ADLİ OLAYLARDA DELİL TOPLAMA VE DİJİTAL DELİLLERİN KOSOVA -TÜRKİYE UYGULAMALARININ KARŞILAŞTIRILMASI

COLLECTING EVIDENCE IN FORENSIC EVENTS AND COMPARISON OF THE KOSOVA-TURKEY APPLICATION DIGITAL EVIDENCE

MENSUR MORİNA

DR.ÖĞR.ÜYESİ MUAMMER KETİZMEN

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim – Öğretim ve Sınav Yönetmeliğinin

Adli Bilimler Anabilim Dalı İçin Öngördüğü

DOKTORA TEZİ olarak hazırlanmıştır.

2023

ÖZET

ADLİ OLAYLARDA DELİL TOPLAMA VE DİJİTAL DELİLLERİN KOSOVA - TÜRKİYE UYGULAMALARININ KARŞILAŞTIRILMASI

Mensur MORİN

Doktora, Adli Bilimler Bölümü

Tez Danışmanı: Dr.Öğr. Üyesi Muammer KETİZMEN

Ocak 2023, 169 sayfa

Delil, bir suçun işlenip işlenmediğini meydana çıkaran önemli bir araçtır Adli olaylarda, olay yeri incelemesinin yöntemleri sayısız ve çeşitlidir. Yargılama aşamasında suçun ne şekilde işlendiğinin anlaşılmasına yarayan ve olayı ispat edecek olan unsur delildir. Bu yüzden deliller, maddî gerçeğe ulaşması işlenen suçun ispatı ile yargılamanın adaletli ve hızlı şekilde yapılmasına yardımcı olur. Ayrıca deliller yargı organlarının n suç ve suçlu arasındaki ilişkiyi anlamalarına ve karar vermelerine yardımcı olur. Olay yerinden elde edilen deliller, suçun işleniş şekli, zamanı, sanığın hareket şekli, mağdur ve olay yerine dair bilgiler vermektedirler. Diğer taraftan, dijital sistemlerin toplumsal yaşamda daha çok yer edinmesiyle birlikte, olay yeri kavramı fiziki bir ortamdan sıyrılıp dijital alana doğru kaymış, bu yüzden yeni suç çeşitlerinin dijital yollarla işlenmesine ve bunun sonucunda dijital delil kavramın doğmasına neden olmuştur. Kosova mevzuatına göre dijital delillerin toplanmasına ilişkin özel yasalar bulunmamaktadır. Buna karşın, Türkiye gibi örnek ülkelerde dijital delillere ilişkin yasal düzenlemeler bulunmaktadır. Bu çalışmada adli olaylarda delil toplama yöntemlerini ve Kosova ile Türkiye'de dijital delillere ilişkin yasal mevzuatının karşılaştırılması yapılacaktır.

Anahtar Kelimeler: Ceza Muhakemesi, Soruşturma, olay yeri, adli olaylar, delil, delil toplama yöntemleri, dijital deliller, Kosova-Türkiye Hukuku karşılaştırması.

ABSTRACT

COLLECTING EVIDENCE IN FORENSIC EVENTSAND COMPARISON OF THE KOSOVA-TURKEY APPLICATION DIGITAL EVIDENCE

Mensur MORİNA

Doctorate, Department of Forensic Science

Supervisor: Dr.Öğr. Üyesi Muammer KETİZMEN

January 2023, 169 page

Evidence is an important tool to reveal whether a crime has been committed. In forensic cases, the methods of crime scene investigation are numerous and varied. Evidence is the element that helps to understand how the crime was committed during the trial phase and will prove the event. For this reason, the evidence helps to make the trial fair and fast with the proof of the crime committed to reach the material truth. Evidence also helps judicial bodies understand the relationship between crime and criminal and make decisions. Evidence obtained from the crime scene gives information about the way the crime was committed, the time of the crime, the course of action of the accused, the victim and the crime scene. On the other hand, with digital systems taking more place in social life, the concept of crime scene has shifted from a physical environment to the digital field, thus causing new types of crime to be committed digitally and as a result, the concept of digital evidence has emerged. According to Kosovo legislation, there are no specific laws regarding the collection of digital evidence. On the other hand, there are legal regulations regarding digital evidence in exemplary countries such as Turkey. In this study, the methods of collecting evidence in forensic cases and the legal legislation on digital evidence in Kosovo and Turkey will be compared.

Keywords: Criminal Procedure, Investigation, crime scene, forensic events, evidence, evidence collection methods, digital evidence, Kosovo-Turkey law comparison.

TEŞEKKÜR

Doktora eğitimini başlatmak ve bitirmeye ulaşmak uzun, meşakkatli ve zor bir süreci içerir. Birçok insanın bana verdiği yardım ve destek sayesinde uzun bir eğitim yolculuğunun sonuna geldim.

Bunun için bu zaman sürecinde yanımda olan ve beni destekleyen herkese takdirimi ve teşekkürlerimi sunmak için bu fırsatı kullanıyorum.

Her şeyden önce yardım, tavsiye ve desteği olmadan bu çalışmanın gerçekleştirilmesi mümkün olamayacak olan rehber hocam Dr. Muammer KETİZMEN'e, teşekkür etmek istiyorum.

Ayrıca, doktora tezimi başarıyla tamamlamak için bilgi toplama ve seçme konusunda bana yardım eden Prof. Dr. Olgun DEĞİRMENCİ ile Doç. Dr. Harun ARTUNER'e , diğer bütün direktörler, profesörler ve doktora eğitimi akademik kadrosına teşekkürlerimi sunmak istiyorum.

Bu fırsatı, bana her düzeyde eğitim veren, analiz etmemi, sentezlememi, yapılandırmamı ve çalışmamı başarıyla yürütmemi kolaylaştıran tüm profesör kadrosuna teşekkür etmek için kullanıyorum.

Sabırlarını ve maddi ve manevi yardımlarını esirgemeyen, cesareti olan, beni dinleyen ve çok yardımcı olan aileme, anne babama, eşim LEONORA'ya, oğlum EYMEN'e, üç ablam ve erkek kardeşime de sonsuz teşekkür ve minnetlerimi sunarım. Onların desteği, özeni ve sevgisi olmadan bugün burada, önünüzde olamazdım. Yanımda durup şikâyetlerimi, stresimi ve yüklerimi dinlediğiniz ve yanınızda olmam gereken an ve anlarda yokluğumu doğru anladığınız için minnettarım.

Hepinize teşekkür ederim.

Mensur MORİNA

Ocak 2023, Ankara

İÇİNDEKİLER

KISALTMALAR

AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AÖAY	Adli ve Önleme Aramaları Yönetmeliği
AYM	Anayasa Mahkemesi
CMK	Ceza Muhakemesi Kanunu
CPU	Central Processing Unit
FSEK	Fikir ve Sanat Eserleri Kanunu
FTK	ForensicsTool Kit
GPS	Global PositioningSystem
HMK	Hukuk Muhakemesi Kanunu
HTML	HyperTextMarkup Language
IDS	IntrusionDetectionSystems
IP	Internet Protocol
ISS	Internet Service Server
IT	Information Technologies
LAN	LocalArea Network
MAC	Media Access Control
PDA	PersonalDigital Assistance
RAM	Random Access Memory
ROM	Read Only Memory
TDK	Türk Dil Kurumu
URL	Uniform Resource Locators
WAN	WideArea Network

1. GİRİŞ

Bilgisayar teknolojisinin gelişimi ile birlikte günümüzde bilgisayar, cep telefonu ve benzeri sayısal elektronik aygıtlarla, elektronik posta, mesaj gibi çok yüksek miktarda veri oluşturulmakta ve iletilmektedir. il. Bu gelişmeler, bireylerin hayatlarının her aşamasını etkilemekte ve bu kapsamda konumuz açısından önem arz ettiği haliyle klasik suç türlerinin yanında bu teknolojilerin kullanıldığı kişisel bilgilere ve finansal araçlara yönelik hırsızlık ve dolandırıcılık suçlarının ortaya çıkmasına yol açmaktadır. Günümüzde ortaya çıkan genel olarak bilişim suçları olarak da adlandırılan soruşturulması, bu suçları işleyen fail ya da faillerin belirlenmesinde klasik fiziki deliller yeterli olmayabilmektedir. Bu nedenle, bu suç türlerinin tespiti ve suç işleyenlerin cezalandırılması amacıyla, dijital delillerin elde edilmesi ve toplanması zorunluluğu ortaya çıkmıştır.

Bilgisayar ve diğer iletişim cihazları, genel adıyla elektronik aygıtlar veya bilişim sistemleriyle işlenen suçlarda,bu aygıt veya sistemler,bazen suçun işlenmesinde doğrudan kullanılan bir araç, bazen de suç delillerinin gizlendiği ortam olmaktadır. Bu tür durumlardadijital delil,suç veya şüphelilerin belirlenmesinde çoğunlukla tek delil olabilmektedir.

Dijital delillerin tespiti ve aranmasına yönelik çalışmaların büyük oranda klasik delil etme yöntemleriyle uyumlu olduğu söylenebilir. Ancak, yapılan arama sırasında veya olay yerinin incelenmesi esnasında dijital delile rastlandığı zaman, bu delile ilk temastan başlayarak, elektronik aygıtın olay mahallinden götürülmesi, imaj alınması gibi tüm işlemlerin hassasiyetle, uzman görevliler tarafından ve tüm yasal kurallar ile prosedürlere uygun yapılması gerekmektedir. Aksi takdirde, elde edilen dijital veri, bozulmuş veya değiştirilmiş olacak ve delil olma özelliğini kaybedebilecektir.

