkarmak ve suçun faillerine ulaşmaktır. Analiz edilen veriler, bilgisayarlar, cep telefonları, sunucular, ağlar ve bulut sistemlerindeki dijital izleri içerebilmektedir. Tüm bunlarla beraber veri analizinin başarısı, kullanılan araçların doğruluğuna ve uzmanların deneyimine bağlıdır [10]. Ayrıca bu aşamada elde edilen bulguların raporlanması süreci de son derece önemlidir. Verilerin adli incelemeye tabi tutulurken bütünlüklerinin korunması ve analiz süreçlerinin doğru bir şekilde kayıt altına alınması gerekmektedir. Her adımın kayıt edilmesi, sonrasında delil zincirinin doğruluğunu ispatlamak açısından hayati önem taşımaktadır. Bu çerçevede veri analiz aşamasından sonra elde edilen bulguların adli mercilere sunulması gerekmektedir. Raporlama aşaması, adli bilişim süreçlerinde son aşamadır ve delillerin nasıl toplandığını, hangi yöntemlerle analiz edildiğini ve bu süreçlerde elde edilen bulguların neler olduğunu detaylı bir şekilde açıklamaktadır [11].

2.3. Dijital Delillerin Toplanması, İncelenmesi ve Raporlanması

Adli bilişim süreçlerinin merkezinde dijital deliller yer almaktadır. Bu delillerin doğru bir şekilde toplanması, incelenmesi ve raporlanması, davaların çözülmesi ve dijital suçların aydınlatılması açısından büyük öneme sahiptir. Dijital deliller, elektronik cihazlarda bulunan, elektronik olarak oluşturulmuş, depolanmış veya iletilmiş her türlü veriyi kapsamaktadır. Bilgisayarlar, mobil cihazlar, ağlar, sunucular ve bulut depolama sistemleri gibi çeşitli kaynaklardan elde edilebilen bu delillerin hukuki süreçlerde geçerli olabilmesi için belirli teknik ve hukuki kurallar çerçevesinde işlenmesi gerekmektedir [12].

Bu süreçle ilişkili olarak Bedii [13], siber güvenlik ve bilişim suçlarına hukuki açıdan geniş bir bakış açısı sunmaktadır. Çalışmada, bilişim suçlarının çeşitliliği ve bu suçların yasal düzenlemelerle nasıl ele alındığı tartışılmıştır. Siber güvenlik tedbirleri ile adli bilişim süreçlerinin kesişim noktasında, özellikle suçların tespiti ve soruşturulması aşamalarında ortaya çıkan hukuki sorunlar detaylandırılmıştır. Ayrıca, adli bilişim süreçlerinin, bu suçların tespiti ve adli süreçlere taşınması açısından nasıl kritik bir rol oynadığını tartışmaktadır [5]. Dijital delillerin işlenmesinde, üç temel aşama bulunur: toplanma, incelenme ve raporlama. Bu süreçler, delillerin güvenilirliğinin korunması ve mahkemelerde kabul edilebilirliğinin sağlanması açısından birbirini tamamlayan kritik adımlardır. Dijital delillerin toplanması, adli bilişim sürecinin ilk ve en önemli aşamasıdır [13].

Bu aşama, delillerin dijital ortamdan güvenli ve yasal yollarla elde edilmesini kapsamaktadır. Delillerin toplanması sırasında yapılan herhangi bir hata, delilin mahkemede geçerli olmasını engelleyebilmekte veya delilin manipüle edildiği iddialarını ortaya çıkarabilmektedir. Bu nedenle dijital deliller toplanırken en önemli prensip, delil bütünlüğünün korunmasıdır. Tüm bunlarla beraber toplanan dijital verilerin orijinalliğini korumak ve verilerin herhangi bir şekilde değiştirildiğine dair şüpheleri önlemek için hash algoritmaları kullanılmaktadır. Hash değeri, delilin toplandığı andaki dijital imzasını belirlemekte ve her türlü değişikliğin tespit edilmesini sağlamaktadır. Dijital delillerin toplandığı cihazlar veya ortamlar, yetkisiz kişilerin erişimine kapatılmalıdır [14].

Bu, delillerin güvenliğini sağlamak ve yetkisiz müdahaleleri önlemek için kritik bir adımdır. Dijital cihazlar olay yerinden alınırken cihazların fiziksel olarak zarar görmemesi ve veri bütünlüğünün korunması önemlidir. Ayrıca cihazlar doğrudan kapatılmadan toplanmalı veya uygun veri çekme yöntemleriyle işlem yapılmalıdır. Tüm bunlarla beraber dijital delillerin toplanmasının ardından, bu verilerin incelenmesi aşamasına geçilmektedir. İnceleme sürecinde delillerin olayla nasıl ilişkilendirildiği ve suçun aydınlatılmasına nasıl katkı sağlayabileceği belirlenmektedir. Dijital delillerin incelenmesi, teknik uzmanlık ve doğru analiz araçlarının kullanımını gerektiren karmaşık bir süreçtir. Deliller incelenirken verilerin asılları hiçbir şekilde değiştirilmemeli ve analizler kopyalanmış veriler üzerinde yapılmalıdır. Bu, delil bütünlüğünün korunması açısından son derece önemlidir. Suç işleyen kişiler genellikle suçla ilgili verileri silmeye çalışmakta fakat silinen veriler birçok durumda geri getirilebilmektedir. Adli bilişim uzmanları, özel yazılımlar kullanarak bu verileri kurtarabilmekte ve incelemeye dâhil edebilmektedir. Dijital deliller üzerinde yapılan incelemeler sırasında dosyaların oluşturulma, değiştirilme ve erişilme zamanları gibi meta veriler incelenmektedir [15]. Bu veriler, olayın zaman çizelgesini oluşturma açısından büyük öneme sahiptir. Özellikle siber suçlarla ilgili olaylarda, ağ trafiği ve sistem logları, suçun nasıl gerçekleştirildiğine dair önemli ipuçları sunmaktadır. Bu kayıtlar incelenerek saldırganın hangi yollarla sisteme sızdığı, hangi verilere eriştiği ve hangi zararları verdiği anlaşılabilmektedir.

3. ULUSLARARASI HUKUK VE TEKNİK STANDARTLAR

Bu bölümde adli bilişim alanında uluslararası hukuk düzenlemeleri ve teknik standartların ne anlama geldiği ve bu standartların neden kritik olduğu üzerinde durulacaktır. Adli bilişim süreçlerinde uyulması gereken protokoller ve uygulamalar açısından ISO/IEC standartları gibi küresel kabul görmüş normlara değinilerek, bu standartların ülkeler arası iş birliğini nasıl kolaylaştırdığı açıklanacaktır.

3.1. Uluslararası Adli Bilişim Standartlarının Tarihçesi

Adli bilişim, dijital dünyada gerçekleşen suçların araştırılmasına yönelik bir disiplin olarak doğrudan teknolojik gelişmelere bağlıdır. İlk başlarda adli bilişim çalışmaları genellikle yerel ve bağımsız yöntemlerle yürütülmüş, standartların ve ortak protokollerin eksikliği nedeniyle farklı ülkelerde büyük farklılıklar göstermiştir fakat dijital suçların ve özellikle siber suçların sınır tanımayan doğası, adli bilişim alanında uluslararası bir standart ihtiyacını ortaya çıkarmıştır. Bu standartlar, dijital delillerin güvenilirliğini, hukuki geçerliliğini ve süreçlerin şeffaflığını sağlamak amacıyla geliştirilmiştir [16]. Bu çerçevede adli bilişim disiplininin resmi olarak ortaya çıkışı, 1990'lı yılların başlarına dayanmaktadır. Bilgisayar ve dijital cihazların yaygınlaşmasıyla birlikte, bu cihazlar üzerinde gerçekleştirilen suçlar da artış göstermiştir. İlk dönemlerde adli bilişim uzmanları, dijital cihazlardan veri elde etme ve inceleme konusunda kendi yöntemlerini geliştirmişlerdir fakat bu yöntemlerin çoğu, belirli bir standarda dayanmıyor ve mahkemelerde dijital delillerin kabul edilmesi zor olabilmektedir. Bu dönemde çeşitli ülkeler ve kurumlar, adli bilişim süreçlerinin standart hale getirilmesine yönelik çalışmalar yapmaya başlamışlardır. ABD'de Federal Soruşturma Bürosu (FBI) ve ABD Gizli Servisi, adli bilişimle ilgili ilk eğitim programlarını ve protokolleri oluşturmuşlardır. 1990'lı yılların ortalarına gelindiğinde bu alanda daha kapsamlı bir yaklaşım benimsenmeye başlanmış ve uluslararası işbirliklerinin önemi vurgulanmıştır [17].

2000'li yılların başında adli bilişim alanında ilk uluslararası standartlar geliştirilmeye başlanmıştır. Bu dönemde, dijital suçların artması ve internetin küresel bir ağ haline gelmesiyle birlikte farklı ülkelerde yürütülen soruşturamalar arasında uyum sağlama ihtiyacı ortaya çıkmıştır. Özellikle sınır ötesi siber suçların soruşturulmasında ortak standartlar geliştirilmesi gereği, uluslararası düzeyde işbirliğini zorunlu kılmıştır. Bu ihtiyaca yanıt olarak 2002 yılında Budapeşte Siber Suçlar Sözleşmesi kabul edilmiştir [18]. Avrupa Konseyi tarafından oluşturulan bu sözleşme, siber suçlarla mücadele konusunda uluslararası işbirliğini güçlendirmeyi ve ortak adli bilişim standartları geliştirmeyi amaçlamıştır. Budapeşte Sözleşmesi, dijital delillerin toplanması, saklanması ve analiz edilmesine ilişkin yasal çerçeveyi belirleyen ilk uluslararası belge olarak adli bilişim tarihinde önemli bir dönüm noktasıdır.

Uluslararası Standartlar Organizasyonu (ISO), adli bilişim süreçlerinde güvenilirliği sağlamak amacıyla 2000'li yılların ortalarından itibaren çeşitli standartlar geliştirmeye başlamıştır. İlk olarak 2005 yılında yayımlanan ISO/IEC 27001, bilgi güvenliği yönetim sistemleri için küresel bir standart haline gelmiştir. Bu standart, adli bilişim süreçlerinde kullanılan dijital sistemlerin güvenliğini sağlama amacı taşımakta ve dijital delillerin saklanması için önemli bir temel oluşturmaktadır. 2000'li yılların sonlarına doğru, adli bilişim alanına yönelik daha özel standartlar geliştirilmiştir. 2012 yılında yayımlanan ISO/IEC 27037, dijital delillerin toplanması, saklanması ve muhafaza edilmesine ilişkin standartları belirlemiştir.

2010'lu yıllar, adli bilişim alanında teknik standartların gelişimi açısından önemli bir dönem olmuştur. 2015 yılında yayımlanan ISO/IEC 27042 ve ISO/IEC 27043 standartları, dijital delil analizine ve olay sonrası analiz süreçlerine dair daha detaylı kurallar sunmuştur. Bu standartlar, olay incelemesinde hangi adımların izlenmesi gerektiğini ve dijital delil analizinde izlenecek yöntemleri detaylandırmıştır. Ayrıca bu dönemde Avrupa Birliği (AB) ve diğer uluslararası kuruluşlar, adli bilişim süreçlerinin standart hale getirilmesi için çeşitli direktifler ve düzenlemeler yayımlamışlardır [20]. 2016 yılında yürürlüğe giren AB Genel Veri Koruma Tüzüğü (GDPR), dijital verilerin korunması ve bu verilerin delil olarak kullanılabilmesi için belirli kurallar koymuştur. GDPR, dijital delillerin işlenmesi ve saklanması sırasında uyulması gereken veri güvenliği standartlarını tanımlayan önemli bir düzenleme olmuştur. 2020'li yıllara gelindiğinde siber suçların giderek daha karmaşık hale gelmesi ve büyük veri gibi teknolojilerin adli bilişim süreçlerinde kullanılmaya başlanması, uluslararası standartların daha da gelişmesine yol açmıştır. ISO/IEC 27050 gibi yeni nesil standartlar, özellikle bulut bilişim ortamlarında dijital delil yönetimini ve elektronik keşif süreçlerini ele almaktadır. Emekçi [20], adli bilişimde bulut bilişim teknolojilerinin yarattığı yeni paradigmaları incelemektedir. Yazarlar, bulut bilişimin adli bilişim süreçlerini nasıl dönüştürdüğünü ve bu yeni düzlemde karşılaşılan zorlukları ele almaktadır. Çalışmada bulut bilişimdeki dijital delillerin toplanması, muhafazası ve incelenmesi gibi süreçlerde karşılaşılan teknik ve hukuki sorunlar tartışılmaktadır. Ayrıca bulut bilişimin adli bilişimdeki geleneksel yöntemleri nasıl değiştirdiği ve bu yeni teknolojinin sunduğu fırsatlar üzerinde durulmuştur [20].

3.2. ISO/IEC 27037 ve Diğer İlgili Standartlar

Adli bilişim süreçlerinin uluslararası düzeyde standartlaştırılması, dijital delillerin güvenilirliğinin korunması ve hukuki geçerliliğinin sağlanması açısından kritik bir öneme sahiptir. Bu süreçlerin uluslararası kabul görmüş teknik standartlarla uyumlu bir şekilde yürütülmesi, delillerin toplanmasından analizine ve raporlanmasına kadar her adımın doğruluğunu ve şeffaflığını garanti altına almaktadır. Bu bağlamda ISO/IEC 27037 standardı, adli bilişim süreçlerinde dijital delil

yönetimi için bir temel oluşturmuş ve diğer ilgili ISO standartları ile birlikte dijital delil süreçlerinin yapılandırılmasına katkı sağlamıştır.

ISO/IEC 27037 standardı, adli bilişim süreçlerinde dijital delillerin yönetimine ilişkin en önemli standartlardan biridir. İlk olarak 2012 yılında yayımlanan bu standart, dijital delillerin nasıl güvenli bir şekilde toplanması, saklanması ve korunması gerektiğine dair ayrıntılı bir rehber sunmaktadır [21]. Standartın temel amacı, dijital delillerin güvenilirliğini ve bütünlüğünü koruyarak, hukuki süreçlerde geçerli olmasını sağlamaktır. Tüm bunlarla beraber delillerin toplanması sırasında uygulanacak prosedürler, delilin bütünlüğünü koruyacak şekilde belirlenmiştir. Standartta göre toplanan her dijital delilin hash değeri alınarak delilin orijinalliği kanıtlanmalı ve bu deliller güvenli ortamlarda saklanmalıdır. Ayrıca veri toplama sırasında kullanılan yazılımların ve donanımların uluslararası standartlara uygun olması gerektiği vurgulanmaktadır. Toplanan dijital delillerin fiziksel ve dijital olarak güvenli bir şekilde saklanması, bu standartta önemli bir yer tutmaktadır. Dijital delillerin saklandığı ortamların güvenli olması, yetkisiz erişimlere karşı korunması ve verilerin bütünlüğünün bozulmadan muhafaza edilmesi gerektiği açıklanmaktadır.

Delil zinciri, toplanan her delilin kim tarafından ve nasıl işlendiğini gösteren bir kayıt sistemidir. ISO/IEC 27037 standardı, delil zincirinin nasıl takip edilmesi gerektiğini ve delilin toplandığı andan itibaren nasıl muhafaza edilmesi gerektiğini ayrıntılı bir şekilde tanımlamaktadır. Bu, delilin mahkemelerde kabul edilebilirliğini sağlamak açısından kritik bir unsurdur. ISO/IEC 27042, dijital delillerin analiz edilmesi sürecini tanımlayan bir diğer önemli standarttır. İlk olarak 2015 yılında yayımlanan bu standart, dijital delillerin incelenmesi ve analiz edilmesine yönelik süreçleri detaylandırmaktadır [22]. ISO/IEC 27042, dijital delillerin nasıl analiz edilmesi gerektiğini ve hangi yöntemlerin kullanılabileceğini açıklamaktadır. Bununla beraber ISO/IEC 27043 standardı, dijital olayların nasıl inceleneceği ve dijital delillerin olay sonrası nasıl değerlendirileceği konularını kapsamaktadır. Bu standart, adli bilişim uzmanlarının olay müdahalesi sırasında hangi adımları izlemesi gerektiğini ve olay yerinden dijital delil toplama işlemlerinin nasıl yürütüleceğini açıklamaktadır. Bununla ilişkili olarak Çil ve Demirci [21] çalışmalarında, ağ adli bilişimi süreçlerinin gereksinimlerini belirleyip yazılım tanımlı ağlar (SDN) üzerinde incelemeler yapmışlardır. Yazarlar, ağ adli bilişiminde süreçlerin nasıl yürütüldüğünü ve bu süreçlerde ihtiyaç duyulan teknik gereksinimleri ele almaktadır. Özellikle SDN teknolojisinin, ağ adli bilişim süreçlerinde sağladığı avantajlar ve karşılaşılan zorluklar detaylı olarak incelenmiştir. Çil ve Demirci [21], ağ adli bilişiminde kullanılacak yöntemlerin ve araçların gelişen teknolojilere uyum sağlaması gerektiğine dikkat çekmektedir [21]. ISO/IEC 27043, özellikle olay sonrası müdahale süreçlerine odaklanarak dijital delil toplama ve analiz süreçlerinin belirli bir disiplin çerçevesinde yürütülmesini sağlamaktadır. Bu standart, dijital olay incelemelerinde hangi metodların kullanılabileceğini, delillerin nasıl işleneceğini ve olayın tekrar yaratılmasına yönelik simülasyon çalışmalarının nasıl yürütüleceğini tanımlamaktadır.

Ayrıca dijital delil inceleme süreçlerinin nasıl belgeleneceği ve bu süreçlerde karşılaşılan zorlukların nasıl aşılabacağı konusunda rehberlik sunmaktadır. Bununla beraber ISO/IEC 27050, adli bilişim süreçlerinde elektronik keşif süreçlerini ele alan bir standarttır [23]. Elektronik keşif, dijital verilerin toplanması, işlenmesi ve incelenmesi sürecini kapsayan bir yöntemdir. Özellikle büyük çaplı davalarda veya kurumsal soruşturmalarda, dijital verilerin analiz edilmesi ve delil olarak kullanılabilmesi için elektronik keşif süreci kullanılmaktadır. ISO/IEC 27001 ise bilgi güvenliği yönetim sistemlerini tanımlamaktadır. Bu çerçevede adli bilişim süreçlerinde kullanılan dijital sistemlerin güvenliğinin sağlanmasına yönelik önemli prensipler sunmaktadır. ISO/IEC 17025 ise laboratuvar ortamlarında gerçekleştirilen testlerin doğruluğunu ve güvenilirliğini sağlamaktadır. Bu standart, adli bilişim analizlerinin gerçekleştirildiği laboratuvarların sertifikasyonu için kullanılmaktadır. NIST 800-86 rehberi ise ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilmiştir. Bu rehber, dijital delillerin toplanması, işlenmesi ve analiz edilmesine yönelik prosedürleri tanımlamaktadır. Tüm bunlarla beraber ISO/IEC 27037 ve diğer ilgili standartlar, adli bilişim süreçlerinin her aşamasında güvenliliğin ve şeffaflığın sağlanması için önemli bir yapı taşı oluşturulmaktadır [1]. Bu standartlar, dijital delillerin toplanması, incelenmesi, saklanması ve mahkemelerde kabul edilebilirliğini garanti altına alırken aynı zamanda uluslararası düzeyde uyumlu bir adli bilişim süreci oluşturulmasına katkı sağlamaktadır.

3.3. ENFSI (European Network of Forensic Science Institutes) Rehberleri

Adli bilimlerin çeşitli dallarında çalışan kurumlar arasında iş birliği ve standartları geliştirmek amacıyla kurulan ENFSI (European Network of Forensic Science Institutes), Avrupa genelinde adli bilişim süreçlerinin uyumlu hale getirilmesi ve güçlendirilmesi için önemli bir rol oynamaktadır. 1995 yılında kurulan bu ağ, adli bilimlerin farklı alanlarında rehberler, standartlar ve iyi uygulama örnekleri sunarak adli süreçlerin bilimsel doğruluğunu artırmayı hedeflemektedir. ENFSI, özellikle dijital adli bilişim alanında güvenilir ve kabul edilebilir delillerin toplanması, analiz edilmesi ve sunulması süreçlerine yönelik rehberler yayımlamış ve bu rehberler, Avrupa genelinde adli bilim kurumları tarafından yaygın olarak benimsenmiştir. ENFSI'nin temel amacı, adli bilimlerin tüm dallarında kaliteyi ve doğruluğu sağlamak ve Avrupa genelinde standartları uyumlu hale getirmektir [2]. Dijital delillerin toplanması, saklanması ve analiz edilmesine yönelik rehberler, adli bilişim uzmanlarına süreçlerin nasıl doğru ve güvenilir bir şekilde yürütüleceğine dair pratik bir kılavuz sunmaktadır. Bu rehberler, adli bilişim süreçlerinin şeffaf olmasını sağlamakla birlikte mahkemelerde delillerin kabul edilebilirliğini artırmak amacıyla bilimsel metotlar ve teknik standartların kullanılmasını teşvik etmektedir. Bu bağlamda ENFSI rehberleri, dijital delillerin güvenilirliğini ve bütünlüğünü korumayı hedeflerken aynı zamanda delil zincirinin (chain of custody) doğru bir şekilde yönetilmesini sağlamaktadır.

Bu durum bağlantılı olarak Nguyen [12] çalışmasında dijital adli bilim alanına genel bir bakış sunulmaktadır. Yazar, dijital adli bilimin temel prensiplerini ve bu alanda kullanılan teknikleri ele alarak, adli bilişim süreçlerinin nasıl işlediğini özetlemektedir. Dijital delillerin incelenmesi, saklanması ve yargı süreçlerine entegre edilmesi üzerine kısa bir değerlendirme sunan Nguyen [12], adli bilişim uzmanlarının karşılaştığı temel sorunlar ve bu sorunların çözümüne yönelik yaklaşımlar hakkında bilgi vermektedir. Çalışma, dijital adli bilimin hızla gelişen teknolojik değişimlere nasıl adapte olduğu ve bu alandaki yeni gelişmelere dair bir bakış açısı sunmaktadır [12].

Delil zinciri, delillerin toplanmasından saklanmasına, incelenmesinden mahkemeye sunulmasına kadar her adımın belgelendiği ve delilin kimler tarafından nasıl işlendiğini gösteren bir sistemdir. ENFSI rehberleri, bu zincirin her aşamasında izlenecek prosedürleri net bir şekilde tanımlayarak delillerin herhangi bir manipülasyona uğramadan mahkemede güvenle kullanılmasını garanti etmektedir. Tüm bunlarla beraber ENFSI'nin dijital adli bilişim rehberleri, Avrupa genelinde adli bilişim süreçlerinin standardizasyonuna katkı sağlamaktadır. Dijital delillerin toplanması, analiz edilmesi ve raporlanması aşamalarında rehberlik sunarak bu süreçlerde izlenecek adımları açık bir şekilde belirlemektedir [3]. Ayrıca rehberler teknik standartlara dayandığı için, adli bilişim uzmanlarının kullandığı yazılım ve donanımların doğruluğunu ve güvenilirliğini garanti altına almaktadır. Örneğin ENFSI'nin "Best Practice Manual for the Forensic Examination of Digital Technology" adlı rehberi, dijital cihazların incelenmesine yönelik en iyi uygulama örneklerini sunmaktadır. Bu rehber, dijital delillerin hangi yöntemlerle toplanacağını, hangi analiz araçlarının kullanılacağını ve bu süreçlerin nasıl belgeleneceğini detaylandırmaktadır.

Rehberin sunduğu yöntemler, adli bilişim uzmanlarına dijital delilleri nasıl güvenilir ve şeffaf bir şekilde yönetebileceklerini öğretirken aynı zamanda adli bilim laboratuvarlarının kalite standartlarını da yükseltmektedir. Tüm bunlarla beraber dijital cihazlardan delil toplama sürecinde rehberler, cihazların fiziksel bütünlüğünün korunmasını, verilerin güvenli bir şekilde elde edilmesini ve delilin orijinalliğinin korunmasını sağlamaktadır. Bu süreçle ilişkili olarak Çağlayan [13] çalışmasında adli bilişim bağlamında kayıt tutma ve delil toplama ilkelerini incelemektedir. Yazar, adli bilişim süreçlerinde delil toplamanın ve bu delillerin güvenli şekilde muhafaza edilmesinin kritik önemini vurgulamaktadır. Çağlayan [13], delil toplama süreçlerinde uluslararası standartlar ve teknik gereksinimlerin uyumlu bir şekilde uygulanmasının önemine de değinmiştir. Adli bilişim uzmanlarının karşılaştığı zorluklar ve bu alandaki gelişmelere yönelik çözüm önerileri de çalışmanın önemli bir bölümünü oluşturmaktadır [13].

ENFSI rehberleri, bu tür teknik prosedürlerin nasıl uygulanacağını ve bu işlemlerin delil zinciri içerisinde nasıl kaydedileceğini açıkça tanımlamaktadır. Tüm bunlarla beraber ENFSI rehberleri, adli bilişim süreçlerinde kalite güvencesini sağlamada kritik bir rol oynamaktadır. Avrupa genelinde faaliyet gösteren adli bilim kurumları arasında ortak standartların benimsenmesini sağlayarak delil inceleme süreçlerinde şeffaflık ve güvenilirliği artırmaktadır. Kalite güvencesi,

sadece delillerin mahkemelerde kabul edilebilirliğini sağlamakla kalmaz, aynı zamanda adli bilişim uzmanlarının uluslararası standartlara uygun çalışmasını ve en iyi uygulamaları takip etmesini teşvik etmektedir [4].

Adli bilişim süreçlerinde kalite güvencesi sağlamak için ENFSI, laboratuvar akreditasyonlarını da teşvik eder. ENFSI'nin önderlik ettiği rehberler ve kalite yönetim sistemleri, laboratuvarların ISO/IEC 17025 gibi uluslararası standartlara uygun olarak çalışmasını desteklemektedir. Bu standartlar, laboratuvarların yürüttüğü testlerin doğruluğunu ve güvenilirliğini garanti etmektedir [5]. Böylece dijital delillerin analiz edilmesi sırasında kullanılan tekniklerin bilimsel geçerliliği ve güvenilirliği artırılmış olmaktadır. ENFSI rehberleri, sadece Avrupa'da değil, küresel çapta da adli bilişim alanında uluslararası işbirliğini desteklemektedir.

Dijital suçların sınırları aşan yapısı nedeniyle farklı ülkelerde yürütülen soruşturmaların birbirine entegre olabilmesi için ortak standartların ve rehberlerin benimsenmesi gerekmektedir. ENFSI'nin geliştirdiği rehberler, Avrupa'daki adli bilim kurumları arasında iş birliğini artırırken aynı zamanda dünya genelinde adli bilişim uzmanlarının ortak bir dil kullanmasını sağlamaktadır. Tüm bunlarla beraber ENFSI (European Network of Forensic Science Institutes) rehberleri, adli bilişim süreçlerinde güvenilirlik, şeffaflık ve uluslararası uyumluluk sağlamak açısından kritik bir rol oynamaktadır [6]. Dijital delillerin toplanması, incelenmesi ve raporlanmasına yönelik sunduğu rehberler, Avrupa genelinde ortak standartların benimsenmesine ve adli süreçlerin bilimsel doğruluğunun artırılmasına katkı sağlamaktadır. Ayrıca kalite güvencesi sağlayarak adli bilim laboratuvarlarının güvenilirliğini artırır ve uluslararası işbirliklerini güçlendirmektedir. ENFSI'nin sunduğu rehberler, dijital delil yönetiminde yüksek kalite standartlarını sağlamayı hedefleyen adli bilişim uzmanları için önemli bir kaynak niteliği taşımaktadır [7].

3.4. Budapeşte Sözleşmesi ve Uluslararası Anlaşmalar

Dijital teknolojilerin hızla gelişmesiyle birlikte, siber suçlar ve dijital ortamda işlenen suçlar küresel bir tehdit haline gelmiştir. Siber suçlar, coğrafi sınırları aşan yapısıyla tek bir ülkenin yargı yetkisiyle sınırlı kalmayan, karmaşık ve uluslararası düzeyde işbirliği gerektiren bir mücadele alanı yaratmıştır [8]. Bu bağlamda dijital suçlarla etkin bir şekilde mücadele edebilmek için ülkeler arasında ortak hukuki düzenlemeler ve işbirliği protokolleri geliştirilmesi zorunlu hale gelmiştir.

Bu ihtiyaca yanıt olarak kabul edilen Budapeşte Siber Suçlar Sözleşmesi (Budapest Convention on Cybercrime), siber suçlarla mücadelede uluslararası işbirliğini sağlayan en önemli hukuki çerçevelerden biri olmuştur. Bu bağlamda Budapeşte Sözleşmesi, Avrupa Konseyi tarafından hazırlanmış ve 23 Kasım 2001 tarihinde Budapeşte'de imzalanmıştır.