Ceza muhakemesi hukukunun amacı şüphesiz maddi gerçeğe ulaşmaktır. Devlet, geleneksel suçları işleyenlerde olduğu gibi, bilişim suçlarını işleyenleri de toplum adına cezalandırmakla görevli olsa da, maddi gerçeğe ulaşırken kullandığı yöntemlerde temel hak ve hürriyetlere saygı göstermek olmak ve hukuk devleti ilkeleri doğrultusunda hareket etmekle yükümlüdür.

Bu çalışmanın başlangıcında öncelikle Kosova ve Türk hukukunda genel anlamda adli olaylarda delil toplama usulü anlatılmıştır. Her iki hukuktaki mevzuat ve delil toplama

usullerine değinilmiştir. Çalışmanın devamında yine Kosova ve Türk hukukunda dijital delillerin neler olduğu, her iki ülke mevzuatına göre nasıl elde edilmesi gerektiği irdelenmiştir. Ayrıca her iki ülkenin mevzuatı incelenerek dijital delili arama ve elkoymanın yasal şartları ve kolluk görevlilerince arama, el koyma ve inceleme sırasında yapılması gerekenler anlatılmıştır. Bununla birlikte çalışmada ceza yargılamasında delil ve dijital delili anlamı, bu delillerde olması gerekli özellikler ve dijital delilin hangisi delil türü içine girdiği incelenecektir. Dijital delilin nasıl ve hangi ortamlarda elde edilebileceği, dijital delilde bulunması gereken özellikler, fiziki delillerle arasındaki farklılıkların neler olduğu, hukuken geçerli delil kabul edileceği hallerin hangileri olduğu, elektronik delille ilgili ortaya çıkan sorunların neler olduğu, dijital delillerin geçersiz olmasına yol açan haller ile ceza yargılamasında kabul edilebilir bir delil olup olmadığı hususlarına değinilecektir.

Dijital delilin kolay değiştirilebilir ve bozulabilir hassas yapısı ve bu delilin elde edilirken bile bozulma olasılığı dikkate alındığında, başka delillerle desteklenmediği sürece, sanıkların mahkûm edilebilmesi için yeterli olup olmadığının da tartışılması gerekmektedir. Ancak, dijital delilin yargılamada kullanılabilmesi ve geçerli bir delil olarak kabul edilebilmesi için şüphelerden uzak ve inandırıcı bir delil olması gerekmektedir. Bu yüzden, dijital delilin hukuka uygun olarak ele geçirilmesi ve yapısında bir bozulma ya da değişime uğramayıp uğramadığının analiz edilmesi gerekmektedir.

Diğer taraftan, hem Türk hukukunda hem de Kosova ceza muhakemesi hukukunda delil serbestîsi ilkesi bulunsa da, bu ilke mutlak değildir ve hukuka uygun şekilde ele geçirilen edilmiş deliller ile sınırlandırılmaktadır. Bu sebeple, delil serbestîsi ilkesi ve bu ilkeye aykırı olan hukuka aykırı deliller de çalışmada irdelenecektir.

Dijital ortamda bulunan ve açığa çıkarılan delillerin bozulabilir ve hassas ve kırılgan yapıları nedeniyle bu delillerin hukuki düzenlemelere uygun olarak soruşturma veya kovuşturma makamlarına ulaşmasını sağlayacak koruma önlemlerine ihtiyaç duyulmaktadır. Bu koruma önlemlerinin sağlanamaması halinde bilişim sistemlerinde bulunan ve dijital delillerle ortaya çıkarılacak suçların kanıtlanamaması neticesini beraberinde getirebilir.

Öte yandan, dijital deliller elde edilirken şüpheli veya sanıklara ait bilişim sistemlerinde üstünde uygulanacak arama, el koyma ve inceleme gibi koruma tedbirleri kişilerin özel hayatlarının gizliliğine saygı hakkı, düşünce özgürlüğü ile haberleşme özgürlüğü hakları gibi temel hak ve hürriyetlere de müdahale etmektedir. Kişilerin temel hak ve özgürlüklerine bu düzeyde etki eden koruma tedbirleri yasa ile getirilmeli ve bu tedbirler uygulanırken bireyler bazı yasal güvencelere sahip olmalıdırlar.

Uluslararası düzenlemelerde dijital delilin ele geçirilmesine dair en önemli Sözleşmelerden biri olan Avrupa Konseyi Siber Suç Sözleşmesi'ne[1] Türkiye taraf olup, Kosova anılan Sözleşmeye taraf değildir.

Kosova hukukunda dijital delillerin elde edilmesine ilişkin düzenlemelere bakıldığında Kosova Ceza Muhakemesi Kanunu'nun (KCMK) "Bilgisayar Analizleri" başlıklı 147. maddesinde bir mahkeme emri veya onay üzerine hukuka uygun bir şekilde alınan bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da benzer teçhizatların içinde bulunan bilgi ya da verilerin ele geçirilmesi ve incelenmesi için resmi bilirkişi olarak polis görevlisi veya bilirkişinin atanacağını öngörmüştür. Ayrıca, KCMK m.105/8'de bilgisayar, kamera, cep telefonu, seyyar elektronik cihazlar ya da korunmaya yarayan seyyar elektronik aygıtların esaslı nedenlerin olması halinde muhafaza altına alınmasına (kontrol) karar verilebileceği, kontrol emri ya da geçici el koyabileceği ve bunlardaki dijital verilerin kopyalanabileceği hükmü yer almaktadır. Yine Kosova hukukunda Sibernetik Suçlarla Mücadele Kanunu gibi kanunlardaki bilgisayar sistemleri kullanılarak işlenen suçlarda dijital delil etme yöntemleri yer almaktadır.

Türk hukukunda ise 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) m.134'de bilgisayar ile bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri düzenlenmiş olup, bu maddeye göre bu bilişim sistemlerindeki dijital delillerin mahkeme kararı ve gecikmesinde sakınca olması durumunda Cumhuriyet savcısı kararıyla el konulabileceği hükmü yer almaktadır. Türk hukukunda da 5651 sayılı Kanun'da erişim sağlayıcı, yer sağlayıcı gibi sağlayıcıların kayıt altına aldıkları verileri adli makamlarla

[1]Avrupa Konseyi Siber Suç Sözleşmesi'ne taraf olan ülkeler için bkz. https://www.coe.int/en/web/conventions/ full-list?module=signatures-by-treaty&treatynum=185, erişim tarihi: 06.04.2022.

paylaşmaları gerektiğine dair hükümler bulunmaktadır. Çalışmada hem Kosova hukukunda hem de Türk hukukunda anılan hükümlerin yeterli olup olmadığı incelenecek ve bu hükümlerin uygulanma örnekleri verilmeye çalışılacaktır.

Ayrıca teknolojik gelişmelerle gündeme gelen uzaktan erişimle arama ve bulut bilişimde arama gibi arama türleri ile her iki ülkede yürürlükteki bu hükümler karşılaştırılacak ve bu teknolojilere anılan hükümlerin uygulanıp uygulanmayacağına dair cevaplar aranacaktır.

Son olarak çalışmada dijital delillerin, delil olarak kabul edilebilmesi için dijital delilin bulunduğu elektronik aygıttan elde edilmesi, toplama safhasında gerekli olan teknolojik ve hukuki alt yapı, dijital delilin bütünlüğünün korunması için yapılması zorunlu olan işlemlerin (imaj alma, hash değeri, koruma zinciri…) neler olduğu, bu delillerin bulunduğu yerden, ortamdan toplanması usulü, uygun ortamlarda taşınması ve korunması gibi hususlar üzerinde durulacaktır.

2. GENEL BİLGİLER

2.1. Genel Olarak Kosova Ceza Muhakemesi Hukukunda İspat ve Deliller

Birbirleri arasında benzeşim, etkilenme söz konusu olabilmekle birlikte her devletin kendi tarihsel sosyo-ekonomik özellikleri kapsamında kendi ceza muhakemesi süreçleri şekillenmektedir. Kosova'da da ceza muhakemesi hukuku Kosova Cumhuriyeti Resmi Gazetesi'nin 28 Aralık 2012 tarihli ve 37 sayılı Resmi Gazetesinde yayımlanan 13 Aralık 2012 tarihli04/L-123 sayılı Kosova Ceza Muhakemeleri Kanunu (KCMK)ile şekillendirilmiştir. Bunun yanında savcılık örgütünün kurulmasına ilişkin 13 Mart 2008 tarihli ve No. 03 / L-052sayılı kanun ve polis teşkilatı ver görevlerine ilişkin 2 Mart 2012 tarihli ve No. 04/L-076sayılı kanunlar önem arz etmektedir. Konunun anlaşılabilmesi açısından Kosova'da bu kanunlarla şekillendirilen ceza muhakemesi sürecine ilişkin olarak aşağıda kısa bir bilgi verilecektir.

Bilindiği üzere, bir suçun işlendiğine ilişkin şüphe söz konusu olduğunda suçu ve suçun failini tespit etmek için, soruşturma ve kovuşturma sürecine katılanlar ispata yönelik olarak delil elde etme, toplama zorunluluğundadır. Nitekim, şüpheden sanık yararlanır ilkesi gereği, işlendiği ileri sürülen bir suç ile bunu işlediği ileri sürülen bir kimsenin, o suçu işleyip işlemediğinin her türlü şüpheden uzak bir biçimde kanıtlanması gerekmektedir. Şüpheden sanık yararlanır ilkesi, 15 Haziran 2008 tarihli Kosova Anayasasının m.31/f.5'de[2] ve 1982 tarihli Türkiye Cumhuriyeti Anayasası m.38/f.4'de[3] yer almıştır.