Siber suçlar konusundaki ilk uluslararası anlaşma niteliği taşıyan bu sözleşme, dijital suçlarla mücadelede ülkeler arasında ortak hukuki standartların belirlenmesini ve işbirliğinin güçlendirilmesini hedeflemiştir. Sözleşme, özellikle internet üzerinden işlenen suçların önlenmesi

ve bu suçlarla ilgili dijital delillerin etkin bir şekilde toplanması, saklanması ve paylaşılması süreçlerini düzenlemektedir. Budapeşte Sözleşmesi'nin ana amacı, siber suçlarla mücadele için ulusal yasaların uyumlu hale getirilmesi ve uluslararası işbirliği mekanizmalarının oluşturulmasıdır [9]. Sözleşme, dijital delillerin toplanması, saklanması ve paylaşılması konusunda ülkeler arasında ortak bir zemin oluşturmaktadır. Aynı zamanda siber suçların soruşturulması sırasında izlenecek adımlar ve uluslararası işbirliğinin nasıl sağlanacağına dair rehberlik etmektedir. Bu sayede siber suçlarla mücadelede daha hızlı, etkin ve uyumlu bir yaklaşım benimsenmesi amaçlanmıştır. Budapeşte Sözleşmesi, dört ana başlık altında düzenlenmiştir. Bunlar siber suçların tanımlanması, dijital delillerin toplanması, siber suçların önlenmesi ve uluslararası işbirliği şeklindedir. Ayrıca sözleşme, bilgisayar ve internet ortamında işlenen suçları çeşitli kategorilere ayırarak tanımlamaktadır [10].

Bu suçlar arasında bilgisayar sistemlerine yetkisiz erişim, veri hırsızlığı, kötü amaçlı yazılım kullanımı, çocuk pornografisi, telif hakkı ihlalleri ve kimlik hırsızlığı gibi suçlar yer almaktadır. Bu kategorilerin tanımlanması, uluslararası işbirliği yapılacak ülkelerin aynı suç türleri üzerinde ortak bir anlayış geliştirmesini sağlamaktadır. Ayrıca sözleşme, dijital delillerin toplanması ve saklanmasına ilişkin prosedürleri belirlemektedir [11]. Dijital delillerin güvenilirliğinin korunması için hangi adımların izleneceği, hangi yazılım ve donanımların kullanılacağı ve delil bütünlüğünün nasıl sağlanacağına dair kurallar sözleşme kapsamında yer almaktadır. Ayrıca delil zincirinin korunması ve bu delillerin uluslararası düzeyde paylaşımı için gerekli teknik ve hukuki adımlar detaylandırılmaktadır.

Budapeşte Sözleşmesi, siber suçlarla mücadelede ulusal önlemlerin artırılması için taraf devletlere çeşitli yükümlülükler getirmektedir. Bu kapsamda taraf devletler kendi iç hukuklarında siber suçlarla ilgili cezai müeyyideler oluşturmali ve bu suçlarla mücadele edecek teknik altyapıları güçlendirmelidir [12]. Ayrıca siber suçların önlenmesi için halkın bilinçlendirilmesi ve eğitim programlarının geliştirilmesi de teşvik edilmektedir. Bu durumla bağlantılı olarak Akbal [6] çalışmalarında adli bilişim mühendisliği müfredatının geliştirilmesi ve bu alandaki eğitim gereksinimlerine odaklanmıştır. Ayrıca adli bilişim mühendisliği eğitiminin uluslararası standartlara uygun olması ve bu alandaki gelişmelerin yakından takip edilmesinin önemi dile getirilmiştir [6].

Bu mekanizma, bir ülkede işlenen siber suçlarla ilgili dijital delillerin başka bir ülkede yürütülen soruşturmalarda kullanılmasını sağlamaktadır. Ayrıca sınır ötesi veri talepleri ve siber suçluların iadesi gibi konularda da işbirliği yapılmasını öngörmektedir. Tüm bunlarla beraber Budapeşte Sözleşmesi, sadece Avrupa Konseyi üyeleri tarafından değil, dünya genelinde birçok ülke tarafından imzalanmış ve kabul edilmiştir [13]. Bugün itibarıyla 65'ten fazla ülke bu sözleşmeye taraf olmuş ve siber suçlarla mücadelede ortak standartları benimsemiştir. Bu durum, sözleşmenin küresel bir etki yarattığını ve siber suçlarla mücadelede uluslararası işbirliğini büyük ölçüde

güçlendirdiğini göstermektedir. Amerika Birleşik Devletleri, Japonya, Kanada ve Avustralya gibi Avrupa dışındaki ülkeler de Budapeşte Sözleşmesi'ni imzalayarak bu uluslararası işbirliği çerçevesine katılmıştır [14].

Budapeşte Sözleşmesi, aynı zamanda diğer uluslararası anlaşmalara ve bölgesel işbirliği protokollerine ilham vermiştir. Örneğin Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve benzeri düzenlemeler, Budapeşte Sözleşmesi'nin dijital delil yönetimi ve veri güvenliği konularında ortaya koyduğu ilkelerle paralellik göstermektedir. Ayrıca INTERPOL ve Europol gibi uluslararası güvenlik örgütleri de bu sözleşmenin hükümlerini benimseyerek, siber suçlarla mücadelede işbirliğini artırmışlardır [15]. Budapeşte Sözleşmesi dışında siber suçlarla mücadelede uluslararası işbirliğini destekleyen çeşitli başka anlaşmalar da mevcuttur. Bunlardan biri, Birleşmiş Milletler'in (BM) Uluslararası Organize Suçlarla Mücadele Sözleşmesidir. Bu sözleşme, organize suçlar ve terörizmle mücadelede uluslararası işbirliğini teşvik etmekte ve siber suçları bu kapsamda ele almaktadır. BM'nin bu sözleşmesi, özellikle terörizm finansmanı, siber casusluk ve uluslararası veri hırsızlığı gibi konularda önemli bir rol oynamaktadır [16]. Genel olarak Budapeşte Sözleşmesi ve diğer uluslararası anlaşmalar, siber suçlarla küresel ölçekte mücadele edilmesi için kritik bir hukuki çerçeve sunmaktadır. Bu sözleşmeler, dijital delillerin toplanması, saklanması ve paylaşılması süreçlerini standartlaştırarak, uluslararası işbirliğini artırmakta ve siber suçlarla mücadelede daha etkin bir yol izlenmesine olanak tanımaktadır.

4. TÜRKİYE’DE UYGULANAN ADLİ BİLİŞİM STANDARTLARI

Bu kısımda Türkiye’de geçerli olan adli bilişim standartları ele alınacak ve Türkiye’deki uygulamaların diğer ülkelerle karşılaştırıldığında ne gibi farklılıklar veya benzerlikler gösterdiğine değinilecektir. Türkiye’deki adli bilişim politikaları, kullanılan teknolojik araçlar ve prosedürler hakkında genel bilgiler verilerek mevcut yasal çerçevenin bu standartları nasıl desteklediği tartışılacaktır.

4.1. Türkiye’deki Yasal Düzenlemeler

Türkiye’de adli bilişim, dijital suçların soruşturulması, dijital delillerin toplanması ve bu delillerin adli süreçlerde kullanılması konusunda belirli yasal düzenlemeler ve kanunlarla çerçevelenmiştir. Adli bilişim, hem cezai hem de hukuki davalarda delil toplama ve analiz sürecinde giderek artan bir öneme sahip olmuştur [17]. Türkiye’de adli bilişim süreçlerinin yürütülmesinde belirli kanunlar ve yönetmelikler uygulanmakta olup, bu süreçler uluslararası normlara ve teknik standartlara uyumlu bir şekilde yürütülmeye çalışılmaktadır. Ayrıca bu konu bağlamında Düden [22], Türkiye’de adli bilişimin gelişimi ve dijital delil incelemelerine odaklanan yüksek lisans tezinde, Türkiye’de adli bilişim alanındaki tarihsel gelişim sürecini incelemiştir. Çalışma, dijital delillerin toplanması, analiz edilmesi ve yargı süreçlerinde kullanılmasıyla ilgili karşılaşılan zorluklara ve bunların çözüm yollarına değinmektedir. Ayrıca dijital delillerin güvenilirliği, mahkemelerde geçerliliği ve bu süreçlerde kullanılan teknolojilerin değerlendirilmesi önemli bir yer tutmaktadır [22]. Türkiye’deki dijital suçlarla mücadelede en önemli yasal düzenlemelerden biri 5237 sayılı Türk Ceza Kanunudur (TCK).

TCK, dijital ortamda işlenen suçları tanımlayan çeşitli maddelere sahiptir. Özellikle bilişim suçlarına yönelik düzenlemeler, kanunun "Bilişim Alanında Suçlar" başlıklı 243, 244 ve 245. maddelerinde yer almaktadır. Bu konuyla ilişkili olarak Alptekin ve Kartal [2] çalışmalarında Türk Ceza Hukukunda bilişim sistemine girme suçuna dair kapsamlı bir inceleme yapılmıştır. Yazarlar, bu suçun özellikle ceza hukuku açısından değerlendirilmesinde dikkat edilmesi gereken unsurları detaylandırmıştır. Bilişim sistemlerine yetkisiz girişin, toplum üzerindeki etkisi ve bu tür suçların önlenmesine yönelik hukuki düzenlemelerin gerekliliği tartışılmaktadır. Alptekin ve Kartal [2] özellikle bilişim suçlarına yönelik cezaların caydırıcılık fonksiyonunu nasıl icra ettiğini ele almış ve bu konuda hukuki boşluklara işaret etmiştir [2].

Bu maddeler, bilgisayar sistemlerine izinsiz giriş, sistemin çalışmasını engelleme veya verileri bozma, silme, değiştirme gibi eylemleri suç olarak tanımlamaktadır. Ayrıca bu maddelerde dijital suçların işlendiği ortamlara ve suç faillerine yönelik cezai müeyyideler de belirtilmektedir. TCK

Madde 243: “(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.” Bu bağlamda madde 243 Bilişim sistemine girme suçu, bir başkasına ait bilişim sistemine izinsiz olarak girilmesi ve burada kalınması fiillerini kapsamaktadır. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu bağlamında TCK Madde 244: “(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.” Şeklinde. Madde 244, Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, bilişim sistemlerinin işleyişine zarar vermek amacıyla gerçekleştirilen saldırıları düzenler. Verilerin bozulması, değiştirilmesi veya silinmesi bu madde kapsamında cezalandırılmaktadır. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu TCK Madde 245 bağlamında “(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır. (3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (4) Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz. (5) (Ek: 6/12/2006 – 5560/11 md.) Birinci

fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.” şeklindedir. Bu bağlamda madde 245 banka veya kredi kartlarının kötüye kullanılması suçu, dijital ortamda yapılan finansal dolandırıcılık ve kimlik hırsızlığı gibi bilişim suçlarını ele almaktadır. Bu maddeler çerçevesinde, bilişim suçlarıyla mücadelede dijital delillerin toplanması ve kullanılması hukuki bir zemine oturtulmuş durumdadır [18]. Ayrıca bu düzenlemeler, adli bilişim uzmanlarının, dijital delilleri toplayıp analiz ederken hangi hukuki çerçeve içinde hareket etmeleri gerektiğini belirlemektedir. Bu durum bağlamında Mahmutoglu [9], Türk Ceza Kanunu’nda bilişim suçlarına yer veren maddeleri yargı kararları ışığında değerlendirmektedir. Yazar, bilişim suçlarıyla ilgili kanuni düzenlemelerin uygulamada nasıl sorunlarla karşılaştığını ve bu sorunların yargı kararları ile nasıl çözüldüğünü ele almıştır.

Mahmutoglu [9], özellikle yargı kararlarının bilişim suçlarına ilişkin içtihat oluşturmada ne kadar etkili olduğunu vurgulamış ve bu alanda gelişmesi gereken noktaları işaret etmiştir [9]. Bu çerçevede İhtiyaroğlu [11], bilişim sistemine girme suçunu yargı kararları bağlamında detaylı bir şekilde incelemektedir. Çalışmada, bilişim sistemlerine yetkisiz giriş suçunun unsurları, bu suça yönelik yargı kararlarının analizi ve Türk Ceza Hukuku’ndaki yerinin kapsamlı bir değerlendirmesi yapılmıştır. Özellikle cezaların caydırıcılık fonksiyonunun nasıl işlediği ve yasal düzenlemelerin yeterliliği üzerine önemli tespitler yapılmıştır [11].

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu bağlamında internet ortamında yapılan yayınların düzenlenmesine ve bu yayınlar yoluyla işlenen suçlarla mücadeleye ilişkin esasları belirlemektedir [19]. Bu kanun, özellikle dijital suçların önlenmesi ve internet üzerinden gerçekleştirilen suçların takibi konusunda önemli bir rol oynamaktadır. 5651 sayılı kanun, internet sağlayıcıları ve içerik sağlayıcılarına yükümlülükler getirirken, aynı zamanda dijital delillerin toplanması ve mahkemelerde kullanılmasına yönelik düzenlemeler de içermektedir. Kanun, belirli suçların işlendiği internet sitelerine erişimin engellenmesine ilişkin hükümlere yer vermektedir. Erişim engelleme kararları, adli bilişim süreçlerinde dijital delil toplama ve suçun tespit edilmesi açısından önemli bir rol oynamaktadır [20]. Kanun kapsamında internet trafiği ve kullanıcı verilerinin belirli sürelerle saklanması zorunlu tutulmuştur. Bu düzenleme, siber suçların tespiti ve dijital delillerin toplanması için önemli bir kaynak oluşturmaktadır [21].

Tüm bunlarla beraber dijital delillerin toplanması ve analiz edilmesi sürecinde kişisel verilerin korunması büyük bir öneme sahiptir. Bu bağlamda, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye’deki adli bilişim süreçlerinde dikkat edilmesi gereken önemli yasal düzenlemelerden biridir. KVKK, kişisel verilerin işlenmesi sırasında bireylerin mahremiyetini koruma amacı taşımakta ve adli bilişim süreçlerinde toplanan verilerin nasıl işleneceğine dair esaslar belirlemektedir. Adli bilişim süreçlerinde toplanan dijital delillerin bir kısmı, kişisel verileri içerebilmektedir. Bu durumda, KVKK’ya uygun hareket edilmesi gerekmektedir [22]. Özellikle

veri sahibinin onayı alınmadan kişisel verilerin işlenmesi yasaklanmış olup adli süreçler için gerekli hallerde yetkili makamlardan alınan izinlerle bu veriler işlenebilmektedir. KVKK, dijital delillerin toplanması ve analizi sürecinde, veri güvenliği ve kişisel gizliliğin korunmasına yönelik çerçeveyi sağlamaktadır. Tüm bunlarla beraber 5271 sayılı Ceza Muhakemesi Kanunu (CMK), ceza davalarında dijital delillerin nasıl kullanılacağına dair hükümler içermektedir [23]. CMK, dijital delillerin elde edilmesi, saklanması, incelenmesi ve mahkemelerde delil olarak sunulmasına yönelik kuralları belirlemektedir. Bu kapsamda, adli bilişim uzmanlarının dijital delil toplama süreçlerinde CMK'ya uygun hareket etmeleri gerekmektedir. Ayrıca belirtmek gerekir ki Özen ve Özocak [7] çalışmalarında, adli bilişim süreçleri ve elektronik delillerin hukuki rejimini incelemiştir. Özellikle CMK m. 134 kapsamında bilgisayarlarda arama ve el koyma tedbirlerinin hukuki boyutları detaylı olarak ele alınmaktadır. Yazarlar, bu tedbirlerin uygulanmasındaki hukuki sınırları ve yargı kararları çerçevesinde nasıl yorumlandığını analiz etmektedir. Özen ve Özocak [7], CMK m. 134'ün uygulanmasında ortaya çıkan pratik sorunları ve bu sorunların çözüm yollarını değerlendirirken, adil yargılanma hakkı ve kişisel mahremiyetin korunması gibi konulara dikkat çekmiştir [7].

CMK'nın ilgili hükümleri, dijital delillerin toplanması sürecinde kolluk kuvvetlerinin nasıl hareket etmesi gerektiğini ve dijital cihazlara nasıl el konulacağını düzenlemektedir. Bu süreçte, dijital delillerin hukuka aykırı bir şekilde elde edilmesi durumunda bu deliller mahkemede geçersiz sayılabilmektedir. Bu nedenle delil toplama aşamasında CMK'ya uygun hareket edilmesi büyük önem taşımaktadır. Dijital delillerin bulunduğu cihazların aranması ve bu cihazlara el konulması, kanunun belirlediği kurallar çerçevesinde gerçekleştirilmektedir. Bu bağlamda CMK bu sürecin nasıl yürütüleceğini ve hangi durumlarda dijital delillere el konulabileceğini detaylı bir şekilde açıklamaktadır [1]. Bu süreçle ilişkili olarak Kara [8] çalışmasında dijital kanıtların incelenmesi ve bu incelemelerin hukuki boyutu üzerine odaklanmıştır. Yazar, dijital delillerin elde edilmesi ve bu delillerin yargı sürecindeki rolüne dair önemli tespitler yapmıştır. Dijital kanıtların doğruluğu ve güvenilirliği, özellikle adli bilişim süreçlerinde kritik bir öneme sahiptir. Kara [8], dijital delillerin incelenmesi sürecinde kullanılan tekniklerin hukuki boyutlarını analiz etmiş ve bu tür delillerin mahkemelerde ne şekilde kullanılabileceği üzerine hukuki değerlendirmelerde bulunmuştur. Ayrıca dijital kanıtların hukuka uygun elde edilmesi ve saklanması gerekliliği üzerinde durulmuştur [8].

Elektronik İmza Kanunu, bu imzaların hukuki geçerliliğini düzenler ve adli bilişim süreçlerinde kullanılabilecek elektronik belgelerin doğrulanmasına ilişkin esasları belirlemektedir. Türkiye'de adli bilişim süreçlerinin yürütülmesi, belirli yasal düzenlemelere ve uluslararası standartlarla uyumlu teknik gerekliliklere bağlıdır. 5237 sayılı Türk Ceza Kanunu, 5651 sayılı Kanun ve 6698 sayılı Kişisel Verilerin Korunması Kanunu gibi düzenlemeler, dijital delillerin toplanması, analizi ve mahkemelerde kullanılması için gerekli hukuki çerçeveyi sağlamaktadır. 1 Haziran 2025 itibarı

ile yapılan deęiřiklikler de Trk Ceza Kanunu'nda geerlilik iin gncellięin n planda tutulduęunu gstermiřtir. Aynı zamanda Ceza Muhakemesi Kanunu ve Bilgi Teknolojileri ve İletiřim Kurumu'nun (BTK) dzenlemeleri de bu srelerde nemli bir yer tutmaktadır. Bu dzenlemeler, Trkiye'de dijital sularla mcadelede ve adli biliřim srelerinin hukuka uygun yrtlmesinde temel dayanak noktalarıdır [2]. Bu durumla baęlantılı olarak Deęirmenci [3] alıřmasında, adli biliřimde kullanılan triyaj ynteminin ceza muhakemesi hukuku aısından nemi ve uygulanabilirlięi incelenmiřtir. Triage yntemi, adli biliřim srelerinde delillerin sınıflandırılması ve nceliklendirilmesi aısından kritik bir rol oynamaktadır. Delillerin toplanmasındaki zaman baskısının azaltılması ve adli srelerin hızlandırılması iin triyaj ynteminin ceza muhakemesi hukuku aısından deęerlendirildięi bu alıřmada, yntemin hem pratik hem de teorik aıdan katkıları analiz edilmiřtir. Deęirmenci [3], triyajın adli biliřim srelerinde uygulanması sırasında karřılařılan sorunlara da deęinmiř ve zm nerileri sunmuřtur [3].

4.2. Trkiye'de Adli Biliřim Alanında Kullanılan Standartlar

Adli biliřim, dijital delillerin toplanması, analizi ve raporlanması srelerinde yksek hassasiyet gerektiren bir disiplindir. Trkiye'de adli biliřim alanında kullanılan standartlar, hem ulusal yasal dzenlemeler hem de uluslararası kabul grmř standartlarla řekillenmektedir. Bu standartlar, adli biliřim uzmanlarının dijital delil toplama ve analiz srelerinde izlemesi gereken yol haritasını belirlerken dijital delillerin gvenilirlięini ve geerlilięini saęlamaya yardımcı olmaktadır. Trkiye'de adli biliřim srelerinde ISO/IEC standartları, uluslararası iyi uygulamalar ve yerel dzenlemeler dikkate alınarak belirlenen eřitli standartlar kullanılmaktadır [3]. İlk olarak ISO/IEC 27037 standardı, Trkiye'de adli biliřim srelerinde kullanılan en nemli uluslararası standartlardan biridir. Bu standart, dijital delillerin nasıl tanımlanacaęı, toplanacaęı, saklanacaęı ve korunacaęına iliřkin kapsamlı bir rehber sunmaktadır. Trkiye'deki adli biliřim uzmanları, delil toplama ve koruma srelerinde bu standardı temel alarak hareket etmektedir. ISO/IEC 27037'nin amacı, dijital delillerin toplanma srecinde btnlęnn korunması ve toplanan delillerin gvenilirlięinin mahkemelerde kabul edilebilirlięini saęlamaktır [4]. ISO/IEC 27042 standardı, dijital delillerin analiz edilmesi ve bu srete izlenmesi gereken adımları dzenlemektedir. Trkiye'de adli biliřim uzmanları, dijital delillerin incelenmesi sırasında bu standardı takip ederek toplanan delillerin nasıl analiz edileceęi ve bu srete hangi yntemlerin kullanılacaęını belirlemektedir [5].

ISO/IEC 27042, delillerin bilimsel doęruluęunun saęlanması ve bu doęruluęun mahkemelerde kabul edilebilmesi iin adli biliřim uzmanlarının izleyebileceęi standartlařtırılmıř analiz prosedrleri sunmaktadır. Bu standart, Trkiye'de adli biliřim laboratuvarlarında kullanılacak analiz yntemlerinin seiminde de yol gsterici olmaktadır. zellikle silinmiř verilerin kurtarılması, řifreli verilerin zlmesi ve zaman damgalarının incelenmesi gibi teknik analiz

süreçlerinde uluslararası normlara uygun bir yaklaşım benimsenmektedir. Bununla beraber ISO/IEC 27043, olay sonrası müdahale ve dijital delil inceleme süreçlerine ilişkin standartları tanımlamaktadır [6].

Türkiye’de siber saldırı veya dijital suç olaylarına müdahale süreçlerinde bu standart esas alınmaktadır. Özellikle büyük çaplı veri ihlalleri, siber saldırılar ve dijital sistemlere yapılan izinsiz erişim gibi durumlarda adli bilişim uzmanları bu standarda uygun bir olay inceleme yöntemi izlemektedir. Bu standardın Türkiye’de uygulanması, özellikle kamu kurumlarında ve büyük ölçekli şirketlerde siber saldırılara karşı alınan tedbirlerin artırılmasına yardımcı olmaktadır [7]. Ayrıca olay müdahalesi sırasında toplanan delillerin güvenilirliğini ve bütünlüğünü sağlayarak, soruşturmalarda kullanılacak delillerin mahkemelerde kabul edilebilirliğini sağlamaktadır. Türkiye’deki kurumsal soruşturmalar ve adli süreçlerde, büyük miktarda dijital verinin incelenmesi gereken durumlarda bu standart kullanılmaktadır. Bu standart, özellikle elektronik ortamda belgelerin toplanması, işlenmesi ve raporlanmasına yönelik prosedürler sunmaktadır. Bu bağlamda Türkiye’deki adli bilişim uzmanları, elektronik keşif süreçlerinde uluslararası standartları takip ederek büyük veri setlerini analiz ederken doğru ve güvenilir sonuçlar elde etmeye çalışmaktadır [8].

Tüm bunlarla beraber Türkiye’de adli bilişim alanında kullanılan yerel bir standart olan TS 13571, Türkiye’de bilişim suçlarıyla mücadeleyle yönelik adli bilişim uygulamalarını düzenlemektedir. Bu standart, Türkiye’deki adli bilişim uzmanlarının dijital delilleri toplarken ve analiz ederken izlemeleri gereken yerel prosedürleri ve yöntemleri tanımlamaktadır. TS 13571 standardı, Türkiye’de adli bilişim süreçlerinin uluslararası standartlarla uyumlu hale getirilmesi amacıyla oluşturulmuş olup yerel ihtiyaçları ve hukuki düzenlemeleri de göz önünde bulundurarak dijital delillerin toplanması ve kullanılması süreçlerine yönelik kapsamlı bir çerçeve sunmaktadır [9]. Genel olarak Türkiye’de adli bilişim süreçlerinde sıklıkla karşılaşılan bir diğer önemli konu, elektronik imza uygulamalarıdır. 5070 sayılı Elektronik İmza Kanunu, dijital belgelerin hukuki geçerliliğini sağlamak amacıyla elektronik imzaların nasıl kullanılacağını düzenlemektedir. Elektronik imzalar, dijital belgelerin güvenliğini ve bütünlüğünü sağlarken, bu belgelerin adli süreçlerde delil olarak kullanılmasını kolaylaştırmaktadır. Bu düzenlemeler, siber suçların takibinde ve dijital delil toplama süreçlerinde önemli bir kaynak oluşturmaktadır [10].

BTK tarafından getirilen düzenlemeler, Türkiye’deki dijital suçlarla mücadelede adli bilişim uzmanlarına, internet trafiği ve kullanıcı verilerini toplama konusunda rehberlik sağlamaktadır. Bu düzenlemeler, adli bilişim uzmanlarının dijital delilleri toplarken hangi verilerin nasıl saklanacağını ve ne şekilde korunacağını belirlemektedir. Türkiye’de adli bilişim alanında kullanılan standartlar, uluslararası kabul görmüş ISO/IEC standartlarıyla yerel düzenlemelerin birleşimi olarak şekillenmektedir [11]. ISO/IEC 27037, 27042, 27043 ve 27050 gibi uluslararası standartlar, Türkiye’deki adli bilişim uzmanlarına dijital delil toplama, analiz etme ve raporlama süreçlerinde

rehberlik etmektedir. Bununla birlikte TS 13571 gibi yerel standartlar ve Elektronik İmza Kanunu gibi düzenlemeler, Türkiye'deki adli bilişim süreçlerinin ulusal gereksinimlerle uyumlu hale getirilmesini sağlamaktadır. Türkiye’de adli bilişim süreçlerinde kullanılan bu standartlar, dijital delillerin güvenilirliğini sağlamak ve ulusal ve uluslararası hukuka uygun hareket etmek için kritik bir rol oynamaktadır.

4.3. Ulusal Yargı Ağı Projesi (UYAP) ve Dijital Delil Yönetimi

Türkiye’de adli bilişim süreçlerinin etkin bir şekilde yönetilmesi ve dijital delillerin adalet sistemine entegre edilmesi amacıyla hayata geçirilen Ulusal Yargı Ağı Projesi (UYAP), dijital dönüşümün adalet sistemine sağladığı en önemli projelerden biridir. UYAP, 2000’li yılların başında Adalet Bakanlığı tarafından geliştirilen, tüm yargı mercilerini, kolluk kuvvetlerini ve ilgili devlet kurumlarını kapsayan kapsamlı bir elektronik yargı bilişim sistemidir. Bu sistem, dijital delillerin toplanması, saklanması, analiz edilmesi ve yargı süreçlerine entegre edilmesi açısından önemli bir rol oynamaktadır [12]. Ulusal Yargı Ağı Projesi (UYAP), adalet hizmetlerinin hızlı, güvenli ve etkin bir şekilde sunulmasını sağlamak amacıyla tasarlanmış bir elektronik sistemdir. Bu proje, Türkiye'deki yargı süreçlerinin dijital ortamda yürütülmesini mümkün kılarken aynı zamanda dijital delillerin yönetimini de önemli ölçüde kolaylaştırmaktadır. UYAP, mahkemeler, savcılıklar, avukatlar, kolluk kuvvetleri ve diğer adli birimler arasında veri paylaşımını dijital ortamda sağlamakta ve süreçlerin daha hızlı ve şeffaf bir şekilde ilerlemesine olanak tanımaktadır [13].

UYAP’ın temel işlevlerinden biri, dijital delil yönetimini bütünsel bir şekilde yargı sistemine entegre etmektir. Bu sistem sayesinde mahkemelerde kullanılan dijital deliller güvenli bir şekilde saklanabilmekte, dosyalar elektronik ortamda yönetilebilir ve dijital delillere erişim kontrollü bir şekilde sağlanabilmektedir [14]. UYAP, bu sayede hem delillerin güvenliğini artırmakta, hem de yargı süreçlerinde dijital delillerin kullanımını yaygınlaştırmaktadır. Dijital deliller, modern hukuk sistemlerinde giderek daha önemli bir yer tutmaktadır. UYAP, bu delillerin etkin bir şekilde toplanması, saklanması ve yargı süreçlerinde kullanılmasını sağlamak amacıyla gelişmiş dijital altyapılar sunmaktadır.

Sistem, dijital delillerin toplanmasından mahkemelerde kullanılmasına kadar olan süreçlerin güvenli ve şeffaf bir şekilde yürütülmesini mümkün kılmaktadır. UYAP, dijital delillerin elektronik ortamda toplanarak sistem üzerinden güvenli bir şekilde yargı mercilerine iletilmesini sağlamaktadır. Emniyet ve jandarma gibi kolluk kuvvetleri tarafından toplanan dijital deliller, UYAP üzerinden adli birimlere aktarılabilir. Bu süreç, delillerin fiziki ortamda taşınmasına gerek kalmadan dijital olarak güvenli bir şekilde aktarılmasını sağlamaktadır. Bu, delil zincirinin korunması açısından kritik öneme sahiptir. UYAP, dijital delillerin güvenli bir şekilde saklanmasına olanak tanımaktadır [15].

Deliller, UYAP'ın dijital altyapısında saklanarak yetkisiz erişimlere karşı koruma altına alınmaktadır. UYAP, aynı zamanda delil bütünlüğünü sağlamak amacıyla güvenlik protokolleri ve şifreleme yöntemleri kullanmaktadır. Bu sayede dijital delillerin manipüle edilmesi veya izinsiz erişim gibi durumlar engellenmektedir. UYAP, dijital delillerin ilgili taraflar arasında güvenli bir şekilde paylaşılmasına olanak tanımaktadır [16]. Avukatlar, savcılar ve hakimler, davalarla ilgili dijital delillere güvenli bir şekilde erişim sağlayabilmekte fakat bu erişimler, yetkilendirme ve izin süreçlerine bağlıdır, böylece delillere sadece yetkili kişilerin erişmesi sağlanmaktadır. Bu da dijital delillerin mahremiyetini koruma açısından önemli bir avantajdır. Tüm bunlarla beraber UYAP, Türkiye'deki adalet sisteminde dijital dönüşümün önemli bir adımıdır. Dijital delillerin etkin bir şekilde toplanması, saklanması ve yargı süreçlerinde kullanılmasına olanak tanıyan bu sistem, adli süreçlerde şeffaflığı ve verimliliği artırmıştır.



5. ULUSLARARASI STANDARTLAR İLE TÜRKİYE'DE UYGULANAN STANDARTLARIN KARŞILAŞTIRILMASI

Bu bölümde uluslararası alanda kabul edilen adli bilişim standartları ile Türkiye'de uygulanan standartlar karşılaştırılarak Türkiye'nin uluslararası normlara uyum durumu değerlendirilecektir. Benzerlikler, farklılıklar ve bu farklılıkların neden olabileceği avantaj veya dezavantajlar analiz edilerek uyum sağlama veya geliştirme gereksinimleri vurgulanacaktır.

5.1. Ortak Özellikler

Adli bilişim süreçlerinde uluslararası standartlar ile Türkiye'de uygulanan standartlar arasında birçok ortak özellik bulunmaktadır. Bu ortaklıklar, dijital delillerin güvenilirliğini ve bütünlüğünü sağlama, delil toplama ve analiz süreçlerini standardize etme ve adli bilişim uygulamalarının hukuki geçerliliğini güçlendirme amacını taşımaktadır [17]. Hem Türkiye'de hem de uluslararası düzeyde kabul edilen standartlar, adli bilişim uzmanlarının dijital delil yönetimi süreçlerini etkin, güvenilir ve şeffaf bir şekilde yürütmesine olanak tanımaktadır. Genel olarak hem uluslararası adli bilişim standartları (örneğin ISO/IEC 27037, ISO/IEC 27042) hem de Türkiye'de uygulanan TS 13571 gibi yerel standartlar, dijital delillerin bütünlüğünün korunması ve güvenilirliğinin sağlanması konusunda benzer prensiplere dayanmaktadır. Dijital delillerin toplanması sırasında delil bütünlüğünün korunması, delillerin mahkemelerde geçerli ve güvenilir sayılması açısından kritik bir öneme sahiptir.

Bu standartlar, delillerin orijinal hallerinin bozulmadan kopyalanmasını, saklanmasını ve analiz edilmesini zorunlu kılmaktadır. Her iki sistem de delillerin bütünlüğünü sağlamak amacıyla hash algoritmalarının kullanılmasını önermektedir. Hash algoritmaları, dijital delilin toplanmasından itibaren orijinalliğinin doğrulanmasını ve her türlü manipülasyona karşı korunmasını sağlamaktadır. Bu süreç, hem uluslararası hem de Türkiye'deki uygulamalarda sıkı bir şekilde takip edilen ortak bir prosedürdür [18]. Tüm bunlarla beraber uluslararası standartlar (ISO/IEC 27037 gibi) ve Türkiye'de uygulanan düzenlemeler, delil zincirinin eksiksiz bir şekilde belgelendirilmesi gerektiğini vurgulamaktadır. Bu süreçte delilin toplanması, kopyalanması, saklanması ve analiz edilmesi gibi her adımın detaylı bir şekilde kayıt altına alınması gerekmektedir. Hem Türkiye'deki hem de uluslararası standartlarda, delil zincirinin herhangi bir kopukluk veya eksiklik olmadan takip edilmesi gerekliliği, delillerin güvenliğinin sağlanması açısından ortak bir özelliktir. Adli bilişim süreçlerinde kullanılan teknik yöntemler ve araçlar, hem uluslararası standartlar hem de Türkiye'de uygulanan standartlar tarafından benzer şekilde tanımlanmakta ve uygulanmaktadır. Dijital delillerin toplanması, analiz edilmesi ve raporlanmasında kullanılan yazılımlar, donanımlar ve teknik prosedürler, uluslararası normlarla uyumlu olacak şekilde düzenlenmiştir [19].

Örneğin ISO/IEC 27042 standardı dijital delil analiz süreçlerinde kullanılacak yöntemleri belirlerken Türkiye'deki adli bilişim uygulamaları da bu yöntemlere büyük ölçüde paralellik göstermektedir. Hem Türkiye’de hem de uluslararası düzeyde, adli bilişim uzmanlarının kullandıkları yazılımlar ve donanımların, delil bütünlüğünü koruyacak şekilde tasarlanmış olması gereklidir [20].

5.1.1. Delillerin Toplanması ve Korunması

Dijital delillerin toplanması ve korunması, adli bilişim süreçlerinde en kritik aşamalardan biridir. Hem uluslararası standartlar hem de Türkiye’de uygulanan adli bilişim standartları, dijital delillerin hukuka uygun, güvenilir ve eksiksiz bir şekilde toplanmasını ve bu delillerin muhafaza edilmesini zorunlu kılmaktadır. Delil toplama ve koruma sürecinde delillerin bütünlüğünün korunması ve herhangi bir manipülasyonun önlenmesi büyük önem taşımaktadır. Bu süreç, delillerin geçerliliği ve mahkemelerde kabul edilebilirliği açısından belirleyici bir unsurdur. Uluslararası standartlar, dijital delillerin toplanması ve korunması aşamalarında detaylı prosedürler sunmaktadır [21]. Bu süreçte en yaygın olarak kullanılan standartlardan biri ISO/IEC 27037’dir. Bu standart, dijital delillerin hangi yöntemlerle toplanacağını, nasıl saklanacağını ve delil bütünlüğünün nasıl sağlanacağını belirlemektedir. Dijital delillerin elde edildiği cihazlardan (bilgisayar, mobil cihaz, sunucular vb.) veri çekme işlemi sırasında orijinal verilerin bozulmadan korunması gerekmektedir. Bunun için delil toplama işlemi sırasında genellikle verilerin kopyalanması ve incelemelerin bu kopya üzerinde yapılması tavsiye edilmektedir. Tüm bunlarla beraber toplanan dijital deliller, güvenli bir ortamda saklanmalıdır. Bu süreçte verilerin yetkisiz erişimlerden korunması ve fiziksel olarak zarar görmemesi sağlanmalıdır.

ISO/IEC 27037, delillerin saklanması sürecinde şifreleme ve fiziksel güvenlik önlemlerinin nasıl uygulanacağını da detaylandırmaktadır. Bu standartlar, uluslararası çapta adli bilişim uzmanlarının dijital delilleri güvenli ve eksiksiz bir şekilde toplaması ve muhafaza etmesi için bir yol haritası sunmaktadır. Bu bağlamda Türkiye’de dijital delillerin toplanması ve korunmasına ilişkin standartlar, büyük ölçüde uluslararası normlara paralel olarak uygulanmaktadır. Türkiye’de uygulanan TS 13571 standardı, bilişim suçlarına yönelik adli bilişim süreçlerinde delillerin toplanması ve korunmasına dair yerel düzenlemeler sunmaktadır [22]. Bu standart, Türkiye’deki adli bilişim uzmanlarının uluslararası en iyi uygulamalarla uyumlu hareket etmelerini sağlayarak dijital delillerin güvenilirliğini temin etmektedir. Türkiye’de dijital delillerin toplanması sırasında orijinal verilerin bütünlüğünün korunması için genellikle kopyalama yöntemi tercih edilmektedir. Bu süreçte adli bilişim uzmanları, dijital cihazlarda bulunan verileri toplarken bu verilerin değiştirilmediğini veya silinmediğini garantilemek zorundadır. Bu kapsamda Çekiç [4] çalışmasında bilgisayar verilerinde arama, kopyalama ve el koyma tedbirlerinin hukuki niteliği üzerine kapsamlı bir değerlendirme yapmıştır.

Yazar, bu tedbirlerin özellikle ceza muhakemesi hukuku çerçevesinde nasıl uygulandığını ele alırken hukuki süreçlerin etkinliği ve adil yargılanma hakkı açısından da bu tür tedbirlerin önemine vurgu yapmaktadır. Çekiç [4], bilgisayar verilerinde yapılan aramaların ve kopyalamaların, delil elde etme sürecinde hassas bir denge gerektirdiğini savunmakta ve hukuki sınırların titizlikle korunması gerektiğini belirtmektedir. Ayrıca el koyma tedbirinin uygulanma usulleri ve bu süreçlerde oluşabilecek hak ihlalleri üzerine de önemli değerlendirmelerde bulunulmuştur [4].

Türkiye’de dijital delillerin toplanması, Ceza Muhakemesi Kanunu (CMK) gibi yasal düzenlemelere uygun olmalıdır. Bu bağlamda, adli bilişim uzmanları, dijital delilleri toplarken yasal prosedürlere uymalı ve delilin hukuka aykırı şekilde elde edilmemesine dikkat etmelidir. Aksi halde dijital deliller mahkemelerde kabul edilmeyebilir. Türkiye’de dijital delillerin korunması sırasında, hem fiziki hem de dijital güvenlik önlemleri alınarak delillerin muhafaza edilmesi sağlanmaktadır. Bilgi Teknolojileri ve İletişim Kurumu (BTK) düzenlemeleri çerçevesinde dijital verilerin saklanması ve bu verilere erişimin denetlenmesi gereklidir. Verilerin yetkisiz kişilerce değiştirilmemesi veya zarar görmemesi için güvenlik protokolleri uygulanmaktadır. Toplanan dijital delillerin güvenli bir ortamda saklanması ve yetkisiz kişilerin erişimine karşı korunması, her iki sistemde de kritik bir gerekliliktir [23]. Delillerin güvenliğine yönelik alınan önlemler, delilin manipülasyona uğramadan muhafaza edilmesini sağlamaktadır. Genel olarak dijital delillerin toplanması ve korunması süreçlerinde uluslararası standartlar ile Türkiye’de uygulanan düzenlemeler arasında önemli ortaklıklar bulunmaktadır.

5.1.2. Raporlama ve Belgelendirme Standartları

Adli bilişim süreçlerinde dijital delillerin güvenilirliği ve hukuki geçerliliği, sadece delillerin doğru bir şekilde toplanması ve korunmasıyla değil, aynı zamanda bu süreçlerin doğru bir şekilde raporlanması ve belgelendirilmesiyle de sağlanmaktadır. Hem uluslararası standartlar hem de Türkiye’de uygulanan adli bilişim standartları, dijital delillerin nasıl raporlanacağı ve süreçlerin nasıl belgelendirileceği konusunda benzer yaklaşımlar sergilemektedir. Raporlama ve belgelendirme, dijital delillerin adli mercilerde kullanılabilirliği açısından büyük bir öneme sahiptir çünkü bu süreçler delillerin bütünlüğünü ve doğruluğunu ortaya koymaktadır. Bu bağlamda uluslararası kabul gören ISO/IEC 27042 standardı, dijital delillerin analiz sürecinde nasıl raporlanacağına dair rehberlik sunmaktadır.

Bu standart, delillerin incelenmesi sırasında yapılan her bir adımın ayrıntılı olarak belgelenmesini ve nihai bulguların anlaşılır bir şekilde raporlanmasını gerektirmektedir. Raporlamada kullanılan yöntemler, analiz araçları ve süreçlerin sonuçları açıklanmaktadır. Bu süreç, dijital delillerin güvenilirliğini ve doğruluğunu doğrulamak için önemlidir. Toplama ve saklama süreçlerinin belgelendirilmesi bağlamında ISO/IEC 27037 standardı, delil toplama ve saklama süreçlerinin belgelenmesine ilişkin ayrıntılı hükümler içermektedir [1]. Tüm bunlarla beraber delillerin nasıl

toplandığı, hangi araçların kullanıldığı ve delillerin saklandığı süreçlerin tümü eksiksiz bir şekilde belgelenmelidir. Bu belgelendirme, delil zincirinin korunmasını sağlamak ve delillerin herhangi bir aşamada manipüle edilmediğini ispatlamak için kritik bir rol oynamaktadır. Genel olarak Türkiye’de adli bilişim süreçlerinde kullanılan raporlama ve belgelendirme standartları, büyük ölçüde uluslararası normlarla uyumludur. Dijital delillerin toplanması, incelenmesi ve mahkemelerde kullanılmasına yönelik süreçlerin belgelendirilmesi, hem yerel yasal düzenlemeler hem de Türkiye’deki teknik standartlar çerçevesinde yapılmaktadır.

Ceza Muhakemesi Kanunu (CMK) gibi yasal düzenlemeler, delillerin toplanması ve raporlanmasına ilişkin yükümlülükler getirirken, TS 13571 gibi yerel standartlar ise adli bilişim süreçlerinin belgelenmesine ilişkin spesifik düzenlemeler sunmaktadır. Türkiye’de uygulanan TS 13571 standardı, dijital delillerin adli süreçlerde kullanılabilirliğini sağlamak amacıyla raporlama ve belgelendirme süreçlerine ilişkin hükümler sunmaktadır. Bu standart, dijital delillerin nasıl toplandığı, hangi yöntemlerle analiz edildiği ve bu süreçlerin nasıl belgelendirileceği konusunda kapsamlı bir yol haritası sunmaktadır. Türkiye’deki adli bilişim uzmanları, raporlama ve belgelendirme aşamalarında bu standardı takip etmektedir. Türkiye’de dijital delillerin toplanması ve kullanılması süreçlerinde 5271 sayılı Ceza Muhakemesi Kanunu (CMK) önemli bir rol oynamaktadır [2]. CMK, adli süreçlerde kullanılacak delillerin nasıl toplanacağı ve raporlanacağı konusunda belirli yükümlülükler getirmektedir. Özellikle delillerin mahkemelerde kabul edilebilmesi için bu delillerin toplanma ve inceleme süreçlerinin eksiksiz bir şekilde belgelenmesi ve raporlanması gerekmektedir. Tüm bunlarla beraber hem uluslararası standartlar hem de Türkiye’deki düzenlemeler, adli bilişim süreçlerinin şeffaf ve detaylı bir şekilde raporlanmasını zorunlu kılmaktadır.

Kullanılan analiz araçları, teknik yöntemler ve elde edilen bulgular raporlanmalıdır. Bu raporlar, adli bilişim uzmanlarının mahkemelerde delillerin güvenilirliğini savunabilmesi için gerekli belgeleri sağlamaktadır. Raporlama ve belgelendirme, dijital delillerin adli süreçlerde geçerliliğinin sağlanmasında kritik bir aşamadır [3]. Hem uluslararası standartlar hem de Türkiye’de uygulanan düzenlemeler, adli bilişim süreçlerinde kullanılan yöntemlerin ve delil zincirinin eksiksiz bir şekilde raporlanmasını ve belgelenmesini zorunlu kılmaktadır.

5.1.3. Veri Bütünlüğü ve Güvenliği

Adli bilişim süreçlerinde veri bütünlüğü ve güvenliği, dijital delillerin güvenilirliğini ve mahkemelerde kabul edilebilirliğini sağlamak açısından hayati bir öneme sahiptir. Hem uluslararası standartlar hem de Türkiye’de uygulanan adli bilişim standartları, dijital delillerin bütünlüğünün korunması ve güvenliğinin sağlanması konusunda benzer ilkeler ve prosedürler benimsemiştir. Dijital delillerin toplanması, saklanması ve incelenmesi aşamalarında verilerin bozulmadan korunması ve yetkisiz erişimlere karşı güvenliğinin sağlanması, adli bilişim süreçlerinin temel

gerekliliklerindendir [4]. Uluslararası standartlar, dijital delillerin bütünlüğünü ve güvenliğini korumak amacıyla belirli prosedürler sunmaktadır. Bu prosedürler, dijital delillerin toplanması sırasında veri bütünlüğünün korunmasını ve delillerin güvenli ortamlarda saklanmasını sağlamaktadır. Uluslararası ISO/IEC 27037 standardı, dijital delillerin toplandığı andan itibaren bütünlüğünün korunması gerektiğini vurgulamaktadır. Bu standart, verilerin değiştirilmediğini veya manipüle edilmediğini ispatlamak için hash algoritmalarının kullanılmasını önermektedir.

Hash değeri, verinin orijinal haliyle korunmasını sağlar ve her türlü değişikliğin tespit edilmesine olanak tanımaktadır. Delillerin doğrulanabilir olması için hash değerlerinin toplama sürecinden itibaren kaydedilmesi ve analiz sürecine kadar saklanması zorunludur. ISO/IEC 27001 standardı, dijital sistemlerde kullanılan verilerin güvenliğini sağlamak için bilgi güvenliği yönetim sistemlerini düzenlemektedir [5]. Bu standart, dijital delillerin toplanması, saklanması ve paylaşılması süreçlerinde güvenliğin nasıl sağlanacağını belirlemektedir. ISO/IEC 27001, dijital delillerin fiziksel güvenliği, erişim kontrolü ve verilerin şifrelenmesi gibi güvenlik önlemlerini içermektedir. Bu önlemler, delillerin yetkisiz erişimlere karşı korunmasını ve bütünlüğünün bozulmamasını sağlamaktadır.

Türkiye’de dijital delillerin toplanması ve güvenliğinin sağlanması süreçleri, uluslararası standartlara büyük ölçüde paralellik göstermektedir. Türkiye’de uygulanan TS 13571 ve Ceza Muhakemesi Kanunu (CMK) gibi düzenlemeler, veri bütünlüğü ve güvenliği konularında belirli prosedürler ve yükümlülükler getirmiştir. Bu düzenlemeler, dijital delillerin güvenilir bir şekilde korunmasını ve mahkemelerde kabul edilebilmesini sağlamak amacıyla geliştirilmiştir [6]. Tüm bunlarla beraber Türkiye’de uygulanan TS 13571 standardı, dijital delillerin bütünlüğünü koruma ve güvenliğini sağlama konusunda uluslararası normlarla uyumlu düzenlemeler sunmaktadır. Bu standart, delillerin toplanması sırasında hash algoritmalarının kullanılmasını ve delillerin güvenli ortamlarda saklanmasını önermektedir. Ayrıca bu standart, dijital delillerin fiziksel güvenliğinin de sağlanması gerektiğini vurgulamaktadır [7]. Delillerin saklandığı ortamlara yalnızca yetkili kişilerin erişebilmesi ve verilerin bozulmaması için gerekli güvenlik önlemleri alınmalıdır.

Türkiye’de adli bilişim süreçlerinde veri güvenliğini sağlama konusunda 5271 sayılı Ceza Muhakemesi Kanunu (CMK) önemli bir rol oynamaktadır. CMK, dijital delillerin nasıl toplanacağı ve saklanacağı konusunda hukuki yükümlülükler getirmektedir. Bu kapsamda, dijital delillerin toplanması sürecinde yetkili mercilerin belirlediği yöntemler kullanılmakta ve delillerin güvenliğini sağlamak için fiziksel ve dijital güvenlik önlemleri alınmaktadır. CMK, dijital delillerin güvenliği ve mahkemelerde geçerliliği açısından önemli bir hukuki çerçeve sunmaktadır.

Dijital delillerin güvenliği, hem uluslararası hem de Türkiye’deki uygulamalarda fiziksel ve dijital güvenlik önlemleriyle sağlanmaktadır. Delillerin saklandığı ortamların güvenliği sağlanmalı, yetkisiz erişimler engellenmeli ve verilerin bozulmaması için güvenlik protokolleri uygulanmalıdır. Hem uluslararası hem de Türkiye’deki standartlar, bu önlemlerin alınmasını zorunlu kılar.

Uluslararası standartlar ve Türkiye’deki düzenlemeler, dijital delillerin toplanması ve saklanması süreçlerinde yetkisiz erişimlerin engellenmesini temel bir gereklilik olarak kabul etmektedir. Bu süreçte sadece yetkili kişilerin delillere erişebilmesi sağlanmalı ve verilerin manipüle edilmesi önlenmelidir [8]. Veri bütünlüğü ve güvenliği, dijital delillerin toplanması, saklanması ve incelenmesi süreçlerinde hem uluslararası standartlar hem de Türkiye’de uygulanan düzenlemelerde temel bir gereklilik olarak kabul edilmektedir. Hash algoritmalarının kullanımı, fiziksel ve dijital güvenlik önlemleri ve yetkisiz erişimlerin engellenmesi gibi uygulamalar, dijital delillerin güvenilirliğini ve adli süreçlerde kabul edilebilirliğini sağlamaya yönelik ortak özelliklerdir. Bu standartlar, adli bilişim uzmanlarının dijital delillerin bütünlüğünü koruyarak güvenli bir şekilde muhafaza etmelerini ve mahkemelerde kullanmalarını mümkün kılmaktadır.

5.2. Farklılıklar

Adli bilişim süreçlerinde uluslararası standartlar ile Türkiye’de uygulanan standartlar arasında pek çok ortak nokta bulunmasına rağmen, belirli farklılıklar da gözlemlenmektedir. Bu farklılıklar, genellikle her ülkenin yasal düzenlemeleri, adli bilişim alanındaki deneyimleri ve uluslararası işbirliği düzeyine bağlı olarak şekillenmektedir [9]. Uluslararası standartlar, daha geniş kapsamlı ve küresel düzeyde uyumluluğu hedefleyen bir çerçeve sunarken Türkiye’de uygulanan standartlar, yerel yasal düzenlemelere ve ülkenin ihtiyaçlarına yönelik belirli düzenlemeler içermektedir. Bu farklılıklar, Türkiye’deki adli bilişim uygulamalarının uluslararası standartlarla tam uyumlu olmasına engel teşkil etmemekle birlikte yerel düzenlemeler ve uygulamalardaki farklılıklar göz önünde bulundurulmalıdır. Uluslararası adli bilişim standartları, farklı ülkelerin hukuk sistemlerine uyum sağlayacak şekilde esnek bir yapıya sahipken Türkiye’deki adli bilişim süreçleri, yerel yasal düzenlemelere daha sıkı bir şekilde bağlıdır.

Türkiye’de dijital delillerin toplanması, saklanması ve analiz edilmesi süreçleri, özellikle Ceza Muhakemesi Kanunu (CMK) ve diğer yerel kanunlar tarafından sıkı bir şekilde düzenlenmiştir. Uluslararası standartlar (ISO/IEC serileri gibi), dijital delillerin toplanması ve işlenmesi süreçlerinde genel kabul görmüş en iyi uygulamaları ve teknik standartları sunmakta fakat bu standartlar, her ülkenin hukuki yapısına tam uyumlu olacak şekilde detaylandırılmamıştır [10]. Bunun yerine, ülkelerin kendi yasal çerçeveleriyle entegre olabilecek esnek bir yapıdadır. Türkiye’de dijital delillerin toplanması ve kullanılması süreçlerinde Ceza Muhakemesi Kanunu (CMK) gibi belirli yasalar ve yönetmelikler doğrultusunda hareket edilmesi zorunludur. Türkiye’de dijital delil toplama süreçleri, CMK’nın belirlediği şartlara uygun olarak yürütülmek zorundadır. Bu durum, Türkiye’deki adli bilişim uygulamalarının uluslararası standartlardan ayrıldığı temel noktalardan biridir. Özellikle mahkemelerde kullanılacak delillerin elde edilmesi, uluslararası standartlardan daha fazla hukuki kontrol ve belgelendirme gerektirebilmektedir.

5.2.1. Mevzuat ve Yasal Çerçeve Farklılıkları

Adli bilişim süreçlerinde uluslararası standartlar ile Türkiye’de uygulanan düzenlemeler arasında en önemli farklılıklardan biri mevzuat ve yasal çerçeveye ilişkindir. Her ülke, kendi hukuk sistemine ve ulusal gereksinimlerine göre dijital delil toplama, saklama ve analiz süreçlerine dair yasal düzenlemeler geliştirmiştir. Uluslararası standartlar, farklı ülkelerde uyarlanabilir esnek bir çerçeve sunarken, Türkiye’de uygulanan yasal çerçeve, daha katı ve yerel hukuka uygun şekildedir. Türkiye’de dijital delillerin toplanması ve kullanılması süreçleri, özellikle Ceza Muhakemesi Kanunu (CMK) gibi kanunlar tarafından detaylı bir şekilde düzenlenmiştir [11]. Bu düzenlemeler, Türkiye’deki adli bilişim uygulamalarıyla uluslararası standartlar arasındaki farklılıkların temel kaynaklarından biridir. Uluslararası adli bilişim standartları, ülkeler arası uyumu kolaylaştırmak ve dijital delil yönetimini küresel düzeyde düzenlemek amacıyla geliştirilmiştir. Bu standartlar, farklı ülkelerin hukuk sistemlerine adapte edilebilecek esneklikte genel kuralları sunmaktadır. Örneğin ISO/IEC 27037 ve ISO/IEC 27042 gibi standartlar, dijital delillerin nasıl toplanması, korunması ve analiz edilmesi gerektiğine dair en iyi uygulamaları belirlemekte fakat bu standartlar, ulusal yasalarla birebir örtüşmez ve her ülkenin kendi yasal sistemine göre uyarlanması gerekmektedir. Türkiye’de dijital delil toplama ve kullanımı süreçleri, ulusal mevzuat tarafından sıkı bir şekilde düzenlenmiştir. Özellikle 5271 sayılı Ceza Muhakemesi Kanunu (CMK), adli süreçlerde dijital delillerin nasıl toplanacağı, saklanacağı ve kullanılacağı konusunda belirli kuralları koymaktadır. Türkiye’de dijital delillerin hukuka uygun olarak elde edilmesi, bu delillerin mahkemelerde geçerli olabilmesi için kritik bir öneme sahiptir. CMK’ya göre hukuka aykırı olarak elde edilen deliller, mahkemede geçerli sayılmamaktadır [12].

Türkiye’de dijital delillerin toplanması ve kullanılması, CMK’da yer alan belirli prosedürlere bağlıdır. Örneğin dijital delil toplama işlemlerinin adli bir karar doğrultusunda yapılması ve delilin bütünlüğünün korunması zorunludur. Delil toplama sırasında izinsiz müdahale veya yetkisiz erişim, delilin hukuka aykırı sayılmasına neden olabilmektedir. Bu durum, uluslararası standartlardan farklı olarak Türkiye’de daha sıkı bir denetim gerektiren bir yasal çerçeve oluşturmaktadır. Türkiye’de kolluk kuvvetleri, adli bilişim süreçlerinde dijital delil toplama yetkisine sahip olmakla birlikte, bu süreçlerin tamamı hukuka uygun şekilde yürütülmek zorundadır. Özellikle dijital cihazlara el konulması, sistemlerin incelemeye alınması ve verilerin kopyalanması gibi işlemler, yasal izinler doğrultusunda gerçekleştirilir. Bu süreçlerin her biri belgelenmeli ve delil zinciri eksiksiz şekilde korunmalıdır.

Türkiye’deki yasal çerçeve, uluslararası standartlara kıyasla daha sıkı bir denetim ve düzenleme mekanizması içermektedir. CMK, dijital delil toplama ve kullanma süreçlerinin her aşamasında yasal denetimi zorunlu kılmaktadır. Bu durum, dijital delillerin güvenilirliğini artırmak amacıyla yerel düzeyde daha fazla kontrol sağlamakta fakat bu yasal düzenlemeler uluslararası standartların esnek yapısına kıyasla daha katıdır ve dijital delil toplama süreçlerinde yerel prosedürlerin her

adımında izlenmesini gerektirmektedir [13]. Uluslararası standartlar, ülkeler arasında dijital delil paylaşımını kolaylaştırmak için esnek bir yapı sunsa da Türkiye’de uygulanan sıkı yasal düzenlemeler, bu süreçlerde zorluklara neden olabilmektedir. Örneğin uluslararası bir dijital delilin Türkiye’de mahkemede kullanılabilmesi için bu delilin Türkiye’deki yasal prosedürlere uygun şekilde toplanmış olması gerekebilir. Aksi takdirde delilin Türkiye’de geçerli sayılmama riski bulunmaktadır.

5.2.2. Süreçte Uygulama Farklılıkları

Adli bilişim süreçlerinde uluslararası standartlar ile Türkiye’de uygulanan yöntemler arasında belirgin uygulama farklılıkları bulunmaktadır. Bu farklılıklar, genellikle dijital delillerin toplanması, analiz edilmesi ve saklanması süreçlerinde kullanılan teknikler, araçlar ve prosedürlerin yerel gereksinimlere ve hukuki düzenlemelere uyarlanmasından kaynaklanır. Türkiye’deki adli bilişim uygulamaları, uluslararası standartlarla büyük ölçüde uyumlu olsa da bazı teknik ve operasyonel farklılıklar, yerel koşullar ve yasal gereksinimler doğrultusunda ortaya çıkmaktadır. Süreçteki bu uygulama farklılıkları, adli bilişim uzmanlarının kullandığı araçlar, teknolojik altyapı, analiz yöntemleri ve raporlama süreçleri üzerinde etkilidir [14]. Uluslararası standartlar ve Türkiye’deki adli bilişim uygulamaları arasında, dijital delillerin toplanma süreçlerinde bazı farklılıklar bulunmaktadır. Uluslararası standartlar (örneğin ISO/IEC 27037), dijital delil toplama sürecini genel geçer teknik ve yöntemlerle açıklarken Türkiye’de bu süreç daha çok yerel yasal düzenlemelere ve teknik imkânlarla göre uyarlanmıştır. Uluslararası standartlar, dijital delillerin hangi tekniklerle toplanacağına ve hangi araçların kullanılacağına dair geniş kapsamlı rehberler sunmaktadır [15].