Ceza muhakemesini yürüten makamlar, KCMK hükümlerinde tanımlanan görevlerini yerine getirirken, suçun işlenip işlenmediğini belirlemeli ve suçun failini tespit etmelidir. Yine 14 Ocak 2019 tarih ve 2 sayılı Kosova Cumhuriyeti Resmi Gazetesi'nde yayınlanan 23 Kasım 2018 tarih ve 06/L-074 sayılı Kosova Cumhuriyeti Ceza Muhakemeleri Kanunu m.69[4] kapsamında fail hakkındaki temel ceza belirlenirken; cezai sorumluluk düzeyi, suç

---

[2] Kosova Anayasası m.31/f.5: "*Ceza gerektiren suçla suçlanan herkes, yasalara uygun şekilde suçluluğu ispatlanmadıkça, suçsuz sayılır*".

[3] 1982 tarihli Türkiye Cumhuriyeti Anayasası m.38/f.4' "*Suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz*".

[4] KCMK m.69: "*1. Polis, suç işlemlerini işbu Kanunun 70. maddesi uyarınca soruşturur ve bunu mümkün olan en kısa zamanda devlet savcısına rapor eder.*

işleme nedenleri, tehlike veya korunan değerlerin zarar görme yoğunluğu, suçun işlenmiş olduğu durumlar, failin önceki davranışları, suçun kabul edilmesi ve failin kişisel durumları ve suç işleminden sonraki davranışları yargılama aşamasında açıklığa kavuşturmalıdır.

Suç, geçmişte meydana gelen ve muhakeme aşamasında fail tarafından işlendiğinin kanıtlanması gereken bir olaydır. Suçun işlenmesindeki koşullar ve sanığın suçlu olup olmadığı sadece delillerle belirlenebilir.

Suçun işlenmesiyle toplum düzeni yani devletin koruması gereken yasal düzen de ihlal edilir. Devlet, ceza kanunları ile korunan hukuki değerleri koruma görevini yerine getirerek, bozulan düzenin yeniden sağlanması için suçların faillerine karşı önlem almalıdır. Bu nedenle, ceza muhakemesi hukuku kuralları esas alınarak, suç işleyen kişiye karşı ilgili cezai yaptırım belirlenebilir. Bununla birlikte, cezai yaptırım belirlenmeden önce, suçun sanık tarafından gerçekleştirildiğinin tüm şüphelerden uzak bir biçimde belirlenmesi gerekir. Bu nedenle, ceza muhakemesinin amacı olan[5]maddi gerçeğin araştırılması ve neticesinde suçun işlendiğinin belirlenmesi halinde ceza kanunlarının öngördüğü koşullara göre faile verilecek cezai yaptırımın tespit edilmesi gerekmektedir. Yasayla düzenlenmiş usullere göre, suçlu olmayan kimsenin cezalandırılmamasına dikkat edilerek, ceza muhakemesi usulünde gerçeğin tespit edilerek, hukuki uygun bir kararın doğru ve tam olarak alınması için önemli olan bulguların kanıtlanması gerekmektedir[6].

Kosova'da suç işlediğinden şüphelenilen bir kişinin soruşturulması sırasında, bir şüphelinin suçu veya suçsuzluğunu tespit edecek delillerin soruşturulması, toplanması ve sunulması, KCMK m.6 uyarınca Polis ve Devlet Savcılığı gibi devlet kurumlarının sorumluluğu altındadır. Yine bu maddedeki soruşturma makamları şüphelinin lehine olan delil ve

---

2. Devlet savcısı ve polis, işbu Kanunun 70. maddesinde belirtilen ön çalışmalar süresince birlikte çalışır.

3. İşbu Kanunun 84. maddesinde belirtilen önlemin uygulanmasına ilişkin yetki ardından veya 102. maddesinde belirtilen ceza muhakemesinin başlaması ardından, suç soruşturmasını gerçekleştiren polis veya diğer organ çalışmasını devlet savcısı yönetir ve denetler.

4. Devlet savcısının, ön çalışmalar süresince polisin sahip olduğu tüm ilgili soruşturma bilgilerine erişimi vardır."

[5]Doğan Soyaslan, Ceza Muhakemesi Hukuku, Güncelleştirilmiş 8.Baskı, Yetkin Yayınları, Ankara 2020, s. 55; Bahri Öztürk / Mustafa Ruhan Erdem, Uygulamalı Ceza Muhakemesi Hukuku, 12.Baskı, Seçkin Yayınevi, Ankara 2008, s. 66.

[6]EjupSahiti, Rexhep Murati, E Drejta E ProceduresPenale (Ceza Muhakemesi Kanunu), Priştine, 2016, s.225.

olguların soruşturmada ileri sürülmesini ve kullanılmasını sağlamakla yükümlüdürler (KCMK m.7/2).

Ceza muhakemesinde soruşturma ve kovuşturma aşamasında, muhakemede yer alan makamların, hukuka uygun bir karar vermeden önce olayları doğru ve eksiksiz bir şekilde belirlemelerine dair yasal yükümlülükleri, KCMK'nin 7. maddesinin 1. fıkrası yer almaktadır[7]. Ceza muhakemesinde, savcı ve polis, ve en önemlisi yargılamayı yapacak olan mahkemenin hukuka uygun bir karar alınması için önemli olan, gerçekleri doğru ve eksiksiz şekilde belirlemesidir[8].Türk hukukunda da soruşturmayı yürüten savcı, maddî gerçeği araştırmak ve adil bir yargılama yapabilmek amacıyla emri altındaki adlî kolluk görevlileri aracılığıyla, şüphelinin leh ve aleyhine olan delilleri elde etmek ve şüphelinin haklarını muhafaza etmekle mükelleftir (CMK m.160/2)[9].

Bu kanun hükmü, kararlarını yalnızca delil ve bulgular dayanan gerçekleri değerlendirdikten sonra vermekle yükümlü olan devlet organlarının uymakla hükümlü olduğu, temel esas ve sınırlamaları ortaya koymaktadır. Ceza muhakemesinde ispat ancak somut gerçekleri doğrulayan delilleri ele aldıktan ve analiz ettikten sonra mümkün olabilir. Bu yasal sınırlama, ceza muhakemelerin temel ilkelerinden biri olan maddi gerçek ilkesini temsil eder.

Yukarıdaki hükme göre, somut ceza davasında gerçekleri tespit etmek anlamında polis, savcılık ve nihayetinde yargılamayı yapan mahkemeler, herhangi bir muhakeme safhasında bir karar vermeden önce, bu gerçekleri inceleyip değerlendirme açısından dikkatli olmalıdırlar. Bu dikkat, özellikle insan haklarını ve özgürlüklerini kısıtlayan kararlar alırken, yani yargılamanın ilk aşamalarında üst düzeyde olmalıdır.[10]

Ayrıca mahkeme, devlet savcısı ve polis hakkında suç isnat edilen kişinin hem aleyhine hem de onun lehine olan delillere ulaşmaya çalışmalıdır. Ayrıca, bu makamlar

---

[7] KCMK m.7/f.1: "Ceza muhakemesinde kapsanan mahkeme, devlet savcısı ve polis, meşru bir kararın alınması için önemli olan olguları doğrulukla ve bütünüyle doğrulamakla yükümlüdür".

[8]Kosova Ceza Muhakemeleri Kanunu, madde 7, fıkra 1.

[9] Nur Centel-Hamide Zafer, Ceza Muhakemesi Hukuku, Beta Yayınları, İstanbul 2015, s.108; Hakan Karakehya- Murat Arabacı, Cumhuriyet Savcısının Hukuki Statüsü, Muhakemedeki Taraf Pozisyonu Ve İspat Yükünün Bulunması Üzerine., Ankara Üni. Hukuk Fak. Dergisi, 65 (4) 2016, ss.2059-2081, s.2064.

[10]AzemHajdari, Komenmtari I Kodit te ProceduresPenale te Kosoves, Priştine, 2016, s.20

muhakemeden önce ve muhakeme sırasında sanığın ve savunma avukatının yargılama öncesi ve sırasında sanık lehine tüm delillere ulaşmasını sağlamaya yardımcı olmalıdırlar.[11]

Delillerle ilgili olarak özellikle savcıya atıfta bulunan bir diğer yasal sınırlama, savcının delilleri ve suçlayıcı ve beraat edici gerçekleri analiz etme yükümlülüğü ve davanın sanığın haklarının tam olarak yerine getirilmesini sağlayacak bir şekilde yapılmasını ve de ayrıca delil toplamanın KCMK'nin XVI. Bölümüne aykırı olmamasını sağlamaktır (Kosova Ceza Muhakemeleri Kanunu'nun bu bölümü ceza yargılamalarında nasıl delil elde edileceğini açık bir şekilde ortaya koymaktadır).[12]

Bilindiği üzere, polisin soruşturma usulleri kapsamında delil elde etmedeki rolü çok önemlidir. Dünyanın birçok ülkesinde polis, pratikte cezai soruşturmalar yürüten ana organdır ve yapısal organizasyona bağlı olarak polis savcılık, mahkeme vb. tarafından kontrol edilir. Ancak, polisin adli görevlerini yerine getirmesi kapsamında kendi içerisinde uzmanlaşma süreci gündeme gelmiş ve bu kapsamda kendi içinde temel ve ayrıca ileri düzey ceza soruşturması bilgilerine sahip olma yönünde bir uzmanlaşmaya gidilmiştir.

Bu kapsamda soruşturma aşamasında polis savcılık arasında ilişki açısından bakıldığında Türk hukukunda asıl yetkinin savcıda olduğu görülür. Nitekim Türk hukukunda5271 sayılı CMK m.158/1'de suç ihbarının kolluk kuvvetlerine yapılabileceği belirtilmişse de, muhakeme işlemleri, savcısın talimatları çerçevesinde yapılacaktır (m.164/2). Polis dahil adlî kolluk görevlileri, elkoyma hali, yakalanan kişiler ile tatbik ettikleri önlemleri emrinde görev yaptıkları Cumhuriyet savcısına hemen bildirmekle ve bu savcının soruşturmaya dair bütün emir ve talimatlarını gecikmeden icra etmekle mükelleftirler (CMK m.161/2)[13].Kosova'da ise polisinin KCMK m.69 ve devamı maddeleri uyarınca yaptığı işlemler, bir suç ihbarını almasından sonra ön inceleme ve araştırma şeklinde işlemlerdir. "Polis soruşturması" başlıklı KCMK m.69/1'de açıkça polisin suç işlemlerini KCMK m.70 gereğince soruşturacağı ve durumu mümkün olan en kısa zamanda devlet savcısına rapor

[11]Kosova Ceza Muhakemeleri Kanunu, madde 7, fıkra 2.

[12]Kosova Ceza Muhakemeleri Kanunu, madde 48.

[13]Karakehya- Arabacı, s.2065; Halil Polat, Teori ve Uygulamada Cumhuriyet Savcısının El Kitabı, Adalet Yayınevi, Ankara 2009, s.569 vd

edeceği belirtilmiştir. Ayrıca, KCMK m.70/2'de devlet savcısı ve polisin, KCMK m.70 kapsamında yürütülen polis soruşturmalarındaki ön çalışmalar süresince birlikte çalışacağı açıkça yer almıştır.

Polis, ön inceleme kapsamında KCMK m.70/1 uyarınca suç işlendiği ihbarını aldıktan sonra suç işlenip işlenmediğine dair makul şüphenin var olup olmadığını araştırır. Ayrıca polis, KCMK m.70/2 ve 70/3 gereğince polis, suç işlemlerini araştırır, failleri ve ona yardım edenlerin kim olduğu ve yerlerini belirlemek, onları durdurmak, suçla ilgili izleri, delilleri ve delil olabilecek diğer unsurları belirlemek, muhafaza etmek ve muhakemede kullanılabilecek bütün bilgileri toplamak için gerekli tüm önlemleri alır.

Polis memurlarının delil toplama için sevk edilmesinden sonra, suç unsurlarının varlığı konusunda şüphelerin olup olmaması ve potansiyel olarak faili (şüpheliler) ile ilgili daha net bir fikir ortaya çıkacaktır. Suçun işlendiğine ve bir veya daha fazla kişinin potansiyel failler olduğuna dair şüphe uyandıran delil topladığında Polis, savcı ile işbirliğinden sonra, bir ceza raporu hazırlar ve ardından savcılığın değerlendirmesine göre, diğer prosedürel işlemlere devam eder ve bunlar kapsamında soruşturmalar, ilave delil toplama veya diğer kişilerin soruşturmaya dâhil edilmesini gerektirerek genişletilebilir. CMK'da olduğu gibi, suçun ihbarı veya öğrenilmesinden sonra Kosova polisi KCMK m.70'deki gereken önlemleri alacak ve devlet savcısı ile temasa geçecektir. KCMK 69 ve 70. maddeleri birlikte değerlendirildiğinde KCMK anlamında da soruşturmanın sahibi devlet savcısıdır ve polis, onun emir ve talimatlarını dikkate alır ve yerine getirir. Kaldı ki, şüpheli ifadesi ve tanık beyanları da dahil olmak üzere polis tarafından toplanan delillerle oluşturulan polis suç isnadı raporunu, devlet savcısının KCMK m.82'ye göre reddedebilme yetkisi, devlet savcısının polis üstündeki yetkisini güçlendirmektedir. Ancak, KCMK m.71 ve devamı uyarınca polisin re'sen şüpheli ifadesi ve tanık beyanı alabilmesi gibi yetkiler de polisin soruşturma aşamasında elini güçlendiren yetkilerdir.

Bununla birlikte, KCMK m.68'de ceza muhakemesinin dört farklı aşamasının olduğu, bunların; soruşturma aşaması, iddianamenin hazırlanması aşaması, yargılama aşaması ve kanuni yollar aşaması olduğu belirtilmiş ve ceza muhakemesinde, KCMKm.84. kapsamındaki polisin ön çalışmaları ile bilgi toplamalar önce gelebileceği belirtilmiştir.

Öte yandan, KCMK m.6'daDevlet savcısı, kamu ve özel kurum ve kuruluşlar, vatandaşlar, basın veya başka ceza soruşturmasında elde edilen bilgilerin alması ya da mağdurun şikayeti veya ihbarı ardından, bu maddenin 2. fıkrasına uygun bir şekilde cezai takibatı başlatabileceği hükmü yer almıştır. Devlet savcısı, kendine yapılan şikayet ve ihbarlar üzerine re'sen harekete geçerek soruşturma başlatabilecektir.

Bu savcılık soruşturmaları olumlu sonuçlanırsa ve bir veya daha fazla kişinin şüphelendiği durumlarda bir suç işlendiğine dair yeterli delil varsa, savcılık iddianameyi açar ve yetkili mahkemeye gönderir. Türk hukukunda da suça dair ihbar ve şikayet, savcılığa ya da kolluk mercilerine yapılabilir. Valilik, kaymakamlık veya mahkemeye gerçekleştirilen ihbar ya da şikâyet, ilgili yer Cumhuriyet Başsavcılığına iletilir (CMK m.158/1-2)[14]. Yine Türk hukukunda da soruşturma safhasında elde edilen deliller suçun işlendiği konusunda yeterli şüphe meydana getiriyorsa savcının iddianameyi düzenleyeceği öngörülmektedir (m.170/2)[15].Polis, genellikle çeşitli yasal ve alt-yasa düzenlemelerinde belirlenen çok sayıda muhakeme işlemlerine ek olarak, maddi delil toplamak ve bunları değerlendirmek için bazı özel yasal yetkilere de sahiptir. Polis, iddia edilen suç ile ilgili olay yerindeki delilleri dikkatlice toplar ve uygun şekilde saklar ve de delillerin yetkili laboratuvar tarafından test edilmesine izin verir[16].

Polis ve savcılığın delillerle ilişkin yasal yükümlülüklerini yerine getirdiğinde ve nihayetinde yargılama yapılmasını gerektiren bir durumun varlığı tespit edildiğinde, savcılık makamı iddianame düzenleyerek (KCMK m.101) mahkemeye sunar. Yargılama, yani kovuşturma aşaması yetkili mahkemede yapılır ve bu durumda kovuşturma organının asıl amacı, suçun işlenip işlenmediğini ve suç işlenmişse bunu belirli bir kişinin işleyip işlemediğini ortaya çıkarmaktır. Türk hukukunda da iddia makamı ve yargılama organının işleyişi hemen hemen benzerdir[17].

---

[14] Hüsamettin Uğur, Suçların İhbarı ve İhbarcıların Korunması, TBB Dergisi, S.108, 2013, s.387.

[15] Ahu Karakurt, Türk Ceza Muhakemesi Hukukunda İddianamenin İadesi, S.8-9, 2004, ss.71-114, s.80; Centel-Zafer, s.368.

[16]Kosova Ceza Muhakemeleri Kanunu, madde 71, fıkra 1.

[17] Ahmet Gökcen- Kerim Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi Ve Delil Yasakları, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., ss. 2911-2951, 2019, s.2916.

Esas yargılama[18] sonucunda, Mahkeme, bağımsız bir kurum olarak, delilleri ele aldıktan sonra dava hakkında esasa dair bir karar verecektir ve bunu sanığın suçluluğu veya masumiyeti hakkındaki kararı, kendisine sunulan veya resmi şekilde aldığı delillere dayanarak alacaktır.

Her delilin ağırlığını ayrı ayrı ve birlikte ele almak, delillerin yasal hükümlere uygun olarak elde edilmesini sağlamak ve bu delillerin bir kişinin suçunu veya masumiyetini ikna edici bir şekilde kanıtlaması mahkemenin yasal yükümlülüğüdür,

Her mahkeme kararı delillere dayanmaktadır, bu nedenle mahkemenin delilleri değerlendirmedeki rolü çok önemlidir. Mahkeme, kararını asla kanuna aykırı delillere dayandırmamalı ve hiçbir zaman bu delillere dayanarak mahkûmiyet kararı almamalıdır. Mahkemenin asıl amacı, yalnızca yasal olarak elde edilen delillere dayanarak, tam bir hukuki dayanağa sahip şekilde esasa ilişkin bir karar vermektir. KCMK ayrıca mahkemenin kararlarını yalnızca dava sırasında incelenecek ve ele alınacak yasal deliller temelinde vermesini öngörmektedir. Mahkeme, ana duruşmada incelenen ve doğrulanan delillere dayanarak karar verir[19].