6. ADLİ BİLİŞİM SÜREÇLERİNDE KARŞILAŞILAN ZORLUKLAR VE ÇÖZÜMLER

6.1. Teknik Zorluklar

Adli bilişim süreçlerinde karşılaşılan teknik zorluklar, özellikle dijital kanıtların toplanması, analiz edilmesi ve mahkemede delil olarak sunulması süreçlerinde yoğunlaşmaktadır. Teknolojik cihazlardaki verilerin güvenli ve doğru bir şekilde elde edilmesi, bu süreçlerin en kritik adımlarından biridir. Dijital delil elde etme sürecinde kullanılan yöntem ve araçların yetersizliği veya hızlı teknolojik gelişmelere ayak uyduramaması, kanıtların güvenilirliğini ve mahkemede kabul edilebilirliğini olumsuz yönde etkilemektedir [24]. Bu bağlamda teknik cihazların ve yazılımların hızla güncellenmesi gerekmektedir. Bunun yanı sıra dijital verilerin hacminin giderek artması, adli bilişim uzmanlarının büyük veri yönetimi sorunlarıyla başa çıkmasını zorunlu kılmaktadır. Özellikle büyük boyutlu veri setlerinin işlenmesi, analiz edilmesi ve arşivlenmesi süreci, hem zaman hem de kaynak bakımından önemli kısıtlamalar yaratmaktadır [25].

Büyük veri yönetimi ve analiz tekniklerinin yetersizliği, delillerin geçerliliğini tehdit etmekte ve süreçlerin uzamasına neden olmaktadır. Ayrıca siber güvenlik tehditleri, adli bilişim süreçlerinde karşılaşılan diğer bir önemli teknik zorluktur. Özellikle dijital delil toplama ve analiz aşamalarında verilerin bütünlüğünü ve güvenliğini sağlamak amacıyla ileri düzeyde şifreleme ve güvenlik önlemlerinin alınması gerekmektedir. Siber saldırılara karşı yeterli güvenlik önlemlerinin alınmaması durumunda, adli bilişim sürecindeki verilerin manipülasyon riski artmaktadır. Bu durum, delillerin güvenilirliğini ve geçerliliğini tehlikeye sokmaktadır. Veri kurtarma işlemlerinde kullanılan yazılımların ve donanımların sınırlı kapasitesi, ayrıca bir zorluk teşkil etmektedir [26]. Özellikle hasar görmüş veya silinmiş verilerin kurtarılması sürecinde kullanılan teknolojik araçların yeterliliği büyük önem arz etmektedir. Donanım ve yazılımın yetersiz kalması, kritik verilerin kurtarılamamasına veya yanlış kurtarılmasına yol açmaktadır. Son olarak uluslararası hukuka uygunluk açısından teknik standartların sağlanması gerekliliği de adli bilişim süreçlerinde karşılaşılan önemli bir teknik zorluk olarak karşımıza çıkmaktadır. Adli bilişimde kullanılan araçların ve yöntemlerin uluslararası geçerliliği olan teknik standartlara uygun olması gerekmekte fakat birçok ülkenin adli bilişim süreçlerinde kullanılan standartlar ve protokoller konusunda farklılıklar göstermesi, teknik süreçlerin evrensel bir doğruluk ve güvenilirlik standardına uyum sağlama ihtiyacını artırmaktadır. Bu uyum, ülkeler arası iş birliğinin sağlanmasında kritik bir önem taşımaktadır [27].

6.1.1. Veri Toplama Aşamasında Karşılaşılan Zorluklar

Veri toplama aşamasında karşılaşılan zorluklar, adli bilişim süreçlerinin en hassas ve kritik adımlarından biri olarak değerlendirilmektedir. Bu aşamada dijital cihazlardan kanıt niteliğindeki verilerin güvenli, eksiksiz ve değiştirilmemiş olarak elde edilmesi gerekmekte ama dijital kanıtların toplanması sırasında karşılaşılan bazı teknik engeller, bu sürecin sağlıklı bir şekilde yürütülmesini zorlaştırmaktadır. Öncelikle veri çeşitliliği ve kaynakların çokluğu, veri toplama aşamasında önemli bir zorluk teşkil etmektedir [28]. Dizüstü bilgisayarlar, cep telefonları, IoT cihazları ve bulut depolama hizmetleri gibi çok çeşitli kaynaklardan veri toplamak gerekmektedir. Her bir cihazın farklı işletim sistemi, dosya yapısı ve güvenlik protokolleri bulunmakta olup bu farklılıklar, veri toplama sürecini karmaşıklaştırmaktadır. Örneğin bir iOS cihazdan veri toplama işlemi ile bir android cihazdan veri toplama işlemi, kullanılan yöntemler ve araçlar açısından farklılık göstermektedir [29].

Yazma koruması, depolama biriminde yer alan verilerin değiştirilmemesini, üzerinde işlem yapılamaması ve yanlışlıkla silinmemesi gibi önlemler sağlar. Toplanan verilerin bütünlüğünü sağlamak adına kullanılan önemli bir tekniktir fakat bazı durumlarda bu koruma mekanizması, özellikle bazı donanım ve yazılım yapılandırmalarında, veri toplama sürecini zorlaştırmaktadır. Yazma koruması uygulanmadığında, elde edilen verilerin güvenilirliği tartışmalı hale gelmektedir. Bulut tabanlı depolama sistemlerinden veri toplama da ciddi teknik engellerle karşılaşılmasına neden olmaktadır. Bulut sistemlerde veri toplama, verinin coğrafi olarak farklı sunucularda depolanması ve bulut sağlayıcıların gizlilik protokolleri nedeniyle oldukça karmaşıktır [30]. Özellikle uluslararası sunucularda bulunan verilere erişim, farklı yasal düzenlemeler nedeniyle sınırlanmakta ve bu durum, adli bilişim uzmanlarının veri toplama sürecini geciktirmektedir. Veri şifreleme, veri toplama aşamasında karşılaşılan bir diğer büyük zorluk olarak öne çıkmaktadır. Şifrelenmiş verilere erişim sağlamak için özel şifre çözme yöntemleri uygulanmakta, ancak bu süreç oldukça zaman alıcı ve teknik olarak zorlu olmaktadır.

Güçlü şifreleme algoritmaları gizlilik, bütünlük, uyumluluk ve esneklik sağlayarak güven oluştururken veri çözme süreci uzayabilmekte ve bu durum, soruşturmanın süresini olumsuz etkilemektedir. Ek olarak bazı cihazlarda kullanılan güvenlik mekanizmaları, veri toplama sürecinde engel teşkil etmektedir. Örneğin biyometrik kilitler veya iki faktörlü kimlik doğrulama sistemleri, adli bilişim uzmanlarının veri toplama işlemini gerçekleştirmesini zorlaştırmaktadır. Bu tür güvenlik önlemleri aşılamadığında, kanıt elde etme süreci kesintiye uğramaktadır. Son olarak adli bilişim uzmanlarının, veri toplama sırasında verinin zaman damgası ve meta verilerini koruması gerekmektedir [31]. Dijital kanıtların bütünlüğü açısından kritik öneme sahip olan meta veriler, herhangi bir değişiklikten korunmak zorundadır ancak veri toplama sırasında meta verilerin yanlışlıkla değiştirilmesi veya zarar görmesi, delilin mahkemede kabul edilebilirliğini olumsuz etkilemektedir.

Veri toplama aşamasında karşılaşılan zorluklar, adli bilişim süreçlerinin doğruluğu ve güvenilirliği açısından büyük önem taşımaktadır. Dijital delillerin güvenli ve değişmez bir biçimde elde edilmesi, adli bilişim uzmanlarının temel hedeflerinden biridir ancak bu süreçte karşılaşılan teknik engeller, delillerin geçerliliğini tehdit edebilmektedir. Öncelikle cihaz çeşitliliği veri toplama aşamasında önemli bir zorluk oluşturmaktadır. Akıllı telefonlar, tabletler, bilgisayarlar, IoT cihazları, bulut depolama sistemleri gibi farklı cihaz ve platformlardan veri elde edilmesi gerekmektedir [32]. Her cihazın kendine özgü dosya yapısı, işletim sistemi ve güvenlik önlemleri bulunmakta olup, bu çeşitlilik, veri toplama süreçlerinin karmaşıklığını artırmaktadır. Örneğin iOS işletim sistemindeki güvenlik önlemleri Android veya Windows işletim sistemlerine göre farklılık göstermekte ve her bir cihaz için özel toplama yöntemlerinin geliştirilmesini zorunlu kılmaktadır. Bununla birlikte veri toplama sürecinde karşılaşılan en büyük sorunlardan biri, şifreleme ve güvenlik protokolleridir. Şifrelenmiş verilere erişim sağlamak amacıyla şifre çözme işlemleri yapılması gerekmektedir ancak bu süreç oldukça zaman alıcıdır ve ileri teknik bilgi gerektirmektedir. Özellikle güçlü şifreleme algoritmaları ile korunmuş cihazlarda veri çözme süreci, delil toplama işleminin hızını önemli ölçüde yavaşlatmaktadır [33].

Veri toplama aşamasında karşılaşılan bir diğer teknik zorluk ise, bulut tabanlı depolama sistemlerinden veri elde edilmesidir. Bulut depolama sistemleri, verilerin fiziksel cihazlarda değil, coğrafi olarak farklı konumlarda bulunan sunucularda saklanmasını sağlamaktadır. Bu durum, bulut verilerine erişimi kısıtlamakta ve farklı yasal düzenlemelere tabi ülkeler arasında veri paylaşımı sorunlarını gündeme getirmektedir. Örneğin Amerika Birleşik Devletleri'nde saklanan bir bulut verisine erişim, yerel düzenlemeler ve veri gizliliği yasaları nedeniyle kısıtlanmakta ve bu durum, adli bilişim uzmanlarının veri toplama sürecini geciktirmektedir [34]. Yazma koruma, delillerin bütünlüğünü korumak için kullanılan bir tekniktir ve toplanan verilerin hiçbir şekilde değişikliğe uğramamasını sağlamakta ama bazı donanım ve yazılım yapılandırmalarında yazma koruma mekanizmalarının uygulanması güçlük arz etmektedir. Yazma korumasının sağlanamaması durumunda, verilerde meydana gelebilecek değişiklikler, delillerin mahkemede kabul edilebilirliğini riske atmaktadır. Ayrıca veri toplama işlemi sırasında verilerin zaman damgaları ve meta verilerinin korunması gerekmektedir. Meta veriler, dijital verinin kimlik bilgilerini, oluşum tarihini ve değişiklik geçmişini içeren önemli bilgilerdir. Veri toplama sırasında meta verilerin korunamaması veya yanlışlıkla değiştirilmesi, delilin mahkemede kabul edilebilirliğini ve güvenilirliğini zayıflatmaktadır [35].

Son olarak büyük veri yönetimi de veri toplama aşamasında karşılaşılan önemli zorluklardan biridir. Büyük veri setlerinin işlenmesi ve analiz edilmesi süreçlerinde güçlü donanım altyapısı ve ileri analiz araçları gerekmekte ama veri toplama sürecinde kullanılan donanım ve yazılımlar çoğu zaman bu hacme uyum sağlayamamakta ve veri işleme sürecini yavaşlatmaktadır [36].

6.1.2. Veri Analizi ve Yorumlamada Yaşanan Sorunlar

Veri analizi ve yorumlama aşamasında yaşanan sorunlar, adli bilişim süreçlerinde güvenilir ve doğru sonuçlara ulaşmak için önemli engeller oluşturmaktadır. Bu aşamada elde edilen dijital verilerin anlamlandırılması, adli olayın aydınlatılması ve hukuki süreçlerde kullanılabilir hale getirilmesi açısından kritik rol oynamakta fakat veri analizi ve yorumlama sürecinde karşılaşılan bazı teknik ve metodolojik zorluklar, sürecin etkinliğini olumsuz etkilemektedir. Öncelikle dijital verilerin büyük hacmi, veri analizi sürecini zorlaştırmaktadır [37]. Büyük veri analizi, birçok farklı kaynaktan gelen büyük miktarda verinin işlenmesini gerektirmektedir. Bu nedenle, analiz sürecinde güçlü yazılım altyapıları ve ileri düzey veri işleme teknikleri kullanılması zorunlu hale gelmekte ama adli bilişim alanında kullanılan birçok analiz aracının büyük veri setlerine uyum sağlayamaması, analiz sürecinin yavaşlamasına ve sonuçların geç elde edilmesine yol açmaktadır. Özellikle makine öğrenimi algoritmaları ve yapay zekâ temelli analiz yöntemlerinin etkin kullanımı, büyük veri analizi sürecinin başarısı açısından kritik önem taşımaktadır [38].

Veri analizi sürecinde karşılaşılan bir diğer önemli sorun, farklı veri formatlarının analiz edilmesi gerekliliğidir. Dijital veriler çeşitli dosya formatlarında saklanmakta olup, her bir formatın kendine özgü bir yapısı ve okunma şekli bulunmaktadır. Örneğin cep telefonlarından elde edilen veriler, bilgisayar verilerine göre farklı formatlarda ve kodlamalarda olabilmekte, bu da verilerin doğru bir şekilde analiz edilmesini zorlaştırmaktadır. Veri formatlarının çeşitliliği, analiz sürecinde kullanılan yazılımların esnekliğini ve uyum kabiliyetini zorunlu kılmaktadır. Ayrıca verilerin bütünlüğünü koruyarak analiz yapma gerekliliği, önemli bir zorluk olarak öne çıkmaktadır. Veri analizi sırasında herhangi bir değişiklik veya veri kaybı yaşanması durumunda, elde edilen sonuçlar güvenilirliğini yitirmektedir [39]. Bu nedenle verilerin işlenmesi sırasında bütünlük kontrollerinin yapılması ve her adımın kayıt altına alınması zorunlu olmaktadır. Özellikle hash değerleri kullanılarak veri bütünlüğünün sağlanması, verinin geçerliliğini korumak adına kritik bir önlem olarak uygulanmaktadır. Veri analiz sürecinde yaşanan zorluklardan bir diğeri ise analiz edilen verilerin doğru yorumlanabilmesi için uzmanlık gerektirmesidir. Dijital veriler, adli bilişim uzmanları tarafından teknik bilgiler ışığında yorumlanmakta olup, yanlış veya eksik yorumlamalar sürecin bütünlüğünü tehlikeye atmaktadır [40].

Örneğin bir log kaydının incelenmesi sırasında tarihler, zaman damgaları ve kullanıcı kimlikleri gibi bilgilerin doğru bir şekilde analiz edilmemesi, olayın akışında hatalı çıkarımlara yol açabilmektedir. Bu nedenle veri analizinde çalışan kişilerin teknik uzmanlık seviyeleri, sürecin doğruluğu açısından önemli bir faktör olarak öne çıkmaktadır. Öte yandan veri analizi sürecinde kullanılan yazılımların ve araçların sınırlamaları, sürecin etkinliğini düşürmektedir.

Analiz araçlarının bazıları yalnızca belirli veri formatlarını işleyebilmekte ve karmaşık analiz tekniklerine uygun olmamaktadır. Bunun yanı sıra analiz sırasında kullanılacak olan araçların lisans sorunları da, veri analizi sürecinde karşılaşılan engellerden biridir [41].

Lisanslı ve yetkin yazılımlar kullanılmadığında analiz sürecinde doğruluğu düşük veya eksik sonuçlara ulaşılabilmektedir. Son olarak analiz edilen verilerin mahkemede delil olarak kabul edilebilmesi için uluslararası standartlara ve yasal düzenlemelere uygun olması gerekmekte ama farklı ülkelerin veri analizi süreçlerine dair farklı yasal düzenlemeleri bulunmakta olup bu durum adli bilişim uzmanlarının analiz sonuçlarını uyarlamasını zorlaştırmaktadır [42]. Özellikle, Avrupa Birliği'nin GDPR gibi veri gizliliği ve koruma yasaları, veri analizi sürecinde belirli sınırlandırmalar getirmekte olup bu sınırlamalar analiz edilen verilerin güvenliğini sağlama gerekliliği ile çatışmaktadır. Bu teknik ve yasal zorluklar, veri analizi ve yorumlama aşamasında karşılaşılan önemli sorunları oluşturmakta olup adli bilişim süreçlerinde doğru ve güvenilir sonuçlara ulaşılabilmesi için bu engellerin aşılması gerekmektedir [43].

6.2. Hukuki ve Etik Zorluklar

Adli bilişim süreçlerinde hukuki ve etik zorluklar, dijital kanıtların güvenli ve doğru bir şekilde toplanması, analiz edilmesi ve kullanılması için önemli bir engel teşkil etmektedir. Dijital delillerin elde edilmesi ve kullanılması, yalnızca teknik standartlara uygunluğu değil, aynı zamanda yasal düzenlemelere ve etik ilkelerle uyumlu olmayı gerektirmektedir. Bu bağlamda, farklı ülkelerin yasal çerçeveleri, veri gizliliği yasaları ve etik kurallar, adli bilişim uzmanlarının karşılaştığı zorlukları artırmaktadır. Öncelikle kişisel verilerin korunması ile ilgili yasal düzenlemeler, adli bilişim süreçlerinde önemli bir hukuki zorluk oluşturmaktadır [44]. Özellikle Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi veri gizliliği yasaları, bireylerin kişisel verilerinin korunmasını zorunlu kılmakta olup, dijital delil toplama süreçlerinde sınırlamalar getirmektedir.

KVKK, Dijital delillerin toplanması ve işlenmesi sırasında kişisel verilerin korunmasına yönelik Türkiye'deki düzenlemeleri içerirken GDPR, verilerin rıza olmadan toplanmasını veya işlenmesini kısıtlamakta ve bu durum, adli bilişim uzmanlarının veri toplama işlemlerini etkileyebilmektedir. Örneğin kişisel bilgilerin bulunduğu bir cep telefonundan veri toplama işlemi yapılırken, bu verilerin yetkisiz kişiler tarafından incelenmesi veya paylaşılması yasal olarak suç teşkil edebilmektedir [45]. Ayrıca adli bilişim süreçlerinde kullanılan dijital delillerin mahkemede kabul edilebilirliği, hukuki bir sorun olarak öne çıkmaktadır.

Dijital delillerin yasal süreçlerde delil olarak kullanılabilmesi için, verilerin toplanma ve analiz edilme yöntemlerinin belirli standartlara uygun olması gerekmekte ama farklı ülkelerdeki adli bilişim standartları arasında uyumsuzluklar bulunmakta olup, bu durum, uluslararası davalarda dijital delillerin geçerliliği konusunda sorun yaratmaktadır [46].

Etik açıdan ise adli bilişim uzmanlarının, topladıkları verilerin gizliliğini koruma yükümlülükleri bulunmaktadır. Adli bilişim süreçlerinde elde edilen dijital veriler, bireylerin özel yaşamlarına dair hassas bilgiler içerebilmekte olup bu bilgilerin korunması etik bir zorunluluk olarak öne

çıkılmaktadır. Verilerin yetkisiz kişilerle paylaşılması veya üçüncü taraflarla izinsiz olarak aktarılması, etik açıdan kabul edilemez olmakta ve adli sürecin tarafsızlığını zedelemektedir. Adli bilişim uzmanlarının, veri toplama ve analiz sürecinde etik ilkeleri gözetmesi, bu bilgileri yalnızca yetkili kişilerin erişimine sunması gerekmektedir. Öte yandan, dijital delillerin elde edilmesi sürecinde bireylerin mahremiyet hakları da ciddi bir etik zorluk olarak görülmektedir [47].

Özellikle cep telefonu, bilgisayar gibi kişisel cihazlardan veri toplama işlemi yapılırken, bu cihazlarda bulunan özel bilgilere erişim, bireylerin mahremiyet haklarını ihlal edebilmektedir. Mahremiyet ihlallerinin önlenmesi adına, adli bilişim uzmanlarının yalnızca soruşturma kapsamında gerekli olan bilgilere erişmesi ve diğer bilgileri göz ardı etmesi gerekmektedir. Bu durum, özellikle kişisel mahremiyetin korunması açısından etik bir sorumluluk oluşturmaktadır. Buna ek olarak adli bilişim uzmanlarının etik davranış ilkelerine bağlı kalması, tarafsızlık ilkesine uygun olarak hareket etmesi gerekmektedir [24]. Adli bilişim sürecinde elde edilen bulguların tarafsız bir şekilde sunulması, adaletin sağlanması açısından büyük önem taşımakta ama bazı durumlarda adli bilişim uzmanları üzerinde baskı kurulmakta ve elde edilen bulguların belirli bir tarafın lehine sunulması talep edilmektedir. Bu tür baskılara direnmek, etik ilkeler doğrultusunda hareket etmek, adli bilişim uzmanlarının sorumlulukları arasında yer almaktadır. Son olarak dijital delillerin yasal olarak tanımlanmış süreler içinde saklanması ve muhafaza edilmesi gerekliliği, hukuki bir zorluk olarak ortaya çıkmaktadır [25]. Özellikle delil olarak kullanılan dijital verilerin saklanma süresi ve güvenliği, hukuki süreçlerin sürdürülebilirliği açısından önem arz etmekte ama bazı durumlarda delillerin saklanması için gerekli olan fiziksel ve dijital altyapının yetersiz olması, bu sürecin etkinliğini düşürmektedir. Dijital verilerin güvenli bir ortamda ve belirli yasal süreler dâhilinde saklanmaması, delilin geçerliliğini tehlikeye atmakta ve hukuki süreçlerin olumsuz etkilenmesine yol açmaktadır [26].

6.2.1. Gizlilik ve Veri Güvenliği İkilemleri

Genel olarak gizlilik ve veri güvenliği ikilemleri, adli bilişim süreçlerinin en karmaşık ve dikkat gerektiren yönlerinden biridir. Dijital delillerin toplanması, analiz edilmesi ve saklanması aşamalarında, elde edilen verilerin gizliliğini koruma zorunluluğu ile verilerin güvenli bir şekilde muhafaza edilmesi gerekliliği arasında bir denge sağlanması gerekmektedir.

Özellikle bireylerin özel hayatına dair hassas bilgiler içeren dijital veriler, hem yasal gereklilikler hem de etik sorumluluklar doğrultusunda dikkatle işlenmektedir. Öncelikle veri gizliliği konusundaki yasal düzenlemeler, adli bilişim süreçlerinde uyulması zorunlu bir çerçeve oluşturmaktadır [27]. Özellikle Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve Amerika Birleşik Devletleri'nde yürürlükte olan çeşitli veri gizliliği yasaları, bireylerin kişisel verilerinin korunmasını amaçlamakta olup, adli bilişim uzmanlarının bu düzenlemelere uymasını zorunlu kılmaktadır.

GDPR kapsamında kişisel verilerin yalnızca belirli bir amaç doğrultusunda işlenmesi, verilerin güvenliğinin sağlanması ve gerektiğinde anonimleştirilmesi gerekmekte ama dijital delil olarak kullanılan verilerin anonimleştirilmesi veya erişimin kısıtlanması, adli süreçlerde bu verilerin etkin bir şekilde kullanılmasını zorlaştırmaktadır. Bir diğer önemli ikilem, verilerin güvenli bir şekilde saklanması ve işlenmesi gerekliliğidir [28]. Adli bilişim süreçlerinde elde edilen dijital veriler, kanıt bütünlüğünü sağlamak amacıyla çeşitli güvenlik önlemleri ile korunmaktadır. Bu süreçte yazma koruma teknikleri, hash algoritmaları ve güvenli depolama yöntemleri kullanılmakta olup verilerin herhangi bir şekilde değiştirilmesini veya zarar görmesini engellemek için gelişmiş güvenlik önlemleri uygulanmaktadır. Ama verilerin güvenli bir ortamda saklanması sırasında uygulanan bu önlemler, veri gizliliği ile çelişebilmekte ve bu verilerin yalnızca ilgili yetkililer tarafından erişilebilir hale getirilmesi gerekmektedir. Örneğin bir soruşturma kapsamında toplanan kişisel verilere yalnızca belirli adli bilişim uzmanlarının veya yetkili makamların erişim iznine sahip olması gerekmektedir [29].

Adli bilişim süreçlerinde sıklıkla karşılaşılan bir diğer gizlilik ve veri güvenliği ikilemi, bulut depolama sistemlerinden veri elde edilmesi sürecinde ortaya çıkmaktadır. Bulut depolama hizmetlerinden toplanan veriler, genellikle farklı coğrafi bölgelerde bulunan sunucularda saklanmakta ve bu verilerin güvenliğine dair farklı ülkelerin yasal düzenlemeleri devreye girmektedir [30]. Bu durumda adli bilişim uzmanlarının bulut sistemlerinden topladığı verilerin hem ilgili ülkenin veri gizliliği yasalarına hem de soruşturma kapsamında belirlenen güvenlik önlemlerine uygun olması gerekmekte ama uluslararası veri güvenliği ve gizliliği protokolleri arasında uyumsuzluklar bulunmakta olup, bu durum adli bilişim süreçlerinde uyulması gereken gizlilik standartlarını zorlaştırmaktadır. Özellikle cep telefonları, bilgisayarlar ve diğer kişisel cihazlarda saklanan dijital veriler, çoğu zaman bireylerin özel hayatına dair hassas bilgiler içermekte olup bu bilgilerin toplanması ve analiz edilmesi sırasında gizliliğin korunması gerekmektedir [31].

Bu durumda adli bilişim uzmanları, gizlilik ilkelerine uygun hareket etmekle yükümlü olmasına rağmen verilerin güvenli bir şekilde elde edilmesi gerekliliği ile bireylerin mahremiyet hakları arasında bir denge kurmak zorundadır. Ayrıca adli bilişim süreçlerinde elde edilen verilerin uzun süreli saklanması ihtiyacı da gizlilik ve veri güvenliği ikilemine yol açmaktadır. Soruşturma sürecinin tamamlanmasının ardından, delil olarak kullanılan dijital verilerin belirli bir süre daha saklanması gerekmektedir [32].

Verilerin uzun süreli saklanması sırasında, gizlilik ihlallerinin yaşanmaması ve bu verilerin yetkisiz kişilerce erişilmemesi için güvenlik önlemlerinin sürekli olarak güncellenmesi gerekmektedir. Bu çerçevede gizlilik ve veri güvenliği ikilemleri, adli bilişim süreçlerinde dengeli bir şekilde ele alınması gereken önemli bir zorluk olarak öne çıkmaktadır. Bu ikilemler, adli bilişim uzmanlarının

hem yasal düzenlemelere uygun hareket etmesini hem de etik sorumluluklarını yerine getirmesini zorunlu kılmakta ve dijital delil yönetimi süreçlerinin güvenilirliğini doğrudan etkilemektedir [33].

6.2.2. Yasal Düzenlemelerdeki Sorunlar

Yasal düzenlemelerdeki sorunlar, adli bilişim süreçlerinin hem ulusal hem de uluslararası düzeyde tutarlılıkla yürütülmesi açısından önemli engeller oluşturmaktadır. Adli bilişim alanında yasal düzenlemelerin belirli bir standarda oturtulamaması, dijital kanıtların toplanması, analiz edilmesi ve mahkemelerde delil olarak sunulmasında hukuki uyumsuzluklara yol açmaktadır. Özellikle ülkeler arasında farklılık gösteren veri koruma yasaları ve dijital delil yönetimi standartları, adli bilişim süreçlerinin etkinliğini olumsuz etkilemektedir [34]. Öncelikle kişisel verilerin korunmasıyla ilgili yasal düzenlemeler, adli bilişim süreçlerinde uyulması zorunlu olan önemli bir yasal çerçeve sunmaktadır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemeler, bireylerin kişisel verilerinin korunmasını zorunlu kılmakta ve bu doğrultuda adli bilişim süreçlerinde kısıtlamalar getirmektedir. GDPR kapsamında, kişisel verilerin yalnızca belirli yasal gerekçelerle işlenmesi ve üçüncü şahıslarla paylaşılmadan önce bireylerin rızasının alınması gerekmektedir.

Bir diğer sorun, dijital delillerin mahkemelerde kabul edilebilirliğiyle ilgilidir. Farklı ülkelerde dijital delillerin nasıl toplanması ve saklanması gerektiğine dair belirli standartlar bulunmakta olup, bu standartlar arasındaki farklılıklar, uluslararası davalarda delillerin geçerliliğini tehlikeye sokmaktadır. Örneğin Amerika Birleşik Devletleri'nde dijital delillerin kabul edilebilirliğini düzenleyen Federal Rules of Evidence, delillerin güvenilir ve doğrulanabilir olmasını şart koşmaktadır [35]. Buna karşın bazı Avrupa ülkelerinde daha farklı prosedürler izlenmektedir. Bu farklılıklar, uluslararası iş birliği gerektiren davalarda adli bilişim uzmanlarının topladığı delillerin bir ülkede geçerli sayılırken başka bir ülkede kabul edilmemesi gibi durumlara yol açmaktadır.

Ayrıca dijital delillerin toplanması ve saklanmasına dair teknik standartların eksikliği, adli bilişim süreçlerinde önemli bir sorun olarak öne çıkmaktadır. Dijital delillerin güvenilirliği ve geçerliliği için belirli teknik standartlara uyulması gerekmektedir ancak bu konuda uluslararası alanda kabul görmüş standartların olmaması, her ülkenin kendi adli bilişim prosedürlerini oluşturmaya yol açmaktadır [36].

Bu durum, dijital kanıtların uluslararası geçerliliğini zayıflatmakta ve özellikle sınır ötesi suçların soruşturulmasında delillerin kabul edilmesi konusunda sorunlar yaratmaktadır. Örneğin bazı ülkeler, dijital delil toplama sürecinde belirli sertifikalı yazılımların kullanılmasını zorunlu kılmakta, diğerleri ise böyle bir zorunluluk getirmemektedir. Bu çeşitlilik, dijital delillerin mahkemede kabul edilebilirliği açısından belirsizlik yaratmaktadır. Bulut bilişim ve uzaktan veri depolama sistemleri de yasal düzenlemelerle ilgili sorunları artırmaktadır. Bulut depolama

hizmetlerinden veri toplama sırasında, verilerin saklandığı sunucuların farklı ülkelerde bulunması nedeniyle yargı yetkisi sorunları ortaya çıkmaktadır [37].

Özellikle farklı ülkelerde bulunan bulut hizmeti sağlayıcından bir soruşturma için veri talep edilmesi, ilgili ülkeler arasındaki veri gizliliği yasalarının çatışmasına neden olmaktadır. Bu tür durumlarda ülkeler arasındaki yasal uyumsuzluklar nedeniyle veriye erişim sınırlanmakta veya tamamen engellenmektedir. Ayrıca dijital delillerin saklanma süresi ve güvenliği konusunda net yasal düzenlemelerin olmaması, delillerin güvenilirliğini tehdit eden bir başka önemli sorundur. Delillerin belirli bir süre boyunca güvenli bir şekilde saklanması gerektiği bilinmekte ancak bu süreye dair yasal düzenlemeler ülkeden ülkeye değişiklik göstermektedir. Bazı ülkeler dijital delillerin uzun süreli saklanmasını zorunlu kılarken diğerleri daha kısa süreli saklama politikaları uygulamaktadır. Bu durum, özellikle uzun süren davalarda delil güvenliğini tehlikeye atmakta ve soruşturma sürecinde delillerin eksilmesine neden olmaktadır [38]. Son olarak dijital delil toplama süreçlerinde gizlilik ve veri koruma yasalarının katı bir şekilde uygulanması, adli bilişim uzmanlarının işini zorlaştırmaktadır. Bireylerin özel hayatına dair hassas verilerin toplanması sırasında, bu verilerin yalnızca belirli yasal çerçevede kullanılabilmesi gerekmekte ancak özellikle terörizm, organize suçlar veya uluslararası suçlar gibi ciddi davalarda bu sınırlamalar, soruşturmanın etkinliğini azaltmaktadır. Adli bilişim uzmanlarının yasal düzenlemeler ile soruşturma gereklilikleri arasında denge kurma zorunluluğu, süreçlerin etkinliğini olumsuz etkilemektedir [39].

7. ADLİ BİLİŞİMDE TEKNOLOJİK GELİŞMELER VE GELECEK YÖNELİMLERİ

7.1. Makine Öğrenimi Uygulamaları

Adli bilişimde makine öğrenimi uygulamaları, veri analiz süreçlerini hızlandırmak, doğruluğu artırmak ve elde edilen bulguların güvenilirliğini sağlamak açısından büyük bir potansiyele sahip bulunmaktadır. Makine öğrenimi, özellikle büyük veri analizlerinde, karmaşık veri setlerinin işlenmesinde ve dijital delillerin sınıflandırılmasında etkili bir araç olarak kullanılmaktadır. Adli bilişim alanında kullanılan makine öğrenimi modelleri, çeşitli veri kaynaklarından gelen bilgileri analiz ederek suç eğilimlerini, anomali tespitini ve veri ilişkilerini yüksek doğrulukla belirlemekte ve bu sayede adli olayların çözümüne katkı sağlamaktadır [40].

Günümüzde dijital deliller çok büyük hacimlerde toplanmakta olup, bu veri yığınlarının manuel olarak analiz edilmesi oldukça zaman alıcı ve hata yapma ihtimali yüksek bir süreç olarak değerlendirilmektedir. Makine öğrenimi algoritmaları, bu veri yığınlarını hızlı bir şekilde taramakta ve önemli bilgileri öne çıkararak analiz sürecini hızlandırmaktadır. Örneğin doğal dil işleme teknikleri, e-posta, mesaj veya sosyal medya verileri gibi metin tabanlı verilerin analizinde kullanılmakta ve adli bilişim uzmanlarının suça ilgili kritik bilgilere daha hızlı ulaşmasını sağlamaktadır [41]. Anomali tespiti de makine öğreniminin adli bilişimdeki önemli uygulama alanlarından biridir. Anomali tespiti algoritmaları, büyük veri setlerindeki olağandışı davranışları veya örüntüleri belirleyerek olası suç faaliyetlerinin tespit edilmesine yardımcı olmaktadır. Örneğin bir ağ trafiği analizinde normal kullanıcı davranışlarından sapmalar tespit edilerek potansiyel bir siber saldırı veya veri ihlali belirlenebilmektedir. Bu tür makine öğrenimi tabanlı anomali tespit sistemleri, özellikle siber güvenlik olaylarında erken uyarı sistemi olarak kullanılmakta ve adli bilişim uzmanlarının hızlı aksiyon almasına olanak tanımaktadır [42].

Makine öğrenimi aynı zamanda yüz tanıma ve görüntü işleme uygulamalarında da adli bilişim süreçlerine katkı sağlamaktadır. Yüz tanıma algoritmaları, suça ilişkili görüntülerin ve videoların analiz edilmesinde kullanılmakta, kayıp veya şüpheli kişilerin tespit edilmesini kolaylaştırmaktadır. Derin öğrenme modelleri, özellikle çok büyük görsel veri setlerinde yüksek doğrulukla yüz tanıma işlemi gerçekleştirmekte ve adli vakalarda delil elde etme sürecini hızlandırmaktadır. Örneğin güvenlik kameralarından alınan görüntülerde belirli bir kişiyi arama sürecinde, makine öğrenimi algoritmaları kısa sürede kapsamlı tarama yapabilmekte ve istenilen özelliklere sahip kişileri belirleyebilmektedir. Öte yandan makine öğrenimi uygulamaları, dijital delillerin sınıflandırılması ve ilişkilendirilmesi süreçlerinde de kullanılmaktadır [43].

Farklı kaynaklardan gelen dijital veriler, makine öğrenimi algoritmaları sayesinde kategorize edilmekte ve suça bağlantılı ilişkiler kurularak analiz edilmektedir. Bu sınıflandırma işlemi, büyük

miktarda veriyi düzenli hale getirerek, adli bilişim uzmanlarının daha anlamlı sonuçlara ulaşmasını sağlamaktadır.

Makine öğrenimi, ayrıca siber suçlarla mücadelede önemli bir yere sahip olmaktadır. Siber suç vakalarında, özellikle zararlı yazılımların ve kötü amaçlı yazılım hareketlerinin tespiti için makine öğrenimi tabanlı analiz yöntemleri kullanılmaktadır. Makine öğrenimi algoritmaları, zararlı yazılım davranışlarını tanımlamakta ve saldırıların önceden belirlenmesine yardımcı olmaktadır. Bu yöntemler sayesinde zararlı yazılımlar bilinmeyen sistemlere bulaşmadan önce tespit edilmekte ve güvenlik tehditlerine karşı hızlı çözümler sunulmaktadır [44]. Son olarak adli bilişimde makine öğrenimi kullanımı, otomatik raporlama ve öngörü analitiği alanlarında da etkili olmaktadır. Makine öğrenimi algoritmaları, dijital delillerin analizinden elde edilen bulguları otomatik olarak raporlayabilmekte ve gelecekte benzer suç olaylarının meydana gelme olasılığını öngörmekte kullanılmaktadır. Öngörü analitiği, suç profillemesi ve risk değerlendirmesi gibi alanlarda karar vericilere değerli bilgiler sağlamak ve olayların önlenmesi konusunda adli bilişim süreçlerine katkı sunmaktadır. Bu kapsamda makine öğrenimi uygulamaları adli bilişimde süreçleri hızlandırmak, doğruluğu artırmak ve büyük veri yönetimini kolaylaştırmak amacıyla kullanılmakta olup gelecekte bu teknolojilerin daha gelişmiş seviyelere ulaşması beklenmektedir [45].

7.1.1. Delil İnceleme Sistemleri

Delil inceleme sistemleri, adli bilişimde dijital kanıtların hızlı, güvenilir ve doğrulanabilir bir şekilde analiz edilmesi için kullanılan kritik araçlardır. Dijital delillerin incelenmesi ve sınıflandırılması sürecinde bu sistemlerin rolü, özellikle büyük hacimli veri setlerinin analiz edilmesi gerektiğinde ön plana çıkmaktadır. Delil inceleme sistemleri, farklı veri türlerini organize ederek, analiz sürecini kolaylaştırmakta ve adli bilişim uzmanlarına hızlı sonuçlar sunmaktadır. Öncelikle delil inceleme sistemlerinin temel işlevlerinden biri, verilerin güvenli bir şekilde toplanması ve incelenmesi sürecini otomatikleştirmektir. Bu sistemler, adli bilişim uzmanlarının verileri toplarken karşılaştığı yazma koruma gerekliliklerini dikkate almakta ve verilerin bütünlüğünü koruyarak analiz sürecine entegre etmektedir. Örneğin hash algoritmalarını kullanarak elde edilen verilerin özgünlüğü doğrulanmakta ve kanıtların herhangi bir değişikliğe uğramadığından emin olunmaktadır. Bu özellik, dijital kanıtların mahkemede kabul edilebilirliğini artıran önemli bir faktör olarak öne çıkmaktadır [46]. Delil inceleme sistemleri aynı zamanda farklı formatlarda kaydedilmiş veri türlerinin analiz edilmesini sağlayan araçlar sunmaktadır. Günümüzde dijital deliller, e-posta yazışmaları, sosyal medya verileri, cep telefonu kayıtları, ağ trafiği gibi çok çeşitli kaynaklardan elde edilmektedir.

Bu çeşitlilik, delil inceleme sistemlerinin farklı veri formatlarını işleyebilmesi gerekliliğini ortaya çıkarmaktadır. Örneğin bazı sistemler metin analizi ve doğal dil işleme özellikleri sunarak e-posta veya mesaj gibi metin tabanlı verileri analiz edebilmekte ve suçla ilişkili önemli bilgileri öne

çıkarabilmektedir. Bu özellikler, delillerin hızlı bir şekilde analiz edilmesini sağlamak ve önemli ipuçlarının tespit edilmesine katkıda bulunmaktadır. Bir diğer önemli özellik, delil inceleme sistemlerinin anomali tespiti ve veri madenciliği tekniklerini entegre etmesidir [47]. Anomali tespit algoritmaları, özellikle büyük veri setlerinde normal olmayan davranışları veya örüntüleri belirleyebilmekte ve bu sayede olası suç faaliyetlerinin daha hızlı bir şekilde tespit edilmesine olanak tanımaktadır. Bu tür algoritmalar, özellikle siber güvenlik olaylarında saldırıların önceden tespit edilmesini sağlamak ve veri ihlali olaylarına karşı hızlı müdahale imkânı tanımaktadır.

Delil inceleme sistemleri ayrıca otomatik sınıflandırma ve ilişkilendirme özellikleri sunarak verilerin anlamlandırılmasını kolaylaştırmaktadır. Bu sistemler, elde edilen delilleri farklı kategorilere ayırarak ve ilişkili veriler arasında bağlantılar kurarak adli bilişim uzmanlarının olayın yapısını daha net bir şekilde görmesini sağlamaktadır. Örneğin finansal dolandırıcılık davalarında farklı hesap hareketleri ve işlem örüntüleri arasında bağlantılar kurularak, suçun kapsamı ve failer arasındaki ilişkiler belirlenebilmektedir. Bu özellik, büyük veri yığınlarını düzenli hale getirerek daha anlamlı analizler yapılmasına olanak tanımaktadır. Bu sistemler, makine öğrenimi algoritmalarını kullanarak benzer suç kalıplarını tanımlamakta ve geçmiş vakalarla kıyaslama yaparak adli bilişim uzmanlarına öneriler sunmaktadır. Örneğin sahtecilik veya kimlik hırsızlığı gibi tekrarlayan suç örüntüleri tespit edilerek mevcut soruşturma kapsamında benzer davranışların olup olmadığı hızlı bir şekilde belirlenmektedir [24].

Bu tür özellikler, suç profillemesi ve öngörü analitiği açısından değerli bilgiler sunmakta ve adli süreçlerde karar vericilere rehberlik etmektedir. Son olarak delil inceleme sistemleri, analiz edilen verilerin otomatik olarak raporlanmasını ve mahkemede delil olarak sunulabilecek şekilde formatlanmasını sağlamaktadır. Bu sistemler, adli bilişim uzmanlarının analiz sürecinde elde ettiği bulguları detaylandırarak ve ilgili kanıtlarla destekleyerek, hukuki süreçlerde kullanılmaya uygun raporlar oluşturmaktadır [25]. Otomatik raporlama özelliği, özellikle büyük hacimli verilerin işlendiği durumlarda zaman kazandırmakta ve analiz sürecini daha verimli hale getirmektedir. Bu kapsamda delil inceleme sistemleri, adli bilişimde teknolojik gelişmelerin önemli bir parçası olarak kullanılmakta olup dijital kanıtların güvenilirliğini, geçerliliğini ve analiz sürecinin hızını artırmaktadır.

7.1.2. Suç Analizinde Veri Madenciliği

Suç analizinde veri madenciliği, büyük ve karmaşık veri kümelerinden anlamlı bilgiler elde etmeye yönelik gelişmiş yöntemlerin kullanılması ile suçun yapısını, suçlular arasındaki ilişkileri ve olası suç eğilimlerini ortaya çıkarmak amacıyla adli bilişim süreçlerinde önemli bir rol oynamaktadır. Veri madenciliği, adli bilişim uzmanlarına farklı veri kaynaklarından elde edilen bilgileri analiz etme ve suç faaliyetlerini daha derinlemesine anlama imkânı sunmaktadır. Veri madenciliği teknikleri, suç analizinde özellikle örüntü tanıma ve anomali tespiti süreçlerinde kullanılmaktadır.

Suçlular arasında tekrarlayan hareketler, işlem kalıpları ve diğer benzer davranışlar, veri madenciliği algoritmaları sayesinde tespit edilmekte ve suç ağları oluşturulmaktadır [26]. Örneğin finansal dolandırıcılık vakalarında benzer para transferi örüntüleri analiz edilerek, suçlular arasındaki finansal bağlantılar belirlenmekte ve dolandırıcılık şemaları ortaya çıkarılmaktadır. Bu tür bağlantılar, suç örgütlerinin faaliyetlerini ve yapılarını çözmek için değerli bilgiler sağlamaktadır.

Veri madenciliği, suç analizinde kümelenme teknikleri ile de önemli katkılar sunmaktadır. Kümelenme teknikleri, benzer özelliklere sahip veri noktalarını bir araya getirerek suçla ilgili farklı gruplar ve ilişki ağları oluşturmaktadır. Özellikle organize suç şebekelerinde, suçlular arasındaki iletişim ve işlem örüntüleri kümelenerek analiz edilmekte ve gruplar arasındaki ilişkiler daha net bir şekilde ortaya konmaktadır. Örneğin uyuşturucu ticareti şebekelerinde farklı coğrafi bölgelerde faaliyet gösteren grupların arasındaki iletişim ve işlem kayıtları kümelenerek ağın yapısı ve suç zincirindeki bağlantılar belirlenmektedir [27]. Suç analizinde kullanılan bir diğer veri madenciliği tekniği olan sınıflandırma algoritmaları, suçun türünü belirleme ve olayın muhtemel sonucunu tahmin etme açısından kullanılmaktadır. Sınıflandırma teknikleri, mevcut verilerden yola çıkarak yeni vakaları sınıflandırmakta ve olası suç eğilimlerini ortaya koymaktadır. Örneğin çeşitli suç kayıtlarından oluşan bir veri setinde olayın türüne göre (hırsızlık, dolandırıcılık, siber saldırı gibi) sınıflandırma yapılmakta ve benzer özelliklere sahip yeni olaylar da aynı sınıfa atanarak suç türü hakkında hızlı bir ön bilgi elde edilmektedir. Bu tür sınıflandırmalar, suça müdahale stratejilerinin geliştirilmesi için önemli bir rehber olmaktadır [28].

Veri madenciliği ayrıca sosyal ağ analizi ile suçlular arasındaki ilişkilerin görselleştirilmesi ve anlaşılmasında etkili olmaktadır. Sosyal ağ analizi teknikleri, bireyler arasındaki bağlantıları, iletişim kayıtlarını ve işlem ağlarını analiz ederek suç örgütlerinin yapısını ve operasyonlarını açığa çıkarmaktadır. Örneğin bir suç örgütüne bağlı kişilerin telefon görüşmeleri ve mesajlaşma verileri analiz edilerek suç ağının liderleri, üyeleri ve alt grupları belirlenmektedir [29].

Bu sayede suç örgütünün yapısı daha net bir şekilde anlaşılakta ve suçun çözülmesine yönelik stratejiler geliştirilmesine katkı sağlanmaktadır. Suç analizinde veri madenciliği tekniklerinin kullanılmasının bir diğer önemli yönü, tahmine dayalı analiz yetenekleridir. Tahmine dayalı analiz, geçmiş suç kayıtları ve olaylarla ilgili verilerden yola çıkarak gelecekte benzer suçların nerede ve ne zaman gerçekleşebileceği hakkında öngörüler sunmaktadır [30].

Bu tür analizler, özellikle büyük şehirlerdeki suç oranlarını düşürmek için suçun olasılıkla gerçekleşeceği bölgelerin belirlenmesinde kullanılmaktadır. Örneğin bir şehirde belirli bir bölgede sık sık hırsızlık olaylarının yaşanması durumunda tahmine dayalı analiz algoritmaları bu bölgelerde gelecekte benzer olayların yaşanabileceğini öngörerek emniyet güçlerinin bu bölgelerde önlem almasını sağlamaktadır. Ayrıca veri madenciliği teknikleri sayesinde siber suç analizleri daha kapsamlı bir şekilde yapılmaktadır. Siber suçlarda özellikle zararlı yazılım hareketleri, IP adresleri

ve şüpheli ağ trafiği gibi veriler analiz edilerek siber saldırı örüntüleri ve suçlular arasındaki ilişkiler belirlenmektedir.

Bu tür analizler, siber güvenlik olaylarına erken müdahale edilmesini sağlamak ve veri ihlallerine karşı koruyucu önlemler alınmasına olanak tanımaktadır. Son olarak suç analizinde veri madenciliği, otomatik raporlama sistemleri ile de entegre edilerek elde edilen bulguların görsel raporlarla desteklenmesini sağlamaktadır [31]. Bu raporlar, suç eğilimleri, örüntüler ve suçlular arasındaki ilişkileri grafiksel olarak sunmakta ve karar vericilere olayın genel yapısı hakkında kapsamlı bir bilgi sağlamaktadır. Bu tür görsel raporlar, suç analiz süreçlerinde adli bilişim uzmanlarına ve kolluk kuvvetlerine etkili bir rehberlik sunmakta, olayın çözülme sürecini hızlandırmaktadır. Bu kapsamda suç analizinde veri madenciliği teknikleri, suçların daha iyi anlaşılması, çözülmesi ve gelecekte benzer olayların önlenmesi açısından kritik bir önem taşımakta olup, adli bilişim süreçlerinin vazgeçilmez bir bileşeni haline gelmektedir.

7.2. Blokzincir Teknolojisi ve Dijital Delillerin Güvenliği

Blokzincir teknolojisi, son yıllarda dijital delillerin güvenliğinin sağlanması ve delillerin manipülasyona karşı korunması amacıyla adli bilişim süreçlerinde dikkate alınan yenilikçi bir çözüm olarak öne çıkmaktadır. Blokzincir, verilerin dağıtık bir defterde kaydedilmesi ve güvenli bir şekilde saklanması için kriptografik algoritmalar kullanmaktadır [32]. Bu yapı, dijital delillerin zaman damgalama, değişmezlik ve şeffaflık gibi temel güvenlik özelliklerini sağlayarak adli bilişim süreçlerinde delil güvenliğini artırmaktadır. Öncelikle blokzincirin merkezi olmayan yapısı, dijital delillerin güvenliğini sağlamak açısından önemli bir avantaj sunmaktadır. Blokzincir teknolojisi, verilerin tek bir merkezi otorite yerine, dağıtık bir ağda birçok düğüm üzerinde saklanmasını sağlamaktadır. Bu yapı, dijital delillerin bir merkezi sunucuda toplanması ve depolanması riskini ortadan kaldırmakta, böylece verilerin manipülasyon veya izinsiz erişim girişimlerine karşı daha dayanıklı hale gelmesini sağlamaktadır [33].

Blokzincir teknolojisi, dijital delillerin güvenilirliğini artırmak amacıyla zaman damgalama özelliğini sunmaktadır. Zaman damgalama, bir dijital delilin belirli bir tarihte var olduğunu ve herhangi bir değişiklik yapılmadığını kanıtlamak için kullanılmaktadır. Blokzincirin kriptografik yapısı sayesinde her bir işlem bir önceki işlemle zincirleme olarak bağlanmakta ve tüm işlemler geri dönülemez bir şekilde kayıt altına alınmaktadır. Bu özellik, delillerin herhangi bir noktada değiştirildiğinde bunu tespit etmeyi mümkün kılmaktadır [33]. Örneğin bir delilin toplandığı an kaydedilerek blok zincirine işlenmekte ve daha sonraki bir tarihte bu delilde değişiklik yapılması durumunda, zincirdeki değişiklik izi kolayca fark edilebilmektedir. Bununla birlikte blokzincir teknolojisi, dijital delillerin bütünlüğünü sağlamak için hash fonksiyonları kullanmaktadır. Hash fonksiyonları, verinin benzersiz bir dijital parmak izini oluşturarak, verinin bütünlüğünü korumaktadır.

Herhangi bir deęişiklik yapıldığında verinin hash deęeri deęiőeęinden dijital delilin geęerlilięi zedelenmiő olmaktadır. Blockchain üzerinde saklanan dijital delillerin hash deęerleri, delilin orijinal halini doęrulamak için kullanılmakta ve delilin bozulmadan saklanması saęlamaktadır. Örneęin bir dijital delilin toplandıęı anda hash deęeri hesaplanmakta ve blockchain aęına kaydedilmektedir. Daha sonra delilin bütünlüęünü doęrulamak isteyen adli biliőim uzmanları, bu hash deęerini karőılaőtırarak delilin güvenirlięini test edebilmektedir [34]. Ayrıca blokzincir teknolojisi adli biliőim süreçlerinde őeffaflık ve izlenebilirlik saęlamaktadır. Blokzincir defterindeki her iőlem, daęıtık aędaki tüm katılımcılar tarafından görülebilmekte olup delillerin nereden geldięi, hangi aőamalardan geętięi ve kimler tarafından eriőildięi kaydedilmektedir. Bu őeffaflık, adli süreçlerde delilin nasıl elde edildięi ve iőlendięi konusunda tam bir izlenebilirlik saęlamakta ve delilin mahkemede kabul edilebilirlięini artırmaktadır [35].

Blokzincirin dijital delillerin güvenlięinde sunduęu bir dięer avantaj, yetkilendirme ve eriőim kontrolü saęlamasıdır. Blokzincir aęı üzerindeki dijital delillere yalnızca belirli yetkilere sahip kullanıcılar eriőim saęlayabilmekte olup bu eriőim yetkileri blokzincir protokolleri ile sınırlandırılmaktadır. Özellikle hassas verilerin korunması gereken durumlarda adli biliőim uzmanları blokzincir teknolojisini kullanarak dijital delillere kimlerin eriőebileceęini belirlemekte ve bu sayede delilin güvenlięini ve gizlilięini saęlamaktadır. Örneęin bir adli soruőturmada elde edilen dijital delillerin yalnızca yetkili adli personel tarafından görüntülenebilmesi için eriőim yetkileri blokzincir üzerinde kısıtlanmaktadır. Son olarak blokzincir teknolojisinin adli biliőimde uzun süreli veri saklama ihtiyacına çözüm sunduęu belirtilmelidir [36]. Blokzincir üzerinde kayıtlı veriler, deęiőtirilemez ve silinemez bir yapıya sahip olduęundan adli süreçlerde delillerin geęerlilięi uzun süre boyunca korunmaktadır. Örneęin bir mahkeme süreci tamamlandıktan sonra dahi, delilin orijinal hali blokzincir üzerinde saklanarak gerektięinde yeniden incelenebilmekte ve delilin zaman içinde güvenlięini yitirmemesi saęlanmaktadır.

Bu özellikleriyle blokzincir teknolojisi, dijital delillerin güvenli bir őekilde saklanmasını, doęrulanmasını ve izlenebilirlięini saęlamaktadır. Adli biliőim süreçlerinde blokzincirin yaygınlaőması, dijital kanıtların manipölasyona karőı korunmasına güvenirlięinin artırılmasına ve delil yönetim süreçlerinin etkinleőtirilmesine önemli katkılar sunmaktadır [37]. Geliően blokzincir teknolojisi ile adli biliőimde daha güvenilir ve őeffaf bir delil yönetimi saęlanması mümkün hale gelmektedir.

Blokzincir teknolojisinin benimsenmesi geleneksel sorunları geleneksel olmayan yöntemlerle çözmemizi saęlar. Ancak bunları yaparken beraberinde getirdięi riskler de mevcuttur. Daęıtılmıő kontrol yapısı ile sistemin anlık kapatılamaması veya baęlantının kesilememesi risk ortaya çıkarır. Aynı zamanda anonim ve deęiőilmez yapısı da her ne kadar avantaj saęlasa da oluőabilecek sıkıntılarda sorunların çözömlenmesi de zor olacaktır.

7.2.1. Blokzincir Tabanlı Kayıt Sistemleri

Blokzincir tabanlı kayıt sistemleri, dijital verilerin güvenilir ve değişmez bir şekilde kaydedilmesi için adli bilişimde giderek daha fazla kullanılmaktadır. Bu sistemler, delillerin güvenliğini sağlamak, izlenebilirliği artırmak ve verilerin manipülasyonunu engellemek amacıyla merkezi olmayan bir yapı kullanmakta olup her bir verinin doğrulanabilir şekilde saklanmasını mümkün kılmaktadır. Blokzincir teknolojisinin sunduğu şeffaflık, güvenlik ve değişmezlik özellikleri, dijital delil yönetimi açısından büyük avantaj sağlamaktadır [38]. Öncelikle blokzincir tabanlı kayıt sistemlerinin temel avantajlarından biri, her bir kaydın dağıtık bir ağ üzerinde, zincirleme bir yapıyla depolanmasıdır. Bu yapı, kaydedilen verilerin merkezi bir sunucuya bağımlı olmadan birden fazla düğümde saklanmasını sağlamakta ve herhangi bir düğüm üzerinde yapılacak bir değişikliğin diğer düğümler tarafından otomatik olarak reddedilmesine olanak tanımaktadır. Örneğin bir adli delilin blokzincir tabanlı bir kayıt sistemine eklenmesi durumunda, bu delil tüm ağda doğrulanmakta ve değiştirilemez bir şekilde kaydedilmektedir [39].

Blokzincir tabanlı kayıt sistemleri, dijital delillerin zaman damgalama yöntemiyle kaydedilmesine olanak tanımaktadır. Zaman damgalama, delilin toplandığı veya işlendiği belirli bir tarihte var olduğunu kanıtlamak amacıyla kullanılan bir doğrulama yöntemidir. Blokzincir üzerinde bir delil kaydedildiğinde bu delil zincirin bir parçası haline gelmekte ve her bir blok bir önceki blokla ilişkili olduğundan delilin kaydedildiği tarih ve saat geri dönülemez bir şekilde kaydedilmektedir. Örneğin bir suç soruşturmasında elde edilen bir delilin blokzincir tabanlı bir kayıt sistemine eklendiği anda zaman damgalanması, delilin o tarihte var olduğunu kanıtlamakta ve ileride bu delil üzerinde yapılan herhangi bir değişikliğin fark edilmesini sağlamaktadır. Blokzincir tabanlı kayıt sistemleri, hash fonksiyonları kullanarak her bir kaydı benzersiz bir dijital imza ile saklamaktadır [40].

Hash fonksiyonları, verinin içeriğine göre benzersiz bir hash değeri oluşturarak verinin bütünlüğünü korumakta ve delilin değiştirilip değiştirilmediğini tespit etme olanağı sunmaktadır. Bu yöntem, dijital delilin saklandığı andaki durumunu korumakta ve herhangi bir değişiklik yapılması durumunda hash değerinin değişmesi sayesinde bu değişiklik kolayca fark edilebilmektedir. Örneğin bir dijital belgenin hash değeri, belgenin blokzincire kaydedildiği anda hesaplanmakta ve bu değer daha sonra karşılaştırılarak belgenin orijinal olup olmadığı kontrol edilmektedir.

Adli bilişim süreçlerinde blokzincir tabanlı kayıt sistemlerinin sağladığı en büyük avantajlardan biri de izlenebilirliktir. Blokzincir teknolojisi, her bir işlemi ağdaki tüm katılımcıların görebileceği bir şekilde kaydetmekte olup bu sayede delilin hangi adımlardan geçtiği, kimler tarafından işlendiği veya kimlerin erişim sağladığı net bir şekilde takip edilebilmektedir [41]. Bu özellik, adli süreçlerde delilin doğrulanabilirliğini artırmakta ve delilin kaynağına dair tüm işlemleri gözler önüne sermektedir. Örneğin bir dijital delil blokzincir üzerinde saklandığında, bu delile hangi yetkililerin

ne zaman erişim sağladığı ve hangi işlemlerden geçtiği detaylı bir şekilde kaydedilmekte, bu da adli sürecin güvenilirliğini desteklemektedir.