Mahkeme kararının alınmasında temel teşkil eden ve doğruluğu teyit edilmiş suçla ilgili herhangi bir delil, ana duruşmada ikame edilmeli ve değerlendirilmelidir. Doğal olarak, bu delillerin uyumuna veya birbirleriyle çelişip çelişmediklerine bakılacaktır ve aynıları mahkeme konuyla ilgili karar vermeden önce birbirileriyle karşılaştırılacaktır.[20]

Asıl yargılama başlamasından önce[21] elde edilen deliller ve nihayetinde yargılamada ileri sürülen deliller, mahkemenin belirli bir karara varmadan önce incelenmeli ve doğrulanmalıdır(KCMK m.8/2).Bunun nedeni, cezai muhakemesinde taraf olanların

---

[18]Kosova ceza muhakemesi hukukunda ön duruşma kurumu bulunmaktadır, bkz. Yener Ünver- Hakan Hakeri, Ceza Muhakemesi Hukuku C.3, Adalet Yayınevi, Ankara, 2019, s.1385 dp.1.

[19]Kosova Ceza Muhakemeleri Kanunu, Madde 8, Fıkra 2, Madde 370, Fıkra 7.

[20]Hajdari, s. 21.

[21]KCMK m.123/2'ye göre ön duruşma devlet savcısı tarafından gerçekleştirilir ve şüpheli ifadesi veya tanık beyanı alınabilir. KCMK m.121 ve devamı maddelerinde, ABD hukukunda "preliminary hearing" denilen ön duruşma kurumu düzenlenmiştir. ABD hukukunda jüri esas yargılama öncesi soruşturma aşamasındaki bu duruşma tek hakim hakim tarafından gerçekleştirilir ve makul şüphenin (probablecause) olup olmadığına bakılır. Bkz. Mehmet Emin Yapar, Amerika Birleşik Devletleri Federal Ceza Hukukunda Plea Bargaining (İddia Pazarlığı) Kavramı Ve Uygulaması, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Konya 2012, s.84.

davanın delillerini bilmesi ve bunlarla ilgili somut ifadelerini verebilmesi gerekliliğinden kaynaklanmaktadır. Delillerin kovuşturmada ele alınması, özellikle mağdur gibi (KCMK m.19/1) yükümlükleri ve çıkarları mahkemenin kararından etkilenenler için de geçerlidir[22].

Herhangi bir hukuk sisteminde, mahkemenin kararlarını kabul edilebilir ve hukuki yollarla elde edilmiş delillere dayandırması, yaygın olarak kabul gören bir standart uygulamadır. Bağımsız ve tarafsız bir yargı sisteme sahip olmayı amaçlayan herhangi bir devlet, mahkeme kararlarının yalnızca delile dayalı olması ve hiçbir koşulda diğer dış faktörlerden etkilenmemesi için çaba gösterir.

Tek kelimeyle, her yargılama, her mahkeme süreci, delil temelinde yürütülmeli ve sonuçlandırılmalı ve deliller herhalükarda yasal hükümlere uygun şekilde sağlanmalı ve elde edilmesi gerekmektedir. Çünkü, yasa dışı yollarla elde edilen herhangi bir delil, çoğu durumda, delilin önemli bir gerçeği açıkça ve doğru bir şekilde gösterdiğine bakılmaksızın kabul edilemez bulunacaktır. Yasa koyucu, yasanın uygulanması adına yasadışı yollarla cezai muhakemelerde delil elde edebilecek devlet kurumlarını, kötüye kullanma eğiliminden kaçınmak için katı muhakeme kısıtlamaları getirmiştir. Bu yasal kısıtlamalar, devlet kurumlarını dikkatli ve hesap verebilir olmaya zorlarken, diğer yandan, bireylere yasa dışı delillerle suçlanmayacağı ya da cezalandırılmayacağı garantisi sunmaktadır.

Mahkeme, kararını kabul edilemez delillere dayandıramaz, bu nedenle, KCMK'nin 258. maddesinin 2. paragrafı[23] uyarınca mahkeme aşağıda belirlenen durumlarda delil alınmasını yasaklayabilir:

---

[22]Hajdari, s. 22.

[23]KCMK m.257'de hukuka aykırı delile ilişkin düzenlemeye yer verilmiştir: "Delillere İlişkin Genel Kurallar

1. Bu madde ile öngörülen delil kuralları, mahkeme huzurunda tüm ceza muhakemelerinde uygulanır ve işbu Kanunun öngördüğü durumlarda, bunlar aynı zamanda devlet savcısı ve polis huzurunda da uygulanır.

2. Ceza muhakemeleri hükümlerinin ihlal edilmesiyle alınan deliller, işbu Kanunun ya da yasanın diğer hükümlerinin açık bir şekilde öngörmesi durumunda, kabul edilemezdir.

3. Mahkeme, kabul edilemez delillere kendi kararını bağlayamaz.

4. Yapılan her mülakat ya da sorguya alım esnasında aşağıdakiler yasaktır:

4.1. kendi görüşünü formüle etmesi ve ifade etmesi için sanığın özgürlüğüne kötü muamele, neden olunan yorgunluk, fiziksel müdahale, uyuşturucu kullanımı, şiddet, zorlama ya da hipnoz aracılığıyla etki etmek;

4.2. yasa ile yasaklanan ölçülerde sanığın tehdit edilmesi;

4.3. yasa ile öngörülmeyen herhangi bir kazancın vaat edilmesi; ve

2.1. Konunun, genel olarak bilinmesi, dolayısıyla, diğer delilleri tamamlamak için bu tür delilleri elde etmek gereksizdir;

2.2. Kanıtlanacak olan gerçek karar için hiçbir önem taşımamaktadır ya da aynısı daha önce kanıtlanmıştır;

2.3. Delil tamamen uygun değildir, mümkün değildir veya alınması mümkün değildir;

2.4. Talep, yargılamayı uzatmak için yapılmıştır. Kabul edilemez deliller, kökenleri bilinmediğinden, söylentilere ve ilk bakışta imkânsız veya güvenilmez olarak kabul edilen delillere veya bilgilere dayanan, esasen desteği olmayan herhangi bir bilgi olarak kabul edilir.[24]

Türk hukukunda da delillerin elde edilmesi ve değerlendirilmesi esnasında gerek soruşturma gerekse kovuşturma makamlarına konulan sınırlamalara "delil yasakları" adı verilmektedir[25]. Bu yasaklar; delillerin elde edilmesinde, öne sürülmesinde ve değerlendirilmesinde ortaya çıkmaktadır[26].

Delil yasakları konusunda CMK'daki düzenlemelerde bakıldığında 206 ncı maddede "kanuna aykırı", m.217'de "hukuka uygun", m.289'da ise "hukuka aykırı" usullerle delil ele geçirilmesinden söz edilmektedir. Yine CMK m.147'de yasaklı kılınan ifade ve sorgu usulleri de delil yasaklarının kapsamına alınmıştır[27].

2.1.1. Genel Olarak Delil Kavramı

Maddi gerçeğin meydana çıkarılması için, yargılamaya konu olan olayın açıklığa kavuşturulması amacıyla kullanılan ispat araçlarına delil adı verilmektedir. Delil, yargılama

---

4.4. sanı hafızasının ya da onun kavrama yeteneğinin.

5. Bu maddenin 4. fıkrasında ifade edilen yasaklar, mülakata ya da sorguya alınan kişinin onayına bağlı olmaksızın uygulanır.

6. Mülakat ya da sorguya alımın bu maddenin 4. fıkrasına aykırı bir şekilde uygulanması halinde, böyle bir mülakat ya da sorguya alım tutanağı kabul edilemezdir".

[24]Doracaku I Provimit te Jurisprudences, Kosova Cumhuriyeti, Priştine, 2016, s. 235.

[25] Timur Demirbaş, Soruşturma Evresinde Şüphelinin İfadesinin Alınması, Ankara 2011, s. 275; Fatih Birtek, AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat, Ankara 2017, s.291-296; Berrin Akbulut, Delil Değerlendirme Yasakları, Fasikül, Y: 2, S: 13, Aralık 2010, s. 6.

[26] Veli Özer Özbek, Ceza Muhakemesi Hukukunda Delil Yasakları, Alman Türk Karşılaştırmalı Ceza Hukuku, Cilt III, İstanbul 2010, s. 913.

[27]Gökcen- Çakır, s.2936.

makamlarının maddi olayı çözmek amacıyla başvurduğu, olayın sonucunu sabit görme ya da görmemesine yarayan araçlardır[28]. Başka bir deyişle delil, yargılama makamlarının ceza muhakemesi aşamalarında muhakeme konusu olaya ilişkin sonuca ulaşarak, maddi gerçeğin meydana çıkarılması için insan veya eşyadan elde edilebilen her çeşit ispat aracıdır[29].

Delillerin bazı niteliklere sahip olması gerekir. Deliller; elde edilebilir, ispat bakımından faydalı olmalı, gerçekçi, akılcı, temsil edici olmalı ve kanuna aykırı olmamalıdır[30]. Delil, ceza yargılamasında bir bulgunun konusu olan olguları öğrenme kaynağı olarak tanımlanmaktadır. Delil, önemli gerçeklerin doğruluğuna değinen belirli bir delil belgesinde yer alan herhangi bir ispat temeli veya nedenidir[31].

Hajdari, ceza yargılamasındaki delillerin, KCMK'deki kurallara uygun olarak elde edilen, suçun işlenip işlenmediğini gösteren, sebep olduğu sonuçları, sanığın suçu veya masumiyetini ve sorumluluğunun derecesini doğrulamaya yardım eden, suçla ilgili olay ve durum bildirimleri anlamına geldiğini ifade etmektedir.[32]

Delil, belirli bir davada suçluluk veya masumiyet belirlemenin bir yolu olarak, yasal şekilde mahkemeye sunulan bir şey olarak kabul edilir[33]. Ayrıca, delil, yasanın maddi varlıklar veya onların sahiplerini (insanlar, hayvanlar, bitkiler, nesneler, izler) kapsayan olgusal veriler anlamına gelmektedir. Bunların temelinde yürürlükteki yasalarca düzenlenen usulde, yetkili organ, cezai suçun mevcut olup olmadığını, belirli bir kişinin suçluluk şeklini ve esasa dayalı karar vermenin diğer önemli koşullarını tespit eder[34].

Bu kapsamda maddi deliller, cezai suç işlemenin aracı olarak kullanılan veya üzerinde izlerin bulunduğu ya da sanığın eylemlerinin nesnesi, suçun ürünü olan maddeler veya

---

[28] Ünver / Hakeri, s. 565-566.

[29]Birtek, s. 26.

[30] Nevzat Toroslu / Metin Feyzioğlu, Ceza Muhakemesi Hukuku, 21.Baskı, Savaş Yayınevi, Ankara 2021, s.201-204.

[31]Prof. Dr. Sc. HajrijaSijerçiq – ÇoliqMr. sc. Haris Haliloviq, asistentilartë E Drejta E ProcedurësPenale Me VështrımTëPosaçëmNëProcedurënPenaleTëKosovës, Priştine, 2007, s.99.

[32] Dr. AzemHajdARI, e DREJTA E ProceduresPenale, Priştine, 2010, s.188.

[33]Mr. Sc. Besim Arifi, Keqyrja e venditntengjarjes, 2012, s. 60.

[34]Dushko Modly, Teoritebashkekohorekriminalistike (Suvremenekriminalisticketeorije), perkthyerngaMustafReqica, Priştine, 2007, s. 120.

müsadere edilmesine izin verilen diğer mülkler ya da davanın koşullarını açıklığa kavuşturabilecek diğer herhangi bir araç veya öğedir[35].

[35]GentianTrenova, Interpretimegjyqesore te Kodit te ProceduresPenale te Shqiperise, BotimiDita, Tiran 2009, s.220; Arnavutluk Cumhuriyeti Genel Savcılığı, (Udhezuesipersekuestrimin e provavemateriale)bu belgeye göredelilolarak aşağıdakileri elde edebilir ve el koyabilir:

-cezai suç işlemenin aracı olarak görev yapan nesneler: bir silah; bir zehir dozu/miktarı; gizli şekilde insan, uyuşturucu ve kaçakçı mallar vb. taşıyan motorlu kara veya deniz taşıtları;

-suçun izlerinin bulunduğu nesneler: kan lekeleri, ateş faktörü ve ateşli silah hasarı içeren kurbanın giysileri veya otomobil; daktiloskopi vb. izlerin bulunduğu nesneler/cisimler;

- suçlu kişinin aktivitelerinin maddesi olan nesneler: çalınan nesneler vb.;

- cezai suçtan faydalanma maddesini oluşturan nesneler: suç faaliyeti, insan ve uyuşturucu kaçakçılığı, fuhuş, çalınan malların satılması aracılığıyla elde edilen gelirler ve nesneler, mali yükümlülüklerin ödenmemesi sonucu elde dilen gelirler vb. ve de;
- cezai suçla bağlantısı olan nesneler:davanın koşullarını açıklığa kavuşturmaya ve suçlunun belirlenmesi için yardımcı olan, failin/suç ortağının pasaportu veya fotoğrafları vb, bkz Udhezuesipersekuestrimin e provavemateriale, Arnavutluk Cumhuriyeti Genel Savcılığı, Tiran 2003, s. 3; Yine KCMK m.121 ön duruşmada ifade alınması öncesi toplanabilecek delillerin örnekleri şu şekilde verilmiştir: "Ön Duruşmada İfadenin Alınması Öncesinde Delillerin Alınması

1. Mümkün olduğu zamanlarda, devlet savcısı yasaya uygun olarak ön duruşmada ifadenin alınması öncesinde ilgili deliller olan tüm belgeleri alır. Bu tür belgeler aşağıdakileri kapsayıp sadece bunlarla sınırlı değildir;

1.1. pasaport, kimlik belgesi ya da gümrük giriş bilgileri;

1.2. finansal bilgileri;

1.3. takip bilgi veya fotoğrafları;

1.4. toprak sahiplik bilgileri;

1.5.araç sahiplik bilgileri;

1.6. ticari şirket veya oluşum bilgileri;

1.7. elektronik posta, metin mesajı veya fotoğraf gibi elektronik evraklar;

1.8. sağlık bilgileri;

1.9. notlar, günlükler veya takvimler; veya

1.10. işbu Ceza Muhakemeleri Kanunu uyarınca meşru bir şekilde alınan diğer belgeler.

2. Mümkün olması halinde, ön duruşmada ilgili ifadelerin alınması öncesinde devlet savcısı meşru bir şekilde tüm somut delilleri alır. Bu tür deliller aşağıdakileri kapsayıp sadece bunlarla sınırlı değildir:

2.1. olay yerinde temin edilen somut deliller;

2.2. sanık mekanlarının kontrolünden temin edilen somut deliller;

2.3. tutuklanması öncesi veya süresince sanığın kontrolünden elde edilen somut deliller;

2.4. somut delillerle ilgili olan fotoğraflar veya adli tıp raporları; veya

2.5. mevcudiyeti ve yapısı işbu Ceza Muhakemeleri Kanunu uyarınca soruşturma için önemli delilleri sağlayan, meşru bir şekilde elde edilen diğer her somut delil.

Ceza muhakemesinde kişiler, nesneler ve bazı eylemler ispat aracı olarak sunulmaktadır. Tüm ispat araçlarının ortak özelliği, yasa tarafından açıkça tanımlanmasıdır. İspat yöntemleri ile ilgili olarak, bu kurallar da dikkate alınmalıdır: 1.Tüm kanıt araçları delildir. Fakat bir eşyanın delil olması ve delil şeklinde kabulü farklı kavramlarıdır. Herhangi bir veriyi doğrudan delil kabul etmek ceza yargılamalarında delillerin kabulünde potansiyel bir keyfilik riski getirir; 2. Sanığın ifadesini sahtekârlık veya aldatmaca ile elde etme durumunda olduğu gibi delil olan nesnelerinin ele alınmasında, özellikle de bir sanıktan veya tanıktan ifade almakla ilgili yeni deliller söz konusu olduğunda, kullanım sırasında ortaya çıkan bazı yasal sınırlamaları da göz önünde bulundurularak, sanığın bir beyanda bulunması için şiddet, yıldırma ve diğer araçların kullanımına ilişkin geleneksel yasaklara da uyulmalıdır[36].

Türk hukukunda 1983 yılında yürürlüğe gire "*Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik*"e (PAGY) göre delil, işlenen bir suçun aydınlatılması ve sanıkların belirlenmesine yarayan tüm ispat araçlarını ifade etmektedir. Maddi delil ise suç itirafı ve tanıklık haricinde kalan sanıklarla ilgili maddi bir yapısı olan , canlı veya cansız şeylerdir[37].

5271 sayılı CMK'da; tüm maddi deliller yanında ileri düzenlemelere yer verilmiş olup, şüpheli, sanık ve başka kişilerin beden muayenesi ve vücudundan örnek alınması, genetik incelemeler, fizik kimliğin tespiti (m. 75 vd.) gibi iz bilimini soruşturma ve kovuşturma makamlarının emrine vermiştir[38].

2.1.2. Adli Bilimler Açısından Delilin Anlamı

Adli bilimler, çok ayrıntılı bir şekilde maddi izler ve delillerle ilgilenir. Balistik, Grafoloji, Traseoloji, Daktiloskopi vb. adli bilimler, farklı izleri çok özel bir şekilde ele alır ve izlemenin yolunu, onların anlamlarını veya yorumlarını belirler, ki bunlar yeterli incelemeden sonra delil yetkisi alırlar ve daha sonra ceza yargılamasında ele alınan diğer delillerin ayrılmaz bir parçası olurlar. Bu kapsamda inceleyecek olursak:

---

[36]Doracaku I Provimit te Jurisprudences, Kosova Cumhuriyeti, 2016, s.234.

[37]Gökcen- Çakır, s.2919.

[38] Oğuz Polat, Kriminoloji ve Kriminalistik Üzerine Notlar, Suç-Suçlu-Suç Yeri, 1. Baskı, Ankara 2004, s. 339 vd.; Mustafa Kaygısız, Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği, Ankara 2010, s. 42 vd.; Gökcen- Çakır, s.2920.

İz, faili tespit etmeye veya belirli bireysel durumları tespit etmeye yardımcı olabilecek bir insan, hayvan, nesne veya araç bırakan herhangi bir şeydir. İzler, bizi faillere götüren olay ve gerçeğin bilinebileceğinin işaretleridir.[39]

"İz" kelimesi Fransızca "le trace" kelimesinden türetilmiştir. Bu kelimeye bilim veya çalışma anlamına gelen logos kelimesi eklenir ve her ikisi de Traseoloji bilimi olarak da adlandırılan izler üzerinde araştırma yapar. Traseoloji, belirli bir dış yapıya sahip nesnelerin bıraktığı izleri inceleyen bir adli bilimler dalıdır[40].