Blokzincir ağlarında her bir kullanıcıya belirli roller ve yetkiler atanabilmekte ve hassas verilere erişim bu yetkilere göre sınırlanabilmektedir. Örneğin bir dijital delilin sadece adli bilişim uzmanları ve belirli yasal yetkililer tarafından incelenmesi gerekiyorsa blokzincir üzerinde bu kişilere özel erişim izinleri atanmakta ve bu sayede delilin yetkisiz kişiler tarafından görüntülenmesi engellenmektedir. Son olarak blokzincir tabanlı kayıt sistemleri, adli bilişimde uzun süreli veri saklama ihtiyacına çözüm sunmaktadır [42]. Dijital delillerin güvenli bir ortamda uzun süre boyunca saklanması gerekmekte olup, blokzincir teknolojisi bu konuda sağlam bir altyapı sağlamaktadır. Blokzincir üzerindeki kayıtlar değiştirilemez ve silinemez olduğundan adli süreçlerde delillerin geçerliliği ve güvenilirliği uzun yıllar boyunca korunmakta, gerektiğinde delilin orijinal haline erişim sağlanmaktadır. Örneğin bir mahkeme sürecinde kullanılan bir dijital delilin, gelecekte aynı delile ihtiyaç duyulması durumunda blokzincir kayıtları üzerinden güvenilir bir şekilde doğrulanması mümkün olmaktadır [43].

7.3. Bulut Bilişim ve Uzaktan Erişim Çözümleri

Bulut bilişim ve uzaktan erişim çözümleri, adli bilişim süreçlerinde dijital delillerin güvenli bir şekilde saklanması, işlenmesi ve paylaşılmasında önemli bir rol oynamaktadır. Bulut bilişim teknolojileri, büyük veri setlerinin işlenmesini kolaylaştırmakta, delillerin farklı konumlarda bulunan adli uzmanlar arasında hızlı bir şekilde paylaşılmasını sağlamaktadır. Özellikle geniş çaplı soruşturmalarda, verilerin hızlıca erişilebilir olması ve uzaktan analiz edilebilmesi, delil toplama ve analiz süreçlerini hızlandırmakta ve verimliliği artırmaktadır. Öncelikle bulut bilişim teknolojisi sayesinde büyük hacimli dijital veriler güvenli bir şekilde depolanabilmektedir [44].

Dijital delillerin fiziksel cihazlarda saklanması, veri kaybı ve güvenlik riskleri açısından çeşitli zorluklar yaratmakta ancak bulut depolama, verilerin merkezi olmayan sunucularda güvenli bir şekilde saklanmasına olanak tanımakta ve veri yedekleme çözümleri ile delillerin bütünlüğünü korumaktadır. Örneğin bir soruşturma kapsamında toplanan büyük boyutlu video kayıtları veya ağ trafiği verileri, bulut üzerinde depolanmakta ve bu sayede verilerin kaybolma riski azaltılmaktadır [45].

Bulut bilişim, adli bilişim uzmanlarına uzaktan erişim imkânı sunarak, delillere her yerden ve her cihazdan güvenli bir şekilde ulaşılmasını sağlamaktadır. Bu özellik, farklı konumlarda bulunan adli uzmanların iş birliği içinde çalışmasına olanak tanımakta ve özellikle uluslararası soruşturmalarda önemli bir avantaj sağlamaktadır. Örneğin bir ülkenin farklı şehirlerinde veya farklı ülkelerde bulunan uzmanlar, bulut tabanlı bir platform üzerinden delillere aynı anda erişebilmekte ve uzaktan analiz gerçekleştirebilmektedir. Bu durum, adli süreçlerde zaman tasarrufu sağlamak ve operasyonel verimliliği artırmaktadır. Bulut bilişimde kullanılan erişim kontrol mekanizmaları,

dijital delillerin güvenliğini sağlamak için geliştirilmiştir [46]. Bulut tabanlı sistemlerde erişim, kimlik doğrulama ve yetkilendirme yöntemleriyle güvence altına alınmakta olup, yalnızca belirli yetkilere sahip kullanıcıların veriye erişmesi sağlanmaktadır. İki faktörlü kimlik doğrulama, şifreleme ve rol tabanlı erişim kontrolü gibi yöntemler, bulut bilişimde delil güvenliğini artırmaktadır. Örneğin hassas bir soruşturma verisine yalnızca yetkili adli bilişim uzmanlarının erişmesine izin verilmekte ve bu veriye yetkisiz kişilerin ulaşması engellenmektedir.

Bulut bilişim çözümleri, adli bilişimde büyük veri analiz süreçlerini de hızlandırmaktadır. Büyük veri setlerinin analiz edilmesi, özellikle siber suç soruşturmalarında önemli bir ihtiyaçtır. Bulut tabanlı analitik platformlar, büyük veri setlerini hızlıca işleyebilmekte ve çeşitli makine öğrenimi algoritmaları ile suç eğilimlerini, örüntüleri ve anormallikleri belirlemektedir [47]. Örneğin büyük bir ağ trafiği analizinde, bulut tabanlı bir sistem üzerinden veriler işlenmekte ve anomali tespit algoritmaları kullanılarak potansiyel tehditler hızla tespit edilmektedir. Bu özellik, siber suçların önceden belirlenmesi ve hızlı müdahale edilmesi açısından kritik bir avantaj sağlamaktadır. Dijital delillerin fiziksel cihazlarda saklanması durumunda, cihaz arızaları, doğal afetler veya siber saldırılar sonucu veri kaybı riski bulunmakta ancak bulut bilişim, verilerin otomatik olarak yedeklenmesini sağlayarak veri kaybı durumunda yedeklerin kullanılmasına olanak tanımaktadır. Örneğin bir adli soruşturma sırasında toplanan deliller, bulut üzerinde yedeklenmekte ve olası bir veri kaybı durumunda deliller hızla geri yüklenmektedir. Bunun yanı sıra bulut bilişim çözümleri esneklik ve ölçeklenebilirlik avantajı sunmaktadır [24].

Bulut bilişim, bu veri artışını kolaylıkla yönetebilmekte ve gerektiğinde depolama kapasitesini artırabilmektedir. Örneğin kapsamlı bir soruşturmada toplanan delil miktarı arttığında bulut bilişim altyapısı, kapasiteyi hızla artırarak bu verilerin güvenli bir şekilde saklanmasını sağlamaktadır. Bu esneklik, adli süreçlerde verilerin verimli bir şekilde yönetilmesine ve daha büyük soruşturmanın rahatlıkla yürütülmesine imkân tanımaktadır. Verilerin bulut üzerinde güvenli bir şekilde saklanması için çeşitli şifreleme algoritmaları kullanılmakta olup yalnızca yetkili kullanıcıların veriye erişebilmesi sağlanmaktadır. Bu sayede dijital delillerin saklandığı bulut ortamında izinsiz erişim riskleri minimize edilmektedir [25].

7.3.1. Bulutta Veri Depolama ve Adli Analiz

Bulutta veri depolama ve adli analiz, adli bilişim süreçlerinde dijital delillerin güvenli bir şekilde saklanması ve büyük veri kümelerinin etkin bir biçimde analiz edilmesi açısından önemli avantajlar sunmaktadır. Dijital delillerin fiziksel cihazlarda saklanması ve işlenmesi, veri güvenliği, erişilebilirlik ve depolama kapasitesi açısından sınırlamalar yaratabilmekte fakat bulut bilişim, bu sınırlamaları ortadan kaldırarak, büyük miktarda veriyi güvenli bir ortamda depolamayı ve analiz etmeyi mümkün kılmaktadır [26]. Özellikle geniş çaplı soruşturmalarda bulut bilişimin sağladığı yüksek depolama kapasitesi ve güçlü analiz araçları, adli sürecin hızlandırılmasına katkı

sağlamaktadır. Bulut tabanlı veri depolama, adli bilişim uzmanlarına büyük veri setlerini güvenli bir şekilde saklama olanağı tanımaktadır. Geleneksel fiziksel depolama yöntemleri, veri kaybı riski, cihaz arızaları ve güvenlik açıkları gibi sorunlara karşı savunmasız kalabilmekte fakat bulut bilişimde veriler merkezi olmayan bir altyapıda, birden fazla sunucuya dağıtılarak yedeklenmekte ve veri kaybı riskine karşı korunmaktadır. Örneğin bir adli soruşturma sırasında toplanan dijital deliller, bulut üzerinde yedeklenmekte ve bu verilerin güvenli bir şekilde saklanması sağlanmaktadır [27].

Bu yedekleme süreci, delillerin kaybolma riskini azaltmakta ve uzun süre güvenli bir ortamda muhafaza edilmesine imkân tanımaktadır. Bulutta veri depolama, adli analiz süreçlerinde uzaktan erişim ve iş birliği imkânlarını da artırmaktadır. Farklı konumlarda bulunan adli bilişim uzmanları, bulut tabanlı depolama sayesinde aynı verilere eşzamanlı olarak erişebilmekte ve uzaktan analiz yapabilmektedir. Özellikle uluslararası soruşturmalarda, farklı ülkelerde bulunan uzmanlar arasında bulut tabanlı platformlar aracılığıyla veri paylaşımı yapılabilmekte ve iş birliği kolaylaşmaktadır. Örneğin, bir siber suç soruşturmasında farklı ülkelerdeki adli bilişim uzmanları, bulut tabanlı bir platform üzerinden suçla ilgili verileri paylaşmakta ve bu veriler üzerinde eşzamanlı analiz gerçekleştirmektedir. Bu durum, delil toplama ve analiz süreçlerinde hız kazandırmakta ve operasyonel verimliliği artırmaktadır [28].

Bulutta veri depolama ayrıca, adli analiz süreçlerinde yüksek işlem kapasitesi sunmaktadır. Büyük veri setlerinin analiz edilmesi, özellikle siber suç ve dolandırıcılık gibi karmaşık olaylarda büyük öneme sahiptir. Bulut tabanlı platformlar, yüksek işlem gücü ve depolama kapasitesi sağlayarak büyük veri setlerinin hızlı bir şekilde analiz edilmesini sağlamaktadır. Bir ağ trafiği analizinde milyonlarca veri kaydının işlenmesi gerektiğinde, bulut tabanlı bir sistem büyük veri kümelerini hızlıca işleyerek anomali tespit algoritmaları ile olağandışı durumları belirlemektedir. Bu sayede siber saldırı veya veri ihlali gibi olaylar hızlı bir şekilde tespit edilmekte ve adli bilişim uzmanlarının olaylara daha çabuk müdahale etmesi mümkün hale gelmektedir [29]. Bulut tabanlı platformlar, makine öğrenimi algoritmalarını büyük veri analiz süreçlerine entegre ederek, suç örüntülerini ve eğilimleri belirlemekte ve tahmine dayalı analizler gerçekleştirmektedir.

Örneğin, finansal dolandırıcılık vakalarında bulut tabanlı makine öğrenimi algoritmaları, çeşitli işlem örüntülerini analiz ederek dolandırıcılık şemalarını ve şüpheli işlem hareketlerini belirleyebilmektedir. Bu sayede adli bilişim uzmanları hızlı ve doğru sonuçlara ulaşmaktadır. Bu tür analiz araçları, suç profillemesi ve risk değerlendirmesi gibi alanlarda da değerli bilgiler sağlamaktadır [30]. Bulut tabanlı veri depolama ve adli analiz çözümleri, güçlü güvenlik önlemleri ile verilerin gizliliğini ve bütünlüğünü sağlamaktadır. Erişim kontrol mekanizmaları, şifreleme yöntemleri ve kimlik doğrulama araçları, bulut ortamında depolanan verilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlamak ve verinin izinsiz erişime karşı korunmasını temin etmektedir. Örneğin iki faktörlü kimlik doğrulama ve şifreleme gibi yöntemlerle, hassas verilerin

güvenliği sağlanmakta ve adli süreçlerde gizlilik ihlalleri önlenmektedir. Bu güvenlik önlemleri, bulutta depolanan dijital delillerin güvenilirliğini artırmakta ve adli süreçlerde kullanılabilirliğini sağlamaktadır.

Dijital delillerin saklandığı bulut ortamında veriler düzenli olarak yedeklenmekte olup, olası veri kayıplarında veriler hızla geri yüklenebilmektedir. Bu durum, adli süreçlerin aksamadan devam etmesini sağlamak ve delillerin her zaman erişilebilir olmasını temin etmektedir [31]. Örneğin, bir sunucu arızası veya doğal afet durumunda bulut üzerinde yedeklenen veriler, hızla başka bir sunucuya aktarılmakta ve adli bilişim uzmanları veriye yeniden erişim sağlayabilmektedir. Bu özellikleri ile bulutta veri depolama ve adli analiz, dijital delil yönetimi ve analiz süreçlerinde verimliliği artırmakta, büyük veri kümelerinin hızlı bir şekilde işlenmesini sağlamak ve güvenli bir çalışma ortamı sunmaktadır [32].

7.3.2. Güvenlik ve Erişim Kontrolü Zorlukları

Bulut bilişimde güvenlik ve erişim kontrolü, adli bilişim süreçlerinde dijital delillerin gizliliği, bütünlüğü ve güvenliğini sağlama açısından kritik bir rol oynamaktadır. Bulut tabanlı çözümler, adli bilişim uzmanlarının veriye uzaktan erişim sağlamasına olanak tanısa da bu avantajlar beraberinde çeşitli güvenlik ve erişim kontrolü zorluklarını getirmektedir.

Dijital delillerin korunması ve yalnızca yetkili kişiler tarafından erişilebilir olması, adli sürecin güvenilirliğini ve delillerin mahkemede kabul edilebilirliğini doğrudan etkilemektedir [33]. Öncelikle bulut bilişimde verilerin merkezi bir sunucu yerine dağıtık bir altyapıda depolanması, güvenlik ve erişim kontrolü zorluklarını artırmaktadır. Verilerin birçok farklı sunucuda saklanması, her sunucunun güvenlik açıklarına karşı korunmasını gerektirmekte olup herhangi bir sunucuda meydana gelecek güvenlik ihlali, tüm sistemin güvenliğini riske atabilmektedir. Örneğin dijital delillerin depolandığı bir sunucuya siber saldırı düzenlenmesi durumunda, delillerin güvenliği tehlikeye girebilmektedir.

Erişim kontrolü, bulut bilişimde güvenliğin en önemli unsurlarından biri olarak öne çıkmaktadır. Bulut sistemlerinde, delillere erişim izninin yalnızca yetkili kişilere verilmesi ve izinsiz erişimlerin engellenmesi gerekmekte fakat bulut tabanlı sistemlerde erişim kontrolü sağlamak, çok katmanlı kimlik doğrulama ve yetkilendirme süreçleri gerektirmekte ve bu süreçler, operasyonel karmaşıklığa yol açabilmektedir [34]. Örneğin, iki faktörlü kimlik doğrulama (2FA) ve rol tabanlı erişim kontrolü (RBAC) gibi güvenlik önlemleri, erişim kontrolü sağlamak için gerekli olsa da bu önlemler tüm kullanıcılar için uygun şekilde uygulanmadığında güvenlik açıkları oluşabilmektedir. Ayrıca büyük bir soruşturma kapsamında birçok uzmanın aynı verilere erişmesi gerektiğinde, kullanıcı yönetimi ve yetki sınırlandırması daha da karmaşık hale gelmektedir. Adli bilişimde bulut bilişim çözümlerinin kullanımı, veri şifreleme gerekliliğini de beraberinde getirmektedir. Dijital delillerin bulut ortamında depolanırken güvenliğinin sağlanması için güçlü

şifreleme algoritmalarının kullanılması gerekmektedir. Örneğin şifreleme anahtarlarının yönetimi ve saklanması, büyük bir güvenlik zorluğu oluşturmaktadır [35].

Şifreleme anahtarlarının güvenli bir şekilde yönetilmemesi durumunda, yetkisiz kişilerin şifreli verilere erişimi mümkün hale gelmekte ve delilin gizliliği tehlikeye düşmektedir. Bu nedenle adli bilişim uzmanlarının şifreleme anahtarlarını güvenli bir şekilde saklamak ve yalnızca yetkili kişilere erişim sağlamak için gelişmiş şifreleme anahtarı yönetim sistemleri kullanması gerekmektedir. Bulut bilişimde güvenlik ve erişim kontrolü zorluklarının bir diğer önemli boyutu, yasal ve uyumluluk sorunlarıdır. Farklı ülkelerdeki veri gizliliği yasaları ve düzenlemeler, bulut tabanlı verilerin güvenliğini sağlamada ek zorluklar yaratmaktadır [36]. Özellikle uluslararası soruşturmalarda, delillerin saklandığı sunucuların coğrafi konumu ve veri aktarımı ile ilgili yasal düzenlemelere uyum sağlanması gerekmektedir. Örneğin Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin yalnızca belirli yasal çerçeveler dahilinde işlenmesini ve güvenli bir şekilde saklanmasını zorunlu kılmakta ama GDPR ve diğer veri koruma yasalarına uyum sağlamak, farklı ülkelerden adli bilişim uzmanlarının bulut tabanlı verilere erişimini kısıtlayabilmektedir. Bu durum, adli bilişim süreçlerinde uluslararası iş birliğini zorlaştırmakta ve güvenlik önlemlerinin karmaşıklığını artırmaktadır [37].

Bulut bilişimde erişim kontrolü sağlarken karşılaşılan bir diğer zorluk, veri izleme ve denetim süreçleridir. Dijital delillere erişim sağlandığında, bu erişimlerin kimler tarafından ne zaman gerçekleştirildiği ve hangi işlemlerin yapıldığı kayıt altına alınmalıdır ama bulut sistemlerinde geniş kullanıcı erişimi olması durumunda, tüm erişimlerin izlenmesi ve denetlenmesi karmaşık bir süreç haline gelmektedir. Erişim izleme ve denetim eksiklikleri, veri manipülasyonu veya izinsiz erişim gibi güvenlik ihlallerinin zamanında tespit edilmesini zorlaştırmaktadır [38]. Bu nedenle adli bilişimde bulut tabanlı çözümler kullanılırken, dijital delillere yapılan tüm erişimlerin kaydedilmesi ve izlenmesi için kapsamlı bir denetim mekanizması geliştirilmesi gerekmektedir.

Son olarak bulut bilişimde güvenlik zorluklarından biri de veri yedekleme ve felaket kurtarma süreçleridir. Dijital delillerin kaybolması durumunda, bu verilerin hızlı bir şekilde geri yüklenmesi büyük önem taşımaktadır. Örneğin yedeklenmiş bir delile erişmek isteyen yetkisiz bir kullanıcının bu verilere ulaşması, delilin gizliliğini ve bütünlüğünü riske atmaktadır. Bu tür durumları önlemek amacıyla, bulut yedekleme sistemlerinde de aynı güvenlik önlemlerinin uygulanması gerekmektedir. Bu güvenlik ve erişim kontrolü zorlukları, adli bilişim süreçlerinde bulut bilişim kullanımını güvenli hale getirmek için kapsamlı güvenlik stratejileri ve erişim yönetim politikaları geliştirilmesini gerektirmektedir. Gelişen bulut bilişim teknolojileri ile birlikte bu zorlukların üstesinden gelmek, dijital delillerin güvenli ve kontrollü bir şekilde yönetilmesini sağlamak açısından büyük önem taşımaktadır [39].

8. MATERYAL VE METOT

8.1. Materyal

Bu çalışma, adli bilişim süreçlerinin uluslararası hukuk ve teknik standartlarla uyumlu bir şekilde geliştirilmesi konusunu incelemek amacıyla çeşitli dijital ve fiziki materyaller kullanılmıştır. Bu çalışma, hem teorik hem de pratik açıdan adli bilişim uygulamalarını kapsadığından kullanılan materyaller, yasal metinlerden teknik araçlara kadar geniş bir yelpazede ele alınmıştır. Materyaller, adli bilişim süreçlerinin yürütülmesinde kullanılan yazılım ve donanımlar ile ilgili literatürü ve Türkiye’de bu alanda uygulanan yasal düzenlemeleri kapsamaktadır. Bu materyaller, çalışmanın temel dayanaklarını oluşturmuş ve analiz edilen verilerin değerlendirilmesinde kullanılmıştır. Bu bağlamda araştırmada kullanılan ilk materyal grubu, dijital delil toplama ve analiz süreçlerinde uyulması gereken uluslararası ve Türkiye’deki yasal düzenlemeler ve standartlardan oluşmaktadır. Bu yasal düzenlemeler, dijital delillerin toplanması, saklanması ve mahkemelerde kullanılmasını düzenleyen yerel ve uluslararası normları içermektedir. Türkiye’de dijital delillerin toplanması ve mahkemelerde kullanılmasına dair düzenlemeleri içeren CMK, bu araştırmada yasal çerçeve açısından en önemli materyallerden biridir. CMK, adli bilişim süreçlerinin hukuka uygun bir şekilde yürütülmesi için gerekli yasal prosedürleri ortaya koymaktadır. Bu bağlamda,

- **6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK):** Dijital delillerin toplanması ve işlenmesi sırasında kişisel verilerin korunmasına yönelik Türkiye’deki düzenlemeleri içeren KVKK, adli bilişim süreçlerinde veri güvenliği ve gizlilik ilkelerinin korunması açısından önemli bir materyaldir.
- **ISO/IEC Standartları:** Uluslararası adli bilişim süreçlerinde kullanılan ISO/IEC 27037, 27042 ve 27050 gibi standartlar, dijital delillerin toplanması, analiz edilmesi ve raporlanması süreçlerinde kullanılan uluslararası normları içermektedir. Bu standartlar, Türkiye’deki uygulamalarla karşılaştırma yapmak için temel kaynaklardan biri olarak kullanılmıştır.
- **TS 13571:** Türkiye’de bilişim suçlarına yönelik adli bilişim süreçlerinde uyulması gereken teknik ve hukuki düzenlemeleri içeren TS 13571 standardı, araştırmada Türkiye’de uygulanan adli bilişim süreçlerine dair önemli bir referans kaynağı olmuştur.

Çalışmanın teorik temelini oluşturan literatür kaynakları, adli bilişim alanında yazılmış akademik makaleler, kitaplar, raporlar ve uluslararası konferans bildirilerinden oluşmaktadır. Bu literatür kaynakları, dijital delil toplama ve analiz süreçlerinde kullanılan yöntemler ve bu yöntemlerin yasal ve teknik çerçeveleri hakkında kapsamlı bilgi sunmuştur.

Adli bilişim süreçlerine yönelik akademik çalışmalar, araştırmanın literatür incelemesi bölümünde önemli bir yer tutmaktadır. Bu makaleler, uluslararası standartlar, yasal düzenlemeler ve dijital delil yönetimi konularında bilgi sağlamıştır. Adli bilişim süreçleri, dijital delil toplama ve analiz yöntemlerine dair temel bilgileri içeren kitaplar ve kılavuzlar, araştırmada önemli bir literatür kaynağı olarak kullanılmıştır. Bu çalışma literatür taramasına dayandığından araştırmanın temel materyalleri adli bilişim alanındaki mevcut literatür kaynaklarıdır. Bu kaynaklar, dijital delil yönetimi, adli bilişim süreçlerinde kullanılan teknikler ve ulusal ve uluslararası standartlarla ilgili kapsamlı bilgi sunmaktadır. Literatür taramasında yer verilen bir diğer önemli materyal grubu ise dijital delil yönetimi süreçlerinde kullanılan ISO/IEC standartları ve Türkiye’de geçerli olan TS 13571 standardıdır. Bu standartlar, dijital delillerin güvenilirliğini sağlamak için belirlenmiş kuralları ve teknik gereksinimleri içermekte olup, uluslararası ve yerel uygulamaların karşılaştırılmasında temel referans kaynakları olarak ele alınmıştır. ISO/IEC 27037, ISO/IEC 27042 ve ISO/IEC 27050 standartları, dijital delil toplama ve analiz süreçlerine dair genel ilkeler sunarken, TS 13571, Türkiye’deki adli bilişim uygulamalarında uyulması gereken teknik ve yasal düzenlemeleri içermektedir. Ayrıca çalışmada Türkiye’deki dijital delil yönetimini düzenleyen başlıca yasal kaynaklar arasında, Ceza Muhakemesi Kanunu (CMK) ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) bulunmaktadır. CMK, dijital delil toplama süreçlerinde hukuki prosedürleri tanımlarken, KVKK dijital delillerin işlenmesi ve saklanması sırasında kişisel verilerin korunmasına yönelik düzenlemeleri kapsamaktadır. Bu yasal çerçeveler, Türkiye’de adli bilişim süreçlerinde uyulması gereken hukuki standartlar hakkında ayrıntılı bilgi sunmakta olup, araştırmanın temel dayanaklarından biri olarak kullanılmıştır. Tüm bunlarla beraber araştırmada kullanılan tüm materyaller, adli bilişim süreçlerinde uygulanan ulusal ve uluslararası standartlar ile yasal düzenlemeleri kapsayan geniş bir literatür taramasına dayanmaktadır. Bu materyaller, dijital delil yönetim süreçlerinin etkinliğini ve güvenilirliğini artırmak amacıyla hem teorik bilgi sağlamış hem de Türkiye’deki uygulamaların uluslararası standartlarla karşılaştırılmasına olanak tanımıştır. Araştırmada kullanılan literatür kaynakları, dijital delil yönetimi süreçlerinde karşılaşılan teknik ve hukuki zorlukları da kapsamlı bir şekilde ele almaktadır. Adli bilişim uzmanlarının dijital delil toplama, muhafaza etme ve analiz etme süreçlerinde yaşadıkları zorluklar, bu kaynaklardan elde edilen bilgiler ışığında değerlendirilmiştir. Özellikle dijital delillerin güvenliğinin sağlanması, delil zincirinin korunması ve hash algoritmaları kullanarak veri bütünlüğünün sağlanması gibi temel konular, araştırmanın ana odak noktalarını oluşturmaktadır. Araştırmanın dayandığı literatür kaynakları, adli bilişim süreçlerinin teknik gereksinimleri ve operasyonel standartları ile ilgili ayrıntılı bilgi sunmakta, Türkiye’deki dijital delil yönetim süreçlerinin geliştirilmesi için yol gösterici niteliğinde olmaktadır. Bu kaynaklardan elde edilen veriler, çalışmanın analiz ve değerlendirme bölümlerinde dijital delil yönetiminde mevcut durumun kapsamlı bir şekilde incelenmesine olanak tanımıştır.

Bu kapsamda elde edilen bilgiler, Türkiye’deki adli bilişim süreçlerinin uluslararası standartlarla uyumluluğunun geliştirilmesine yönelik somut öneriler sunmaktadır. Özellikle dijital delillerin toplanması ve analizinde uygulanması gereken teknik prosedürler, Türkiye’deki mevcut yasal çerçeveler ile ISO/IEC standartları arasındaki uyum analiz edilerek incelenmiştir. Çalışmada ele alınan literatür, Türkiye’deki adli bilişim uygulamalarının güvenilirliğini ve delil bütünlüğünü sağlamak için belirli standartların uygulanmasının önemini vurgulamaktadır. Bu bağlamda, dijital delillerin saklanması sırasında güvenlik protokollerinin uygulanması, delil zincirinin izlenebilirliği ve şeffaflık gibi unsurların uluslararası standartlara uygun şekilde sürdürülmesi gerekliliği öne çıkan önemli bulgular arasındadır. Son olarak adli bilişim uzmanlarının mesleki gelişimi ve güncel tekniklere hakimiyeti de bu literatür taramasında dikkat çeken bir diğer konudur. Literatürde adli bilişim süreçlerinin etkinliğini artırmak için sürekli eğitim ve kapasite geliştirme programlarının gerekliliği vurgulanmıştır. Türkiye’de adli bilişim uzmanlarının dijital delil yönetiminde karşılaştıkları teknik ve operasyonel zorlukları aşabilmesi için hem teknik standartlara hem de yasal gerekliliklere dair düzenli olarak eğitim alması önerilmektedir. Bu tür eğitimlerin yaygınlaştırılması, Türkiye’nin dijital suçlarla mücadelede daha güvenilir bir konuma ulaşmasına katkı sağlayacaktır. Toparlayacak olursak bu araştırmada kullanılan tüm materyaller, dijital delil yönetiminin uluslararası hukuk ve teknik standartlarla uyumlu hale getirilmesine katkı sağlamak amacıyla yapılan kapsamlı bir literatür taramasına dayanmaktadır.

8.2. Metot

Bu çalışmada uluslararası hukuk ve teknik standartlarla uyumlu adli bilişim süreçlerinin geliştirilmesine yönelik araştırma, çeşitli adımlardan oluşan sistematik bir metot izlenerek gerçekleştirilmiştir. Dijital delil yönetimi süreçlerinin incelenmesi ve Türkiye’deki uygulamaların uluslararası standartlarla karşılaştırılması amacıyla kullanılan yöntemler hem teorik hem de pratik boyutları kapsayacak şekilde yapılandırılmıştır. Çalışmada literatür taraması gibi bilimsel yöntemler kullanılmıştır. Bu metodoloji, adli bilişim süreçlerinin hukuki, teknik ve pratik yönlerinin detaylı bir şekilde analiz edilmesini sağlamıştır. Araştırmanın ilk adımı, adli bilişim süreçleri, dijital delil yönetimi ve ilgili uluslararası standartlar konusunda kapsamlı bir literatür taraması ile başlamıştır. Literatür taraması, akademik makaleler, kitaplar, teknik raporlar, ulusal ve uluslararası kılavuzlar, konferans bildirileri ve standart dokümanlarını içermektedir. Bu tarama, araştırmanın teorik temellerini oluşturmak ve dijital delil yönetimine dair mevcut bilgi birikimini ortaya koymak amacıyla yapılmıştır. Google Scholar gibi akademik veri tabanlarında adli bilişim, dijital deliller, uluslararası standartlar ve Türkiye’deki uygulamalara dair anahtar kelimelerle tarama yapılmıştır. ISO/IEC standartları, Türkiye’de uygulanan yasal düzenlemeler (örneğin Ceza Muhakemesi Kanunu, Kişisel Verilerin Korunması Kanunu), adli bilişim kılavuzları ve vaka çalışmaları bu tarama kapsamında incelenmiştir. Bu durumla ilişkili olarak Aydın [14], bilgi

yönetimi uygulamalarının süreç iyileştirmede nasıl kullanılabileceğini bir vaka analizi üzerinden incelemektedir. Çalışmada bilgi yönetimi uygulamalarının kurumsal süreçlerde verimliliği artırma potansiyeli değerlendirilmiştir. Özellikle süreç iyileştirme çalışmalarında bilgiye erişim, bilginin paylaşımı ve etkin kullanımının önemi vurgulanmıştır. Süreç iyileştirme ve bilgi yönetimi arasındaki ilişkinin incelendiği bu çalışma, organizasyonların operasyonel süreçlerini optimize etmek için bilgi yönetimine nasıl başvurabileceklerini göstermektedir [14].

Türkiye’de uygulanan yasal düzenlemeler ile uluslararası hukuk ve standartlar arasında karşılaştırma yapabilmek amacıyla, dijital delil yönetimine dair Türkiye’deki mevzuat incelenmiştir. Bu aşamada Ceza Muhakemesi Kanunu (CMK), Kişisel Verilerin Korunması Kanunu (KVKK) ve diğer ilgili düzenlemeler ile birlikte ISO/IEC standartlarının yasal gerekliliklerle nasıl uyumlu olduğu analiz edilmiştir. Türkiye’deki yasal çerçevenin incelenmesi, dijital delil toplama ve işleme süreçlerinde uygulanan prosedürlerin hukuki boyutunu anlamak amacıyla yapılmıştır. Özellikle Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK), dijital delil yönetiminde yasal gerekliliklerin nasıl şekillendiğini göstermektedir. Dijital delillerin toplanması, saklanması ve analiz edilmesi süreçlerine dair ISO/IEC 27037, 27042 ve 27050 gibi uluslararası standartların yasal gerekliliklerle uyumu bu aşamada değerlendirilmiştir. Araştırmada Türkiye’de uygulanan adli bilişim standartları ile uluslararası standartlar arasında karşılaştırmalı bir analiz yapılmıştır. Bu aşamada, dijital delil yönetiminde kullanılan yöntemler, yasal çerçeve ve teknik uygulamalar karşılaştırılarak incelenmiştir. Dijital delil toplama, saklama, analiz ve raporlama süreçlerinde uygulanan teknikler, yasal gereklilikler ve standartlar karşılaştırılmıştır. Özellikle veri bütünlüğü, delil zinciri, delillerin güvenliği ve raporlamaya dair prosedürler karşılaştırmalı analizde değerlendirilmiştir.

Çalışmanın karşılaştırmalı analiz aşamasında Türkiye’deki adli bilişim uygulamalarının uluslararası standartlarla uyum düzeyi detaylı bir şekilde incelenmiştir. Bu süreçte, dijital delillerin toplanması ve korunması için belirlenen teknik standartların uygulanabilirliği, Türkiye’deki yasal çerçevelerle ne ölçüde uyumlu olduğu gözden geçirilmiştir. Türkiye’de uygulanan TS 13571 standardı, ISO/IEC standartlarıyla karşılaştırılarak incelenmiş ve bu standartların örtüşen ve farklılaşan yönleri ortaya konmuştur. Böylelikle Türkiye’deki dijital delil yönetim süreçlerinin güçlendirilmesi ve uluslararası normlara tam uyum sağlaması için gerekli iyileştirme alanları belirlenmiştir. Ayrıca adli bilişim süreçlerinin etkinliğini artırmaya yönelik vaka analizlerine de başvurulmuştur [19]. Bu tür vaka analizleri, Türkiye’deki adli bilişim süreçlerinin uluslararası düzeyde geçerlilik kazanması için hangi alanlarda geliştirilmesi gerektiğine dair somut bulgular sunmuştur. Çalışmanın son aşamasında elde edilen literatür ve analiz sonuçlarına dayanarak dijital delil yönetiminde karşılaşılan temel sorunlara yönelik öneriler geliştirilmiştir.

Bu öneriler, Türkiye’deki adli bilişim süreçlerinin uluslararası standartlarla daha uyumlu hale getirilmesi için gerekli adımları içermekte ve adli bilişim uzmanlarının teknik yeterliliklerinin

artırılması, veri güvenliğinin sağlanması ve delil zincirinin etkin bir şekilde korunması gibi konulara odaklanmaktadır. Önerilerin oluşturulmasında, Türkiye'deki mevcut yasal ve teknik altyapının iyileştirilmesine dair literatürde sunulan çözüm yollarından yararlanılmıştır. Bu çalışmada uygulanan metodoloji, adli bilişim süreçlerinin geliştirilmesi için sadece mevcut durumu analiz etmekle kalmamış, aynı zamanda uluslararası standartların Türkiye’de nasıl daha etkin bir şekilde uygulanabileceğine dair stratejik öneriler sunmuştur.

Elde edilen bulgular ışığında, Türkiye’nin dijital delil yönetimi alanındaki eksikliklerinin giderilmesine yönelik yapılması gereken yasal ve teknik düzenlemeler belirlenmiş; ayrıca, adli bilişim uzmanları için eğitim ve kapasite geliştirme önerileri getirilmiştir. Bu kapsamda Türkiye’nin ulusal standartlarını uluslararası normlarla uyumlu hale getirebilmesi için teknik altyapının iyileştirilmesi ve yasal çerçevede gerekli güncellemelerin yapılması gerektiği vurgulanmıştır. Bu kapsamlı metodolojik yaklaşım, dijital delil yönetimi süreçlerinin Türkiye’deki uygulamalarını değerlendirirken aynı zamanda uluslararası standartlarla örtüşen ve ayrışan yönleri açıkça ortaya koymuştur. Özellikle Türkiye’deki yasal düzenlemelerin teknik standartlarla nasıl bütünleştirilebileceğine dair elde edilen bulgular, adli bilişim süreçlerinde güvenilirliği artırmak için yapılması gereken yapısal değişiklikleri de gözler önüne sermiştir. Bu doğrultuda çalışmada sunulan metodoloji, yalnızca mevcut durumu analiz etmekle kalmayıp aynı zamanda sürdürülebilir bir dijital delil yönetim sistemi kurulması için stratejik bir temel oluşturmaktadır. Çalışmanın sistematik yapısı, adli bilişim alanında yapılan araştırmalara ve uygulamalara katkı sağlayacak nitelikte olup Türkiye’deki dijital delil yönetiminde karşılaşılan teknik ve hukuki zorlukların aşılabilmesi için yol gösterici niteliğe sahiptir. Bu araştırma, dijital delil güvenliğinin sağlanması, delil zincirinin korunması ve uluslararası işbirliği süreçlerinin etkinleştirilmesi konularında uluslararası standartlara uygun, kapsamlı bir adli bilişim altyapısı oluşturulmasına yönelik çözüm önerileri sunmaktadır. Tüm bunlarla beraber bu çalışma, Türkiye’deki dijital delil yönetiminin uluslararası hukuk ve teknik standartlarla uyumlu hale getirilmesi için atılması gereken adımlara dair kapsamlı bir çerçeve çizmiştir. Bu metodolojik yaklaşım, Türkiye’nin dijital suçlarla mücadelede daha etkin ve güvenilir bir pozisyona gelmesi için ihtiyaç duyduğu yapısal reformlara katkı sağlamaktadır.

9. BULGULAR VE TARTIŞMA

Araştırmanın bulgularına göre Türkiye’de uygulanan adli bilişim standartları ile uluslararası standartlar arasında birçok ortak özellik bulunmaktadır. Dijital delillerin toplanması, saklanması ve analiz edilmesi süreçlerinde uluslararası standartlar (ISO/IEC 27037, ISO/IEC 27042, ISO/IEC 27050) ile Türkiye’de uygulanan TS 13571 ve ilgili yasal düzenlemeler (CMK, KVKK) büyük ölçüde paralellik göstermektedir. Özellikle veri bütünlüğü, delil zinciri ve dijital delillerin güvenliği konularında benzer ilkeler benimsenmiştir. Hem uluslararası standartlarda hem de Türkiye’deki uygulamalarda dijital delillerin bütünlüğünün korunması, delillerin güvenilirliği açısından temel bir gereklilik olarak kabul edilmektedir [17]. Dijital delillerin toplanması sırasında hash algoritmalarının kullanılması, delilin orijinal halinin korunmasını sağlamak amacıyla her iki sistemde de yaygın bir şekilde uygulanmaktadır. Delil zincirinin izlenmesi ve belgelenmesi, hem uluslararası standartlar hem de Türkiye’deki yasal düzenlemelerde kritik bir öneme sahiptir. Dijital delillerin toplanmasından adli süreçlerde kullanılmasına kadar geçen tüm aşamaların eksiksiz bir şekilde kaydedilmesi ve delil zincirinin korunması, her iki sistemde de vurgulanmaktadır. Uluslararası standartlar ve Türkiye’deki uygulamalar, dijital delillerin güvenliğinin sağlanması için çeşitli güvenlik protokolleri uygulanmasını zorunlu kılmaktadır. Bu protokoller, delillerin saklandığı ortamların güvenliği, yetkisiz erişimlerin engellenmesi ve dijital delillerin şifrelenmesi gibi önlemleri içermektedir [18].

Her ne kadar Türkiye’deki adli bilişim süreçleri uluslararası standartlarla büyük ölçüde uyumlu olsa da belirli alanlarda farklılıklar gözlemlenmiştir. Bu farklılıklar, genellikle yasal çerçeve, teknik altyapı ve uygulama pratiklerinde ortaya çıkmaktadır. Türkiye’de uygulanan adli bilişim süreçleri, Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yerel yasal düzenlemeler tarafından sıkı bir şekilde denetlenmektedir. Uluslararası standartlar, farklı ülkelerde geçerli olabilecek esnek bir çerçeve sunarken Türkiye’de bu süreçler yerel hukuki düzenlemelere daha fazla bağlıdır. Özellikle Türkiye’deki delil toplama süreçlerinde mahkeme kararlarının gerekliliği ve dijital delillerin hukuka uygun şekilde elde edilmesi zorunluluğu, uluslararası uygulamalardan daha sıkı bir denetim ve yasal süreç gerektirebilir [19]. Türkiye’deki adli bilişim süreçlerinde kullanılan teknolojik altyapı, uluslararası standartlara kıyasla bazı farklılıklar göstermektedir. Türkiye’de kullanılan yazılımlar ve donanımlar, yerel ihtiyaçlara ve kamu kurumlarının teknik imkânlarına göre uyarlanmış olabilir. Bu durum, dijital delillerin toplanması ve analiz edilmesinde kullanılan araçların uluslararası geçerliliği olan yazılım ve donanımlarla tam anlamıyla örtüşmemesine neden olabilmektedir. Araştırmada elde edilen bulgular, dijital delillerin toplanması ve işlenmesi süreçlerinde karşılaşılan bazı sorunlara da ışık tutmuştur. Özellikle Türkiye’de, adli bilişim süreçlerinde yasal, teknik ve operasyonel zorluklarla karşılaşmaktadır.

Türkiye’deki yasal düzenlemelerin sıkı denetim gereksinimi, dijital delil toplama süreçlerinde yasal uyum zorluklarına yol açabilmektedir. Mahkeme kararı gerekliliği ve kişisel verilerin korunmasıyla ilgili yasal düzenlemeler, delillerin toplanmasını yavaşlatabilir veya kısıtlayabilir. Türkiye’deki adli bilişim uzmanlarının kullandığı teknolojik araçların sınırlı olması, dijital delillerin analiz edilmesinde zorluklara neden olabilmektedir [20].

Dijital delil yönetimi, özellikle siber suçlar ve dijital suçlar gibi sınır ötesi olaylarla karşılaşıldığında uluslararası işbirliğini gerektirmektedir. Araştırmada Türkiye'deki adli bilişim süreçlerinin uluslararası işbirliği gerektiren durumlarda bazı uyum zorlukları yaşadığı gözlemlenmiştir. Özellikle Budapeşte Sözleşmesi gibi uluslararası siber suçlarla mücadeleye yönelik anlaşmalarda dijital delillerin toplanması ve paylaşılması süreçlerinde daha sıkı bir işbirliği gerekmektedir. Türkiye'nin uluslararası adli bilişim standartları ile tam uyum sağlayarak dijital delil yönetimi süreçlerinde daha etkin bir işbirliği oluşturması gerekmektedir. Bu, dijital delillerin sınır ötesi soruşturmalarda güvenli bir şekilde paylaşılabilmesi için önem taşımaktadır. Ayrıca diğer ülkelerle yürütülen dijital suç soruşturmalarında Türkiye'deki adli bilişim süreçlerinin uluslararası standartlarla uyumlu olması, bu süreçlerin daha şeffaf ve güvenilir bir şekilde ilerlemesini sağlamaktadır. Önel ve Irmak [19], adli bilişim süreçlerinde dijital delillerin Windows işletim sistemi üzerinde incelenmesine odaklanmaktadır. Yazarlar, Windows sisteminde bulunan dijital delillerin nasıl toplanması, analiz edilmesi ve mahkemelerde kullanılmak üzere raporlanması gerektiğini detaylandırmıştır. Ayrıca dijital delillerin güvenilirliği ve doğruluğu açısından dikkat edilmesi gereken hususlar ele alınmıştır [19]. Türkiye’de adli bilişim süreçlerinde karşılaşılan bir diğer önemli sorun, dijital delillerin mahkemelerde kabul edilmesi ve geçerliliği konusundadır. Dijital delillerin hukuka uygun bir şekilde toplanması ve delil zincirinin eksiksiz bir şekilde korunması, bu delillerin mahkemelerde kabul edilmesi için kritik bir gerekliliktir.

Türkiye'deki adli bilişim süreçlerinde dijital delillerin geçerli sayılabilmesi için Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemelere tam uyum sağlanmalıdır. Bu yasalar çerçevesinde, dijital delillerin hukuka aykırı bir şekilde elde edilmesi, delillerin mahkemelerde geçersiz sayılmasına yol açabilmektedir. Dolayısıyla delil toplama süreçlerinin hukuki çerçevede doğru bir şekilde yürütülmesi gerekmektedir. Delil zincirinin izlenebilirliği ve dijital delillerin bütünlüğünün korunması, mahkemelerde bu delillerin kabul edilebilmesi için önemlidir. Türkiye’de delil zincirinin eksiksiz belgelenmesi konusunda yapılan hatalar veya ihmaller, dijital delillerin geçerliliğini riske atabilir. Bu nedenle delillerin toplandığı andan itibaren tüm aşamaların doğru bir şekilde belgelenmesi ve delil zincirinin bozulmaması sağlanmalıdır.

Türkiye’de adli bilişim süreçlerinde yerli ve milli yazılım ve donanımların kullanımı teşvik edilmeli, ancak bu çözümlerin uluslararası standartlarla uyumlu olmasına özen gösterilmelidir. Yerli teknolojilerin geliştirilmesi, Türkiye’nin siber güvenlik alanındaki bağımsızlığını artırmakla

birlikte bu teknolojilerin küresel normlara uygunluğu da göz önünde bulundurulmalıdır. Bu araştırmanın bulguları, Türkiye'deki adli bilişim süreçlerinin büyük ölçüde uluslararası standartlarla uyumlu olduğunu fakat bazı alanlarda iyileştirmeler gerektiğini göstermiştir. Dijital delillerin adli süreçlerde kullanılabilirliği, sadece teknik doğrulukla değil, aynı zamanda bu süreçlerin şeffaflığı ve denetlenebilirliği ile de ilişkilidir [21]. Araştırmada Türkiye’de uygulanan adli bilişim süreçlerinde dijital delillerin denetlenebilirliği ve şeffaflığının artırılması gerektiği tespit edilmiştir. Dijital delil yönetiminin şeffaf bir şekilde yürütülmesi, adaletin sağlanması açısından kritik bir öneme sahiptir. Dijital delillerin toplanması ve analiz edilmesi sürecinde şeffaflığın sağlanması, delillerin denetlenebilir olmasını gerektirmektedir. Türkiye’de bu süreçlerin eksiksiz bir şekilde belgelenmesi ve delil zincirinin açık bir biçimde izlenebilmesi, adli süreçlerde delillerin güvenilirliği açısından önemlidir. Tüm bunlarla beraber adli bilişim laboratuvarlarının uluslararası geçerliliği olan ISO/IEC 17025 standardına göre akredite edilmesi, Türkiye'deki adli bilişim süreçlerinin kalitesini artıracaktır [22]. Bu standart, laboratuvarların teknik yeterliliğini ve doğruluğunu garanti eden bir kalite yönetim sistemidir. Türkiye'deki adli bilişim laboratuvarlarının bu standarda göre akredite edilmesi, dijital delillerin uluslararası alanda daha güvenilir kabul edilmesini sağlamak ve dijital delil yönetiminde hata oranını minimize etmektedir. Türkiye'deki adli bilişim laboratuvarlarının kalite yönetim sistemlerini geliştirmesi ve sürekli iyileştirme faaliyetlerini hayata geçirmesi, dijital delil yönetimi süreçlerinde hataların önlenmesine ve süreçlerin şeffaf bir şekilde yürütülmesine katkıda bulunacaktır.

Araştırmanın sonuçlarına göre Türkiye'deki adli bilişim süreçlerinin uluslararası standartlara uyum sağlaması için laboratuvar akreditasyonunun yanında sürekli eğitim ve kapasite geliştirme programlarının uygulanması gereklidir. ISO/IEC 17025 standardına uygunluk, sadece laboratuvarın teknik kapasitesini artırmakla kalmayıp aynı zamanda adli bilişim uzmanlarının yetkinliğini de güçlendirmektedir. Bu bağlamda, Türkiye'deki adli bilişim uzmanlarının eğitim seviyelerinin ve teknik bilgi birikimlerinin uluslararası standartlara uygun seviyeye getirilmesi, dijital delil yönetimindeki hata oranını düşürebilecek önemli bir adımdır [23]. Bulgular, Türkiye'deki adli bilişim süreçlerinde karşılaşılan zorlukların bir kısmının teknolojik altyapıdan kaynaklandığını göstermektedir. Özellikle veri analizi ve delil inceleme süreçlerinde kullanılan yazılım ve donanım eksiklikleri, dijital delillerin işlenmesinde zaman zaman sınırlamalara yol açmaktadır. Uluslararası geçerliliği olan adli bilişim yazılımlarının temin edilmesi ve bu yazılımların güncel versiyonlarının kullanılabilmesi, Türkiye’deki süreçlerin etkinliğini artıracaktır. Örneğin gelişmiş veri kurtarma ve analiz araçlarının eksikliği, bazı dijital delillerin incelenmesinde karşılaşılan teknik zorlukları artırmakta ve adli bilişim uzmanlarının iş yükünü artırmaktadır [24].

Dijital delil güvenliğinin sağlanması açısından Türkiye’de uygulanan veri muhafaza protokolleri, uluslararası standartlarla uyumlu olmakla birlikte bazı durumlarda geliştirilmesi gerekmektedir.

Türkiye'deki adli bilişim laboratuvarlarının dijital delillerin saklandığı ortamların güvenliğini artırmak adına ek önlemler alması önerilmektedir. Bu öneriler arasında, delillerin saklandığı alanlarda biyometrik güvenlik sistemlerinin uygulanması, yetkisiz erişimlerin daha etkin bir şekilde engellenmesi ve güvenlik açıklarının minimize edilmesi bulunmaktadır [25]. Bu tür güvenlik protokollerinin uygulanması, delillerin mahkemelerde güvenilir bir şekilde kullanılabilmesi açısından kritik bir önem taşımaktadır. Bunun yanı sıra Türkiye'nin dijital delil yönetiminde karşılaştığı bir diğer önemli zorluk, sınır ötesi dijital suçlarla mücadelede uluslararası işbirliği eksikliklerinden kaynaklanmaktadır.

Türkiye'nin Budapeşte Sözleşmesi gibi uluslararası anlaşmalar çerçevesinde diğer ülkelerle dijital delil paylaşımında daha güçlü bir işbirliği yapabilmesi için standart protokollerin uygulanmasına ve karşılıklı güvenin sağlanmasına ihtiyaç duyulmaktadır. Araştırmada Türkiye'nin uluslararası delil paylaşım süreçlerinde daha şeffaf ve uyumlu bir yaklaşım benimsemesi gerektiği vurgulanmaktadır [26]. Bu yaklaşım, dijital delillerin sınır ötesi soruşturmalarda güvenilir ve hızlı bir şekilde kullanılabilmesine olanak tanıyacaktır. Araştırma sonuçlarına göre dijital delil yönetiminde Türkiye'de karşılaşılan yasal ve operasyonel zorlukların çözümü, ulusal düzeyde adli bilişim politikalarının geliştirilmesini gerektirmektedir. Özellikle Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemelerin dijital delil süreçlerinde uygulanması, delillerin güvenilirliği ve kabul edilebilirliği açısından belirleyici rol oynamaktadır. CMK'nın 134. maddesi, dijital delil elde etme sürecinde yasal izin gerekliliğini öngörmekte olup bu gereklilik, özellikle hızlı hareket edilmesi gereken dijital suç soruşturmalarında süreci yavaşlatabilmektedir [27]. Yine KVKK, kişisel verilerin korunması amacıyla bazı sınırlandırmalar getirmekte ve bu sınırlandırmalar, dijital delillerin toplanması ve analiz edilmesinde kısıtlayıcı etki yapabilmektedir. Türkiye'deki yasal çerçevenin sağladığı bu koruma mekanizmaları, birey haklarını güvence altına almak açısından önemli bir katkı sunmakla birlikte, dijital delil toplama sürecinde adli bilişim uzmanlarının hareket alanını da sınırlamaktadır. Yasal sürecin karmaşıklığı ve sıkı denetim gereksinimi, bazı durumlarda dijital delillerin hızlı bir şekilde toplanmasını engelleyebilmekte ve delillerin geçerliliğini tehlikeye atabilmektedir. Bu durum, Türkiye'de dijital delil yönetiminin daha esnek ve hızlı bir yapıya kavuşturulması gerektiğini ortaya koymaktadır [19]. Ayrıca Türkiye'nin uluslararası adli bilişim süreçlerine uyum sağlama yolunda, dijital delillerin güvenli bir şekilde paylaşılmasını ve korunmasını sağlayacak uluslararası işbirliği mekanizmalarının güçlendirilmesi gerekmektedir. Türkiye'nin Budapeşte Sözleşmesi'ne taraf olması, siber suçlarla mücadelede uluslararası ortak çalışmaları mümkün kılmakta ancak bu sözleşme kapsamında dijital delillerin güvenli ve hızlı bir şekilde paylaşılması için yerel altyapının güçlendirilmesi gerektiği vurgulanmaktadır [28].

Araştırmada Türkiye'deki adli bilişim süreçlerinde uluslararası işbirliği ve dijital delil paylaşımı alanında yaşanan uyum zorluklarının aşılması için dijital delil paylaşımı ve doğrulama süreçlerinin

geliştirilmesi önerilmektedir. Dijital delil yönetiminin bir diğer önemli boyutu, kullanılan teknolojik altyapının uluslararası standartlarla uyumlu olması gerekliliğidir. Türkiye’de, yerli ve milli yazılım ve donanımların geliştirilmesi teşvik edilmekte olup, bu araçların uluslararası geçerliliği ve güvenilirliği açısından belirli standartları karşılaması zorunludur [25]. Bu doğrultuda Türkiye’de kullanılan yazılımların uluslararası geçerliliği olan akreditasyon süreçlerinden geçirilmesi, adli bilişim süreçlerinin uluslararası standartlara daha uyumlu hale gelmesine katkı sağlayacaktır. Son olarak araştırmanın bulguları, Türkiye’deki adli bilişim süreçlerinin iyileştirilmesi için eğitim ve kapasite geliştirme programlarının önemini ortaya koymaktadır. Adli bilişim uzmanlarının mesleki gelişimlerini sürdürebilmeleri için uluslararası standartlara göre sürekli güncellenen eğitimlere ihtiyaç duyulmaktadır. Özellikle dijital delillerin güvenilirliğini sağlama, veri bütünlüğünü koruma ve delil zincirini yönetme konusunda eğitimlerin artırılması, uzmanların mesleki yeterliliklerini güçlendirecektir [29]. Araştırmanın sonuçlarına göre, Türkiye’deki adli bilişim süreçlerinde uluslararası uyumluluğu artırmak adına yerel düzenlemelerin güncellenmesi ve teknolojik altyapının geliştirilmesi gerektiği görülmektedir [19]. Bu durum, dijital delillerin uluslararası soruşturmalarda geçerlilik kazanmasını zorlaştırmakta, Türkiye’nin dijital delil yönetiminde uluslararası işbirliği süreçlerini etkileyebilmektedir. Türkiye’nin dijital delil toplama ve analiz süreçlerinde ISO/IEC 27037 ve ISO/IEC 27042 gibi uluslararası standartlara uyum sağlaması, adli bilişim süreçlerinin daha güvenilir ve şeffaf hale gelmesine katkı sunmaktadır. Bu standartlar, dijital delillerin korunması, bütünlüğünün sağlanması ve adli süreçlerde güvenilir bir şekilde kullanılabilmesi için gerekli prosedürleri içermekte ama araştırmada Türkiye’de bu standartların uygulanmasında karşılaşılan operasyonel zorluklar gözlemlenmiştir. Özellikle TS 13571 standardına göre düzenlenen süreçlerde, yerel hukuki düzenlemelerin katılığı ve bazı durumlarda bürokratik engellerin etkisiyle sürecin yavaşlayabildiği ifade edilmektedir [17]. Araştırmanın bir diğer önemli sonucu, Türkiye’nin siber suçlarla mücadelede uluslararası işbirliğine daha fazla önem vermesi gerektiğini ortaya koymaktadır. Budapeşte Sözleşmesi gibi uluslararası siber suç anlaşmaları çerçevesinde yürütülen işbirliği süreçlerinde, Türkiye’nin dijital delil paylaşımı ve veri güvenliği konularında daha kapsamlı bir yaklaşım benimsemesi gerekmektedir. Genel olarak Türkiye’nin adli bilişim süreçlerinde dijital delil yönetimini iyileştirmek adına hem teknolojik altyapıyı hem de yasal düzenlemeleri geliştirmesi gerekmektedir. Bu bağlamda, adli bilişim laboratuvarlarının ISO/IEC 17025 gibi uluslararası kalite standartlarına uygun hale getirilmesi, Türkiye’de adli süreçlerin şeffaflığını ve güvenilirliğini artıracaktır [29]. Bu standartların uygulanması, dijital delillerin uluslararası geçerliliğini sağlamakta ve Türkiye’nin dijital suçlarla mücadeledeki etkinliğini artırmaktadır. Dijital delillerin güvenliğinin sağlanmasında en önemli adımlardan biri, delil zincirinin eksiksiz bir şekilde kaydedilmesi ve belgelenmesidir [17]. Bu eksiklikler, dijital delillerin mahkemelerde geçerlilik kazanması açısından risk oluşturmaktadır. Filiz, delil zincirinin sağlanmasının, adli

süreçlerin güvenilirliği ve şeffaflığı için temel bir gereklilik olduğunu vurgulamaktadır. Ayrıca araştırmanın bulguları dijital delil toplama ve analiz süreçlerinde hash algoritmalarının etkili bir şekilde kullanılmasının önemine de değinmektedir. Türkiye’de dijital delillerin bütünlüğünü koruma amacıyla hash algoritmalarının yaygın olarak kullanıldığı, ancak bu algoritmaların doğru ve etkin kullanımında bazı bilgi ve donanım eksiklikleri yaşandığı tespit edilmiştir [18]. Bu eksikliğin giderilmesi, adli bilişim uzmanlarının dijital delillerin güvenilirliğini sağlama kapasitelerini artıracak ve mahkemelerde delillerin kabul edilebilirliğini güçlendirecektir. Türkiye’de adli bilişim süreçlerinin iyileştirilmesi adına öne çıkan bir diğer önemli öneri, yerli teknolojilerin geliştirilmesi ve bu teknolojilerin uluslararası standartlarla uyumlu hale getirilmesidir [24]. Türkiye’nin yerli yazılımları uluslararası kabul gören standartlara göre geliştirmesi, ülkenin adli bilişim alanında bağımsızlığını artırmakla kalmayacak, aynı zamanda uluslararası alanda daha fazla işbirliği yapabilmesini sağlayacaktır. Ayrıca adli bilişim süreçlerinde şeffaflığın artırılması ve dijital delil yönetiminde hesap verilebilirliğin sağlanması, araştırmanın altını çizdiği bir diğer önemli konudur [19]. Bu tür kayıt sistemlerinin geliştirilmesi, dijital delillerin adli süreçlerde güvenilirliğini artıracak ve mahkemelerde daha şeffaf bir delil sunumu sağlayacaktır. Delil yönetim süreçlerinde yapılan her adımın kayıt altına alınması, dijital delillerin denetlenebilirliğini kolaylaştırmakta ve delil zincirinin güvenilirliğini desteklemektedir. Son olarak, Türkiye’deki adli bilişim uzmanlarının eğitim ihtiyaçları, araştırmanın en önemli bulguları arasında yer almaktadır [20]. Bu tür eğitimlerin sürekliliği, Türkiye’deki adli bilişim süreçlerinin uluslararası düzeyde daha etkin ve güvenilir bir yapıya kavuşmasına katkı sağlayacaktır. Bu araştırmanın bulguları, Türkiye’deki adli bilişim süreçlerinin uluslararası standartlarla tam uyum sağlaması adına kapsamlı bir dizi iyileştirme yapılması gerektiğini ortaya koymaktadır. Özellikle delil zincirinin korunması, hash algoritmalarının doğru kullanımı, yerli teknolojilerin uluslararası uyumluluğu ve uzmanların eğitim gereksinimleri gibi konularda yapılacak iyileştirmeler, Türkiye’de dijital delil yönetiminin kalitesini artıracak ve dijital suçlarla mücadelede daha etkin bir yapı oluşturacaktır.