İz oluşturmadan bahsedildiğinde, izi bırakan nesne veya araç ve de alıcı nesnenin söz konusu olduğu gerçeği de dikkate alınmalıdır. Böylece, iz bırakan nesnenin, alıcı nesne üzerindeki dinamik eylemi söz konusu olmakta ve izin yaratılmasına neden olunmaktadır. Bu durumda alet izlerinin bırakılmasını ele alabiliriz. Belirli bir nesne, diğer bir yüzey ile temasa geçtiğinde aynısı o yüzeyde iz bırakmaktadır. Bu iz bırakma, o durumda kullanılan nesnenin dinamik eylemi sonucu ortaya çıkmaktadır.[41]

Olay yerindeki izler aşağıdaki gibi çeşitli şekillerde sunulmaktadır:

1. Geçici izler (koku, sıcaklık, lekeler vb. gibi geçici izler);
2. Özel izler (özel örnekli olan);
3. Şartlı izler (ışık, duman, yangın, pozisyon, vb.), ve
4. Temas izleri (kişiler ve nesneler arasındaki fiziki temas sonucu ortaya çıkan).[42]

Delil olarak kullanılabilecek çeşitli izler, modern ekipman kullanarak iyi eğitimli personel tarafından profesyonel olarak olay yerinde, fail üzerinde, mağdurun bedeninde (cesedinde) ve eşyalarında, suç işlerken kullanılan nesnelerde (araçlarda) ve de cezai suçun planlandığı yer, şüphelinin suçun işlenmesinden sonraki çalınan eşyaları veya suçu işlediği araçları bırakmak için kullandığı yer gibi suçla ilgili diğer yerlerde aranmalıdır.[43]

---

[39]Mr.Sc. Besim Arifi, Keqyrja e vendit te ngjarjes, sayfa 85, Sayı I, Priştine 2012, Priştine, 2012, s.85.

[40] Dr. Vesel Latifi, Kriminalistika, zbulimidhe te provuarit e krimit, Priştine, 2009, s.366.

[41] Arifi, s.85.

[42] Henry C. Lee, Materijalnitragovi (Materyal İzler), Zagreb, 1998, s.3.

[43] Arifi, s.92-94.

2.1.3. Delilin Yasal Açıdan Anlamı

Kuşkusuz, her zaman bir mahkeme kararıyla sona eren kovuşturma safhasında kanıtlama süreci, önemli bir yere sahiptir. Bu nedenle, cezai takibata ilişkin hukuki düzenlemeler yapılırken kanıtlama/tartışma süreci ve genel olarak deliller için gerçekleri kanıtlamak için delil sunumu, tespiti ve kullanımı ile ilgili usuller oluşturulmalıdır[44].

Ceza muhakemesinde gerçeklerin ortaya çıkarılmasında kullanılan bulgular, cezai muhakeme boyunca işleme tabi tutulur. Onlar aracılığıyla, ceza davasının fiili ve hukuki çözümüne ilişkin cezai ve usuli hukuki gerçekleri teyit edilir.

Ceza muhakemesinde, olaya ilişkin gerçeklerin belirlendiği çeşitli delillerle karşılaşmaktayız. Cezai-hukuki anlamda delil ise aslında, ceza yargılamalarının konusunu oluşturan fiil ve olaylar hakkında bilgi kaynağı oluşturur. İsnat konusu fiilin varlığı ya da yokluğu veya ne şekilde oluştuğu hakkında yani ispatı söz konusu bilgi kaynağı irdelenmek suretiyle bir kanaate ulaşılır. İspat kavramı üç unsurdan oluşur: 1) Delil nesnesi (themaprobandi); 2) Delil temeli (argumentumprobatio) ve 3) kanıtlayıcı araç (mediaprobatio). Delil nesnesi, kanıtlanması gereken bir gerçektir. Delil nesnesi; delil temelinden kanıtlanırken, delil aracı delil temelinin elde edildiği kaynaktır. Dolayısıyla, sanık cinayet suçundan yargılanırsa, delil amacı, diğer kişiyi tabanca ile vurarak sanığın onu hayatından mahrum etmesidir. Bu gerçek, diğerlerin yanı sıra, sanığın ifadesi veya sanığın kurbanı silahla nasıl vurduğunu gören tanıkların ifadesiyle doğrulanabilir. Bu durumda, şüpheli ya da sanığın beyanı ifadesi ve tanığın beyanı delil temelini oluşturur. Bu arada, sanık, delil aracı olarak suçlamanın kaynağı ve tanık delilinin kaynağıdır. Başka bir deyişle, araçlar, delil nesnesinin kanıtlandığı kanıtlayıcı temelin kaynağıdır. Delil temelinin daha fazla olması ve delil araçlarının sınırlamasının bulunması sebebiyle delil temeli ve delil aracı arasında niceliksel uyum yoktur. Bu durumda, yargılama sürecinin daha fazla kanıt toplaması olduğu anlamına gelir.[45]

Türk hukukunda ispat kavramı, masumiyet karinesi ile yakından ilgili şekilde ele alınmıştır. Sanık, atılı suçu işlediğine ilişkin her türlü şüphe ortadan kaldırılmadığında sanık mahkûm

[44]EjupSahiti, RexhepMurati, E drejta e procedurespenale (Ceza Muhakemesi Kanunu), Priştine, 2016, s.226.

[45]Sahiti / Murati, s.230.

edilemeyecektir[46]. Hâkimin mahkûmiyet kararı verebilmesi için, maddi olaya ilişkin vicdani kanaatinin gerçekleşmesi gerekmektedir. Vicdani kanaat ise delil sistemi içerisinde yer almaktadır. Vicdani delil sistemi ise, gerek delil serbestliği gerekse delillerin ele alınmasındaki serbestliği kapsar. Delillerin serbest şekilde hakimce takdir edilmesi, hâkimin ispat kurallarıyla başka bir deyişle hangi koşullara göre bir olayın sabit kabul edileceği hususundaki düzenlemelerle bağlı olmamasıdır. Yargılama sırasında ortaya çıkacak bir inanç ya da zan yeterli olmayıp, hâkim tam bir vicdani kanaate ulaşmalıdır[47].

Uyuşmazlığın çözümünün birinci aşaması, yani ispat sorunu sanık aleyhine neticelendiğinde, başka bir deyişle eylem sabit kabul edildiğinde, hâkim ikinci safhada bu eylemin hukuki vasıflandırmasını yapar ve cezayı tayin eder. Eylemin sanık tarafından işlenip işlenmediğinin sabit olmadığı hallerde ikinci aşamaya geçilmeden sanık lehine (beraat) karar verilir[48]. İspat külfeti, iddianame ile ceza davasını mahkeme önünde açan iddia makamından beklenmektedir ve savcı, iddiasını ispatlamalıdır[49].

2.1.4. Delillerin Yasallığı İlkesi

Soruşturma aşamasında sağlanan tüm deliller ve hatta yargılama sırasında sunulan herhangi bir delil, yasal düzenlemelere tam olarak uygun şekilde sağlanmalı ve elde edilmelidir. Kanun hükümlerine aykırı olarak düzenlenen delillerin kabul edilemez delil[50] olarak değerlendirilmesi, bu delillerin dava dosyasından ayrılması ve mahkemenin hiçbir şekilde kabul edilemez delillere dayanarak kesin bir karar vermemesi gerekmektedir[51].

---

[46] Yalçın Şahinkaya, İnsan Hakları Avrupa Mahkemesi Kararlarında ve Türk Hukukunda Suçsuzluk Karinesi, Seçkin Yayınevi, Ankara 2008, s. 204.

[47] Faruk Turhan, Ceza Muhakemesi Hukuku, Asil Yayınevi, Ankara 2006, s. 152-153.

[48] Erdener Yurtcan, Ceza Yargılaması Hukuku, 8. Baskı, Melisa Matbaacılık, İstanbul 2002, s. 273

[49] Metin Feyzioğlu, Ceza Muhakemesinde Vicdani Kanaat, Yetkin Yayınevi, Ankara 2002, s.160.

[50] Feridun Yenisey/ Ayşe Nuhoğlu, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Güncellenmiş 9.Baskı, Ankara 2021, s. 548; Bahri Öztürk, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Güncellenmiş 14.Baskı, Ankara 2020, s. 399; Cumhur Şahin,/ Neslihan Göktürk, Ceza Muhakemesi Hukuku Temel Hukuk Dizisi, 3. Baskı, Seçkin Yayıncılık, Ankara, 2020, s.206; Ali Eryılmaz, Ceza ve Disiplin Hukukunda Hukuka Aykırı Delil, Ankara 2013, s. 105.

[51] KCMK m.10/3: "Davada yer alan sanık ya da bir diğer kişiden, işkenceyle, zorla, gözdağı vererek veya uyuşturucu altında ya da diğer benzeri eylemlerle zorla suçluluğun veya herhangi bir diğer beyanatı kabul ettirmesi yasaktır ve bunlar aleyhinde cezalandırılır".,
KCMK m.257'de hukuka aykırı delile ilişkin düzenlemeye yer verilmiştir: "Delillere İlişkin Genel Kurallar

Kosova Ceza Muhakemesi Kanunu m.105 ve devamı maddeleri uyarınca muhafaza altına alma tedbirinin (kontrolün)[52] uygulanması sırasında delil toplama kurallarının, gizli teknik soruşturma ve gözetim önlemlerinin uygulanmasından delil sağlarken sınırlamaların, tanıkların, mağdurların ve sanıkların ifadelerinin nasıl alınması gerektiği ve diğer yasal

---

1. Bu madde ile öngörülen delil kuralları, mahkeme huzurunda tüm ceza muhakemelerinde uygulanır ve işbu Kanunun öngördüğü durumlarda, bunlar aynı zamanda devlet savcısı ve polis huzurunda da uygulanır.