Araştırmanın bulgularına göre Türkiye’deki adli bilişim standartları ve süreçleri, uluslararası standartlarla büyük ölçüde uyumlu olmakla birlikte belirli alanlarda farklılıklar bulunmaktadır. Bu çerçevede yasal düzenlemeler ve uygulama pratikleri Türkiye’de adli bilişim süreçlerinde Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemeler oldukça sıkı bir denetim mekanizması sunmaktadır [24]. Uluslararası standartlar ile Türkiye’de uygulanan standartlar ve yasal düzenlemelerin delil bütünlüğü, delil zinciri, veri güvenliği, teknik altyapı ve uluslararası işbirliği açısından karşılaştırılması Tablo 9.1’de detaylandırılmıştır.

Tablo 9.1. Uluslararası Standartlar ve Türkiye Mevzuatı Karşılaştırılması

Kategori	Uluslararası Standartlar (ISO/IEC)	Türkiye’de Uygulanan Standartlar ve Yasal Düzenlemeler (TS 13571, CMK, KVKK)
Delil Bütünlüğü	Hash algoritmalarının kullanımı yaygın; delil zinciri yönetimi ISO/IEC 27037 ve 27042 standartlarına uygundur.	Türkiye’de de hash algoritmaları kullanılmakta ancak yasal izne tabi süreçler (CMK 134. madde gereği) bulunmaktadır.
Delil Zinciri	Delil zincirinin korunması standart bir gereklilikler bulunmaktadır.	Delil zincirinin korunması zorunlu ancak bazı bürokratik süreçler süreci yavaşlatabilmektedir.
Veri Güvenliği	Uluslararası standartlarda güvenlik protokolleri, biyometrik sistemler ve yetkisiz erişim önlemleri önerilmektedir.	Türkiye’de veri güvenliği yasal düzenlemelerce korunmakta ancak biyometrik sistemler gibi ek güvenlik protokollerinde kısıtlılıklar vardır.
Teknik Altyapı	Gelişmiş veri kurtarma araçları ve uluslararası geçerliliği olan yazılımlar önerilmektedir.	Türkiye’de yerli yazılım ve donanımlar teşvik edilmekte ancak bunlar uluslararası standartlarla tam uyumlu olmayabilmektedir.
Uluslararası İşbirliği	Budapeşte Sözleşmesi gibi uluslararası anlaşmalarda delil paylaşımı standartlaştırılmıştır.	Türkiye, Budapeşte Sözleşmesi’ne taraf ancak altyapı eksiklikleri sınır ötesi işbirliğinde zorluklar yaratmaktadır.

Uluslararası standartlar, esnek ve genel çerçeveler sağlarken Türkiye’deki süreçlerin daha sıkı yasal düzenlemelere tabi olması, uygulamada bazı operasyonel zorluklara yol açmaktadır. Türkiye’nin uluslararası alanda geçerli olan standartlarla tam uyum sağlayabilmesi için dijital delil toplama süreçlerinde daha esnek bir yapıya kavuşturulması gerektiği sonucuna varılmaktadır [25]. Adli bilişim çalışmalarında kullanılan ulusal standartların getirdiği avantaj ve dezavantajlara Tablo 9.2’de detaylandırılırken uluslararası standartların getirdiği avantaj ve dezavantajlara Tablo 9.3’de detaylandırılmıştır.

Tablo 9.2. Adli Bilişim Çalışmalarında Ulusal Standartlara Uyumun Getireceği
Olası Avantaj ve Dezavantajlar

Ulusal Standartlara Uyumun Getireceği Olası Avantajlar	Ulusal Standartlara Uyumun Getireceği Olası Dezavantajlar
• Adli bilişim süreçlerinde tutarlılık sağlanır ve daha güvenilir çalışma sonuçları elde edilir. • Güvenilirliğe paralel olarak çalışmaların geçerliliği de artar. • Uluslararası akreditasyona uyumu artırır. • Uzmanların tamamını bir kural altında birleştirir. • Denetim, tek standart üzerinden olacağı için kolaylaşır.	• Kurallar her duruma uyarlanamayacak kadar katı olabilir. • Extra maliyet ve zaman gerektirir. • Kimi zaman yenilikçi yöntemlerin kullanımını sınırlandırır. • Ulusal standartları gelişen teknoloji doğrultusunda güncellemek gerekir, bu durum da zaman alıcı ve maliyetli olabilmektedir.

Tablo 9.3. Adli Bilişim Çalışmalarında Uluslararası Standartlara Uyumun Getireceği
Olası Avantaj ve Dezavantajlar

Uluslararası Standartlara Uyumun Getireceği Olası Avantajlar	Uluslararası Standartlara Uyumun Getireceği Olası Dezavantajlar
• Bu standartlar uzun süreli test ve incelemelere dayandığı için oldukça güvenilirdir. • Uluslar arasında işbirliklerini kolaylaştırır. • Yapılan çalışmanın geçerliliğini küresel boyuta taşır. Verileri/delilleri sosyolojik toleranslardan uzaklaştırır. • Standartlara uyumlu eğitimlerin verilmesi adli bilişim uzmanlarının uzmanlık seviyelerini artırır. • Farklı ülkelerde çalışan adli bilişim uzmanlarını tek bir çatı altında birleştirir. Nesnelliği artırır, yorumlamayı azaltır.	• Uluslararası kurallardaki katılık ve netlik her ülkenin yasal ve kültürel yapısına uymayabilir. • Ülkeler arasında uygulama zorlukları/farklılıkları oluşabilir. • Uluslararası uyum için çalışmak daha zaman alıcı ve maliyetlidir. • Geniş bir çerçeve niteliği taşıyan uluslararası standartları ülke /olay bazında özelleştirmek zordur. • Dil engeli söz konusu olabilir, bu engeli aşmak için ayrıca maliyet ve emek gerekir.

Türkiye’de adli bilişim süreçlerinde kullanılan yazılım ve donanımlar, uluslararası standartlarda önerilenlerle kıyaslandığında, bazı farklılıklar göstermektedir. Türkiye’de yerli ve milli yazılım ve donanımların geliştirilmesi teşvik edilmekte olup bu araçların uluslararası geçerliliğe sahip akreditasyon süreçlerinden geçirilmesi gerekmektedir. Örneğin gelişmiş veri kurtarma ve analiz

araçlarının sınırlı olması, dijital delillerin etkin bir şekilde incelenmesini zorlaştırmakta ve adli bilişim uzmanlarının iş yükünü artırmaktadır [26]. Bu durum, dijital delillerin uluslararası soruşturmalarda kabul edilmesi ve güvenilirliğini sağlama sürecinde ek bir zorluk olarak değerlendirilmektedir. Türkiye'nin ulusal yazılımlarını uluslararası normlarla uyumlu hale getirmesi, ülkenin adli bilişim alanında bağımsızlığını artırırken, aynı zamanda dijital suçlarla mücadelede daha etkin bir yapı sunacaktır [27]. Dijital delil yönetimi, özellikle sınır ötesi siber suçlarla mücadele gibi durumlarda uluslararası işbirliğini gerektirmektedir. Türkiye'nin Budapeşte Sözleşmesi gibi uluslararası anlaşmalara taraf olması, uluslararası soruşturmalarda dijital delil paylaşımını kolaylaştırmaktadır. Araştırmanın bulgularına göre Türkiye'nin dijital delil paylaşımı ve doğrulama süreçlerini geliştirmesi, uluslararası işbirliği alanında daha etkin bir yaklaşım benimsemesine katkı sağlayacaktır. Özellikle dijital delillerin sınır ötesi soruşturmalarda güvenli ve hızlı bir şekilde kullanılabilmesi için Türkiye'nin dijital delil paylaşımında şeffaflık ve uyum gerekliliklerini artırması önerilmektedir [28].

Bu çerçevede araştırmanın sonuçları, Türkiye'deki adli bilişim uzmanlarının eğitim ihtiyaçlarına da işaret etmektedir. Dijital delil yönetiminde uzmanların delil zinciri yönetimi, veri bütünlüğünü koruma ve güvenilir delil sağlama konularında sürekli güncellenen eğitimlerle desteklenmesi gerekmektedir. Türkiye'deki adli bilişim süreçlerinde uzmanların mesleki yeterliliklerini artıracak kapasite geliştirme programlarına duyulan ihtiyaç vurgulanmaktadır [29]. Bu tür eğitimlerin, adli bilişim süreçlerinin uluslararası standartlara uygun şekilde yürütülmesine katkı sağlayacağı ve dijital delillerin güvenilirliğini artıracığı düşünülmektedir. Bu kapsamda dijital delil toplama süreçlerinin hızlandırılması ve yasal çerçevenin esnetilmesi, özellikle acil durumlarda süreçlerin daha hızlı ilerlemesini sağlayacaktır [30]. Ayrıca Türkiye'de kullanılan yerli yazılım ve donanımların uluslararası geçerliliği olan akreditasyon süreçlerinden geçirilmesi, dijital delillerin uluslararası kabul edilebilirliğini artıracaktır. Bu iyileştirmelerin, Türkiye'nin dijital suçlarla mücadelesinde etkinliğini artıracığı ve dijital delillerin uluslararası kabul edilebilirliğini sağlamada önemli bir katkı sunacağı düşünülmektedir [31].

10. SONUÇLAR

- Sonuç olarak bu çalışmada uluslararası hukuk ve teknik standartlara uyumlu adli bilişim süreçlerinin geliştirilmesi amacıyla Türkiye’deki uygulamalar ile uluslararası standartlar arasındaki benzerlikler ve farklılıklar incelenmiştir.
- Dijital delillerin güvenilir bir şekilde toplanması, saklanması, analiz edilmesi ve mahkemelerde kullanılması süreçlerinde Türkiye’deki yasal çerçeve ve uygulamalar detaylı bir şekilde ele alınmış ve uluslararası normlarla karşılaştırılmıştır. Elde edilen bulgular, Türkiye’nin adli bilişim alanında önemli bir gelişim kaydettiğini, ancak bazı alanlarda iyileştirilmesi gereken yönlerin bulunduğunu göstermektedir.
- Araştırma, Türkiye’deki adli bilişim süreçlerinin genel anlamda uluslararası standartlarla uyumlu olduğunu ortaya koymuştur. Özellikle dijital delillerin bütünlüğünün korunması, delil zincirinin izlenmesi ve güvenliğinin sağlanması konusunda Türkiye’de uygulanan prosedürler, ISO/IEC standartları ile büyük ölçüde paralellik göstermektedir. Bu kapsamda Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemeler, dijital delillerin hukuka uygun şekilde toplanması ve kullanılmasını sağlamak için sağlam bir zemin sunmaktadır.
- Türkiye’deki adli bilişim süreçlerinde uluslararası standartlarla tam uyum sağlanamayan bazı noktaları da ortaya koymuştur. Özellikle yasal çerçeve, teknik altyapı ve süreçlerin uygulama pratiklerinde karşılaşılan farklılıklar, dijital delil yönetiminde gelişime açık alanları işaret etmektedir. Türkiye’de dijital delillerin toplanması ve kullanılması süreçleri, sıkı bir yasal denetime tabi olup mahkemelerde delillerin kabul edilebilirliği hususunda uluslararası uygulamalardan daha fazla yasal gereklilik ve belgelendirme şartı aranmaktadır. Bu çerçevede Türkiye’de kullanılan adli bilişim teknolojileri, uluslararası standartlara göre daha sınırlı olabilmektedir. Özellikle dijital delil analizinde kullanılan yazılım ve donanımların modernize edilmesi ve uluslararası geçerliliği olan araçlarla uyumlu hale getirilmesi, bu alandaki etkinliği artıracaktır.
- Türkiye’deki adli bilişim süreçlerinin uluslararası işbirliği ve dijital delil paylaşımı açısından güçlendirilmesi gerekmektedir. Türkiye’nin siber suçlarla daha etkin mücadele edebilmesi ve dijital delillerin uluslararası alanda geçerliliğini artırabilmesi için uluslararası normlara uyum düzeyi yükseltilmelidir.
- Dijital delillerin mahkemelerde kabul edilebilirliği, adli bilişim süreçlerinin güvenilirliği ve doğruluğu açısından büyük bir öneme sahiptir. Türkiye’deki yasal düzenlemelere göre, dijital delillerin hukuka uygun şekilde toplanması ve delil zincirinin eksiksiz bir biçimde belgelenmesi zorunludur.

- Araştırmada elde edilen bulgular, dijital delillerin mahkemelerde kullanılabilmesi için hukuki süreçlerin daha etkin bir şekilde uygulanması gerektiğini göstermektedir. Türkiye’de dijital delillerin toplanması ve kullanılması sırasında Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemelere uyum sağlanması, delillerin mahkemelerde geçerli olabilmesi için kritik öneme sahiptir.

Genel olarak araştırma, Türkiye’deki adli bilişim süreçlerinin uluslararası hukuk ve teknik standartlarla tam uyum sağlamasının sadece ulusal düzeyde değil, aynı zamanda uluslararası soruşturma ve yargılama süreçlerinde de büyük önem taşıdığını göstermektedir. Özellikle siber suçlar gibi sınır ötesi faaliyetlerde dijital delillerin uluslararası kabul edilebilirliği, bu delillerin toplandığı ülkenin standartlarla ne ölçüde uyum sağladığı ile doğrudan ilişkilidir. Türkiye’nin, siber suçlarla mücadele için imzaladığı Budapeşte Sözleşmesi ve diğer uluslararası anlaşmalara tam uyum sağlaması, dijital delil yönetimi süreçlerinin küresel kabul edilebilirliğini güçlendirecektir. Türkiye’deki adli bilişim süreçlerinin bu sözleşmelerin gereklilikleri ile uyumlu hale getirilmesi, uluslararası işbirliğini kolaylaştıracak ve dijital suçlarla mücadelede etkinliği artıracaktır. Uluslararası adli bilişim standartlarının (örneğin ISO/IEC 27037, 27042, 27050) Türkiye’de daha geniş bir şekilde benimsenmesi, dijital delillerin yönetiminde karşılaşılan teknik ve operasyonel zorlukları ortadan kaldıracaktır. Bu standartların Türkiye’de daha yaygın kullanılması, hem ulusal hem de uluslararası davalarda dijital delillerin güvenilirliğini artıracaktır. Bu bağlamda çalışma, Türkiye’deki adli bilişim süreçlerinin uluslararası normlarla büyük ölçüde uyumlu olduğunu, ancak bazı alanlarda geliştirilmesi gerektiğini ortaya koymuştur. Özellikle yasal çerçevede daha fazla uyum ve esneklik sağlanması, dijital delillerin toplanması ve analiz edilmesinde kullanılan teknolojik altyapının güçlendirilmesi gerekmektedir. Genel olarak Türkiye, dijital delil yönetimi süreçlerinde önemli ilerlemeler kaydetmiştir, ancak uluslararası standartlarla tam uyumu sağlamak ve küresel düzeyde rekabet edebilir hale gelmek için yasal, teknik ve eğitimsel açılardan bazı iyileştirmelere ihtiyaç duymaktadır.

ÖNERİLER

Bu araştırmanın sonuçlarına dayanarak Türkiye’de uygulanan adli bilişim süreçlerinin uluslararası standartlarla tam uyumlu hale getirilmesi ve dijital delil yönetiminde karşılaşılan zorlukların aşılması için aşağıdaki öneriler sunulmaktadır. Bu öneriler, hem yasal düzenlemelerin geliştirilmesi hem de teknik altyapının modernize edilmesi açısından kritik öneme sahiptir. Bu bağlamda,

- Ceza Muhakemesi Kanunu (CMK) ve Kişisel Verilerin Korunması Kanunu (KVKK) gibi yasal düzenlemeler, dijital delil yönetimi süreçlerinde uluslararası standartlarla uyumlu hale getirilmeli ve dijital delillerin mahkemelerde geçerli kabul edilmesini sağlamak için gerekli hukuki prosedürler güçlendirilmelidir.
- Dijital delil yönetiminde kullanılan teknolojik araçların modernize edilmesi ve uluslararası standartlara uygun hale getirilmesi gerekmektedir. Türkiye’deki adli bilişim laboratuvarları ve güvenlik birimlerinin kullandığı yazılım ve donanımların geliştirilmesi, dijital delil toplama ve analiz süreçlerinin daha güvenilir ve hızlı bir şekilde yürütülmesine olanak sağlayacaktır.
- Dijital delillerin güvenilir ve geçerli bir şekilde toplanıp analiz edilmesi için adli bilişim laboratuvarlarının uluslararası standartlara göre akredite edilmesi büyük önem taşımaktadır. Türkiye’deki adli bilişim laboratuvarlarının uluslararası geçerliliği olan akreditasyonlara sahip olması, dijital delillerin mahkemelerde kabul edilebilirliğini artıracak ve süreçlerin güvenilirliğini sağlayacaktır. Adli bilişim laboratuvarlarının teknik yeterlilik ve kalite açısından uluslararası kabul görmüş ISO/IEC 17025 standardına göre akredite edilmesi sağlanmalıdır.
- Türkiye’deki adli bilişim laboratuvarlarının kalite yönetim sistemlerinin güçlendirilmesi, dijital delil analizinde hataların en aza indirilmesine ve güvenilir sonuçlar elde edilmesine katkıda bulunacaktır. Laboratuvarların düzenli olarak denetlenmesi ve iyileştirme faaliyetlerinin uygulanması, adli bilişim süreçlerinin kalitesini artıracaktır. Dijital delillerin güvenliği ve kişisel verilerin korunması, adli bilişim süreçlerinde en önemli hususlardan biridir.
- Türkiye’de Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında dijital delillerin toplanması ve işlenmesi süreçlerinde veri gizliliği kurallarına tam uyum sağlanmalıdır. Özellikle kişisel verilerin korunması ile ilgili yükümlülüklerin ihlal edilmemesi için bu süreçlerin daha titiz bir şekilde yönetilmesi gerekmektedir. Türkiye’de elektronik keşif alanında daha gelişmiş yazılımlar ve analiz araçları kullanılmalı ve bu süreçler uluslararası standartlara uygun hale getirilmelidir.

- Sınır ötesi soruşturmalarda kullanılacak dijital delillerin paylaşımı ve doğrulanması için elektronik keşif süreçlerinin geliştirilmesi ve bu süreçlerin daha hızlı ve güvenilir bir şekilde yürütülmesi sağlanmalıdır. Türkiye’de e-discovery süreçlerinin daha etkili hale getirilmesi, uluslararası işbirliğini güçlendirecektir. Türkiye’de dijital delil yönetiminde kullanılan Ulusal Yargı Ağı Projesi (UYAP), adli süreçlerin dijitalleşmesini ve dijital delillerin adalet sistemine entegrasyonunu destekleyen önemli bir platformdur.
- UYAP’ın dijital delil yönetim süreçlerinde daha gelişmiş altyapılar sunması, dijital delillerin güvenli bir şekilde saklanması ve paylaşılması süreçlerinde önemli bir katkı sağlayacaktır. Özellikle dijital delil saklama, erişim kontrolü ve veri güvenliği gibi alanlarda UYAP’ın kapasitesinin artırılması gerekmektedir. UYAP üzerinden dijital delillerin doğrulanması ve güvenli bir şekilde saklanması için elektronik imza ve şifreleme gibi güvenlik protokolleri daha geniş çapta uygulanmalıdır.

Genel olarak Türkiye’de adli bilişim süreçlerinin uluslararası standartlarla tam uyumlu hale getirilmesi ve dijital delil yönetiminde karşılaşılan zorlukların aşılması için atılacak adımların temelini oluşturmaktadır. Yasal reformlar, teknik altyapının modernize edilmesi, uzman eğitimlerinin güçlendirilmesi ve uluslararası işbirliği süreçlerinin iyileştirilmesi, Türkiye’nin dijital suçlarla mücadeledeki etkinliğini artıracak ve adli süreçlerde dijital delillerin daha güvenilir ve hızlı bir şekilde kullanılmasına katkı sağlayacaktır.

KAYNAKLAR

- [1] A. E. B. Yüksel, “Hukukun Bağımsız Bir Alanı Olarak Bilişim Hukuku”, *Taad*, Sy. 54, Ss. 395-414, Nisan 2023, Doi: 10.54049/Taad.1274452.
- [2] G. Alptekin, P. Kartal, “Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 29 (1), 2023.
- [3] O. Değirmenci, “Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi”, *Bilişim Hukuku Dergisi*, 2(1), 47-79, 2020.
- [4] B. Çekiç, “Bilgisayar Verilerinde Arama, Kopyalama, El Koyma Tedbirinin Hukuki Niteliği Ve Benzer Kavramlar”, *Nku Hukuk Fakültesi Dergisi*, C. 2, Sy. 1, Ss. 153–185, 2021, Doi: 10.51562/Nkuhukuk.2021217.
- [5] K.M. Bedii, “Hukuki Açından Bilişim Suçları-Siber Güvenlik Ve Adli Bilişim”, *Bgd Siber Güvenlik Ve Savunma Kitap Serisi*, 2, 213-279, 2019.
- [6] E. Akbal, Ş. Doğan, Ve M. Kaya, “Adli Bilişim Mühendisliği Müfredatı Ve Gereksinimleri”, *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, C. 28, Sy. 2, Ss. 149–158, 2016.
- [7] M. Özen, G. Özocak, “Adli Bilişim, Elektronik Deliller Ve Bilgisayarlarda Arama Ve El Koyma Tedbirinin Hukuki Rejimi (Cmk M. 134)”, *Ankara Barosu Dergisi*, (1), 2015.
- [8] İ. Kara “Dijital Kanıtlarının İncelemeleri Ve Hukuki Boyutu”, *Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 24(3), 183-188, 2019.
- [9] F. Mahmutoglu, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, *Journal Of Istanbul University Law Faculty*, C. 71, Sy. 1, Ss. 855–889, 2013.
- [10] C. Şahin, “Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma (Cmk M. 134)”, *Yaşar Hukuk Dergisi*, C. 1, Sy. 2, Ss. 271–286, 2019.
- [11] U. İhtiyaroğlu, “Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi”, *Hacettepe Hfd*, C. 10, Sy. 2, Ss. 406–440, 2020, Doi: 10.32957/Hacettepehfd.726568.
- [12] L.D. Nguyen, “Dijital Adli Bilime Kısa Bir Bakış”, *Adli Bilimler Ansiklopedisi: Cilt 1-4, Üçüncü Baskı (Cilt 1, S. 19–25)*, 2022
- [13] F. Çağlayan, “Adli Bilişim Bağlamında Kayıt Tutma Ve Delil Toplama İlkeleri”, *Taad*, Sy. 16, Ss. 21–40, Ocak 2017.
- [14] O.F. Aydın, “Süreç İyileştirmede Bilgi Yönetimi Uygulamalarının Kullanılması Üzerine Bir Vaka Analizi”, *Yüksek Lisans Tezi*, 2007, 1 - 148

- [15] Ö. Çakır, M.H. Calp. A. Doğan, Uzaktan Eğitimde İçerik Geliştirme Süreci: Gazi Üniversitesi Bilişim Enstitüsü Örneği, *Cumhuriyet International Journal Of Education-Cije*, 4(1), 2015, 1 - 20
- [16] M. Özcan, Süreç Yönetimi Ve Süreç İyileştirmenin İşletme Performansına Etkilerinin Analizi, *İşletme Araştırmaları Dergisi*, 13 (2), 2021, 1144-1161.
- [17] Yusuf, B. Adli Bilişim Sürecinde Karşılaşılan Sorunlar Ve Çözüm Önerileri, *Tbb Dergisi*, 2020, 148, 47 - 76
- [18] A.A. Süzen, K. Kayaalp. Endüstri 4.0 Ve Adli Bilişim, Bilim Ve Teknoloji Araştırmaları, 2019, *Çizgi Yayınevi*
- [19] B. Önel. E. Irmak. Adli Bilişim Ve Dijital Delillerin Windows İşletim Sistemi Üzerinde İncelenmesi, *Politeknik Dergisi*, 24(3), 2021, 1187-1196
- [20] A. Emekçi. E. Kugu, Murtaza, T. Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 2(1), 8 - 14
- [21] Çil A. Demirci M., “Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi Ve Yazılım Tanımlı Ağlarda İncelenmesi”, *Journal Of Polytechnic*, 27(2), 2024, 665-679.
- [22] S. Düden. Türkiye’de Adli Bilişimin Gelişimi Ve Dijital Delil İncelemeleri, *Yüksek Lisans Tezi*, 2019
- [23] A. Aldoori. Uluslararası Hukukta Siber Suçla Mücadele, *Yüksek Lisans Tezi*, 2020
- [24] İ. Çiçek. A. Okatan. Ülkemizde Adli Bilişim Laboratuvarı Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları, *Yüksek Lisans Tezi*, 2008
- [25] M, Turan. Adli Bilişim Ve Dijitalleştirme: Roller, Etkileşim Ve Sorunlar. *Kurumsal Belleklerin Geleceği*, 121, 2016
- [26] T, Henkoğlu. Adli Bilişim: Dijital Delillerin Elde Edilmesi Ve Analizi. *Pusula*, 2020
- [27] U, Taşçı. A, Can. Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 25(2), 2015, 229-248
- [28] M, Önok. Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadele Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları D Dergisi*, 19(2), 2013, 1229-1270.
- [29] A, Efe. Uluslararası Hukuk Çerçevesinde Yolsuzlukla Mücadele. *Journal Of Politics Economy And Management*, 4(2), 2021, 59-86.
- [30] G, Erdoğan. Yapay Zekâ Ve Hukukuna Genel Bir Bakış. *Adalet Dergisi*, (66), 2021, 117-192.
- [31] S. Özel, Uluslararası Uyuşmazlıkların Çözümünde Güncel Durum Ve Büyük Veri. *Dicle Üniversitesi Hukuk Fakültesi Dergisi*, 28(48), 2023, 65-121.

- [32] M.İ., Aytekin. Adli Muhasebe Kapsamında Uzman Tanıklık (Bilirkişi Tanıklığı), Dava Destekleri, Hile, Yolsuzluk Ve Suistimal Denetçiliği: Karaman İlinde Bir Araştırma. *Yüksek Lisans Tezi*, 2022
- [33] P, Özkaya. Adli Bilişimde Standardizasyon Sertifikasyon Akreditasyon Ve En İyi Uygulamalar. *Yüksek Lisans Tezi*, 2021
- [34] K, Şimşek. Uluslararası İç Denetim Standartları Kapsamında Yürütülen İç Denetim Uygulamalarının Kurumsal Yönetim Kalitesi Üzerindeki Rolü: Borsa İstanbul Kurumsal Yönetim Endeksinde Yer Alan Şirketler Üzerinde Bir Anket Çalışması. *Doktora Tezi*, 2019
- [35] Ö, Sağlık. Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi. *Doktora Tezi*, 2021
- [36] G, Yücel. Yapay Zekâ Teknolojilerinin Kolluk Faaliyetlerinde Kullanımı. *Yüksek Lisans Tezi*, 2024
- [37] M. B., Kaya. İnsan Hakları Ekseninde İnternetin Kontrolü Ve Hukuki Sorumluluk Rejimi. *Anayasa Yargısı*, 37(2), 2020, 159-203.
- [38] E, S., Kızmaz, M., Yardımcıoğlu. Bilişim Sistemlerinin Ve Teknolojilerinin Muhasebe Ve Finansal Raporlama Uygulamalarına Etkisi. *Eğitim Yayınevi*, 2021
- [39] M, Turan. Adli Bilişim Ve Dijitalleştirme: Roller, Etkileşim Ve Sorunlar. *Kurumsal Belleklerin Geleceği*, 2016, 121.
- [40] Ö.F., Yakut, F., Ertam. Android Cihazların Adli Bilişim Analizlerinde Parola Tespitine Bağlı Yeni Süreç Tanımlama Modelinin Geliştirilmesi. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 32(1), 2020, 147-156.
- [41] E, Akbal. F., Güneş. Adli Bilişim Mühendisliği Eğitiminin Kurumlar Açısında Önemi. *Düzce Üniversitesi Bilim Ve Teknoloji Dergisi*, 4(2), 2016, 395-402.
- [42] B., Önel, E., Irmak. Adli Bilişim Ve Dijital Delillerin Windows İşletim Sistemi Üzerinde İncelenmesi. *Politeknik Dergisi*, 24(3), 2021, 1187-1196.
- [43] İ, Dilber. Çetin, A. Adli Bilişim İncelenme Süreçlerinde Yapay Zeka Kullanımı: Vgg16 İle Görüntü Sınıflandırma. *Düzce Üniversitesi Bilim Ve Teknoloji Dergisi*, 9(5), 2021, 1695-1706.
- [44] İ, Kara. Adli Bilişim İncelemelerinde Şifre Kırma Yöntem Ve Teknikleri. *Acta Infologica*, 5(1), 2021, 27-38.
- [45] A, Çil. M., Demirci. Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi Ve Yazılım Tanımlı Ağlarda İncelenmesi. *Politeknik Dergisi*, 27(2), 2022, 665-679.
- [46] Z, M. Sakar. (2021). Adli Bilişim Kavramıyla Bilişim Suçları Ve Uygulamaları İstatistiklerine Genel Bakış. *Turan-Sam*, 13(52), 2021, 218-227.

- [47] H, Karaca. Adli Muhasebenin Sunduđu Fırsatlar Ve Geliştirilmesi Gereken Yönleri.
Bulletin Of Economic Theory And Analysis, 8(2), 2023, 156-17



ÖZGEÇMİŞ

Mustafa PEKDEMİR

████████████████████

██████████

████████████████████

██████████

114

114

[REDACTED]

████████████████████

████████████████████

████████████████████

10/10/2016

[REDACTED]

[REDACTED]

[REDACTED]

AKADEMİK FAALİYETLER

Bildiriler:

1. Pekdemir Mustafa, Ertam Fatih (2023) The Importance of Examining Digital Evidence in Terms of Digital Forensics (IIC2023), 2023, Batman