2. Ceza muhakemeleri hükümlerinin ihlal edilmesiyle alınan deliller, işbu Kanunun ya da yasanın diğer hükümlerinin açık bir şekilde öngörmesi durumunda, kabul edilemezdir.

3. Mahkeme, kabul edilemez delillere kendi kararını bağlayamaz.

4. Yapılan her mülakat ya da sorguya alım esnasında aşağıdakiler yasaktır:

4.1. kendi görüşünü formüle etmesi ve ifade etmesi için sanığın özgürlüğüne kötü muamele, neden olunan yorgunluk, fiziksel müdahale, uyuşturucu kullanımı, şiddet, zorlama ya da hipnoz aracılığıyla etki etmek;

4.2. yasa ile yasaklanan ölçülerde sanığın tehdit edilmesi;

4.3. yasa ile öngörülmeyen herhangi bir kazancın vaat edilmesi; ve

4.4. sanı hafızasının ya da onun kavrama yeteneğinin.

5. Bu maddenin 4. fıkrasında ifade edilen yasaklar, mülakata ya da sorguya alınan kişinin onayına bağlı olmaksızın uygulanır.

6. Mülakat ya da sorguya alımın bu maddenin 4. fıkrasına aykırı bir şekilde uygulanması halinde, böyle bir mülakat ya da sorguya alım tutanağı kabul edilemezdir".

"İfade alma ve sorguda yasak usuller" başlıklı 5271 sayılı CMK m 148 şu şekildedir: "– (1) Şüphelinin ve sanığın beyanı özgür iradesine dayanmalıdır. Bunu engelleyici nitelikte kötü davranma, işkence, ilâç verme, yorma, aldatma, cebir veya tehditte bulunma, bazı araçları kullanma gibi bedensel veya ruhsal müdahaleler yapılamaz. (2) Kanuna aykırı bir yarar vaat edilemez. (3) Yasak usullerle elde edilen ifadeler rıza ile verilmiş olsa da delil olarak değerlendirilemez. (4) Müdafi hazır bulunmaksızın kollukça alınan ifade, hâkim veya mahkeme huzurunda şüpheli veya sanık tarafından doğrulanmadıkça hükme esas alınamaz. (5) Şüphelinin aynı olayla ilgili olarak yeniden ifadesinin alınması ihtiyacı ortaya çıktığında, bu işlem ancak Cumhuriyet savcısı tarafından yapılabilir.

Yine kanuna aykırı delillerin yargılamada kullanılamayacağına dair 5271 sayılı CMK m206 şu şekildedir: "(1) Sanığın sorguya çekilmesinden sonra delillerin ortaya konulmasına başlanır. (Ek cümleler: 25/5/2005 - 5353/29 md.) Ancak, sanığın tebligata rağmen mazeretsiz olarak gelmemesi sebebiyle sorgusunun yapılamamış olması, delillerin ortaya konulmasına engel olmaz. Ortaya konulan deliller, sonradan gelen sanığa bildirilir. (2) Ortaya konulması istenilen bir delil aşağıda yazılı hâllerde reddolunur: a) Delil, kanuna aykırı olarak elde edilmişse. b) Delil ile ispat edilmek istenilen olayın karara etkisi yoksa. c) İstem, sadece davayı uzatmak maksadıyla yapılmışsa."

[52]5271 sayılı CMK m.123'de ispat aracı olan eşya ve kazancın "muhafaza altına alınması" olarak tanımlanan kurum, KCMK'da "kontrol" olarak tanımlanmıştır. Kontrolde esas olan şüpheli veya sanığın kendi mülkiyetinde olan eşyayı, gönüllü şekilde işlemi yapan görevlilere devretmektedir. Şüpheli onay vermediği takdirde bu eşyaya el konulamaz (KCMK m.105/1-2). Ancak bu durumda ön duruşma hakiminden ilgili yerde kontrol yapılması kararı alınır (KCMK m.105/3). KCMK'de "arama" kavramı açıkça düzenlenmemiştir. KCMK m.105/3'de şüphelinin kontrole rıza göstermemeis halinde ön duruşma hakimi kararı ile şüphelinin evi ve diğer mekanlarında kontrol yapılması, CMK 116 ve devamı maddelerinde düzenlenen arama ve el koyma gibidir.

kısıtlamaların açıkça belirlendiği, çeşitli delillerin sağlanmasına ilişkin bazı katı kısıtlamalar içerir. Bu kısıtlamalara uyulmadıkça deliller, kabul edilemez olacaktır.

Türk hukukunda da Anayasanın 38/6. maddesine yasaya aykırı şekilde ele geçirilmiş delil ve bulgular, delil şeklinde kabul edilemeyecektir. Yine CMK uyarınca delil, yasaya aykırı şekilde ele geçirilmişse reddedilir (m.206/2-a). Başka bir deyişle bu düzenlemeler, hukuka aykırı delilin dosyaya girmesine olanak vermemektedir[53]. Ancak dosyaya giren ve hâkimin vicdani kanaatini etkileme olasılığı bulunan hukuka aykırı delilin de, hukuka aykırı olup olmadığını denetlemek için dosyada tutulması gerektiği ileri sürülmüştür[54].

Ceza muhakemesinde delillerin toplanması sırasında ortaya çıkabilecek yasal eksiklikler, muhakemenin taraflarınca ileri sürülmeli ve yargılamanın her aşamasında mahkeme delillerin hukuka uygunluğunu değerlendirmelidir. Bununla birlikte, KCMK hükümlerine göre, delil toplamanın hukuka uygunluğunu değerlendirmek için erken aşamalardan itibaren bazı usuli işlemler öngörülmektedir. Bu işlemler, özellikle teknik soruşturma ve koruma tedbirlerinin uygulanmasıyla sağlanan delillerle ilgilidir ve bu delillerin alınmasından hemen sonra, yapılan işlemin yasallığını değerlendirmek gerekli olabilir.

Kosova Ceza Muhakemesi Kanunu[55], bu tür hukuka aykırı elde edilmiş delillere ilişkin olarak yargılama aşamasına dair de hükümler getirmiştir:

1. Bu bölümdeki tedbir yoluyla elde edilen delil, tedbir kararı ve uygulanmasının hukuka aykırı olması halinde kabul edilemez.

2. Özel yerlerdeki konuşmaların gizlice izlenmesinden, posta teslimatlarının kontrolü, aramaların dinlenmesi, bilgisayar ağı üzerinden iletişimin dinlenmesinden, posta, gönderilerinin kontrollü teslimatından, konum izleme araçlarına dair teçhizatların kullanımı, herhangi bir nesne satışının muvazaası, bir rüşvetçilik eyleminin uydurulması ya

[53]Gökcen- Çakır, s.2943; Adli Kolluk Yönetmeliği m.6/8'e göre de adlî kolluk görevlileri, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, Cumhuriyet savcısının emirleri doğrultusunda şüphelinin lehine veya aleyhine olan tüm delilleri, kanunda öngörülen koşullara uyarak toplamak, muhafaza altına almak ve bunları bir fezleke ile Cumhuriyet savcısına sunmakla yükümlüdür. Hukuka aykırı delil elde edildiğinin tespiti hâlinde, fezlekede bu hususa da yer verilir.

[54]Gökcen- Çakır, s.2944

[55]Kosova Ceza Muhakemesi Kanunu, Madde 97.

da gizli soruşturmadan elde edilen delillere, sadece bu Kanunun 88. maddesinin 3. paragrafında tanımlanan cezai suçla ilgili cezai işlemlerde izin verilir.

3. İddianamenin okunmasının ardından, ikinci oturumdan önce itiraz edilmesi halinde, tek duruşma hakimi veya duruşmaya başkanlık eden yargıç, sanığın toplanan delillerin kabul edilebilirliğine ilişkin itirazlarını değerlendirir. Bu fıkrada belirtilen itiraza ilişkin karara karşı temyiz yoluna gidilebilir.

4. Nihai mahkeme kararı verilmeden önceki tüm süreçlerde, tek yargı hakimi veya mahkeme heyeti başkanı, resmi görevi icabı, maddi delil ve olguların yasadışı bir şekilde toplanıp toplanmadığına dair belirtilerin mevcut olması halinde sanığın anayasal haklarının ihlal edilmesine ilişkin işbu Kanun 88.[56] maddesi kapsamında belirtilen toplanmış malzemelerin kabul edilebilirliğini gözden geçirebilir.

---

[56] KCMK Madde 88:

"Takip ve Soruşturma Gizli ve Teknik Önlemleri

1. Fotoğraf ya da videoyla gizli takip, kamuya açık yerlerde konuşmaların gizlice dinlenmesi, telefon çağrılarının kaydedilmesi ya da finansal bilgilerin tespit edilmesi, aşağıdaki durumlarda bir kişi veya belirli bir yer aleyhine emredilebilir:

1.1. resen kovuşturulan suç işlemi için bir kullanıldığına ya da ilgili kişinin suçu işlediğine dair esasa dayalı şüphenin bulunması veya suç girişiminin cezalandırıldığı durumlarda resen kovuşturulan suç işleminde bulunması; ve

1.2. emredilen önlemlerden alınabilecek bilginin suç işleminin soruşturulmasına yardım etme ihtimalinin bulunması ve diğerleri için gereksiz zorluk ya da olası tehlike oluşturmadan diğer soruşturma tedbirlerinin alınma imkanının bulunmaması.

2. Telefon konuşmalarının kaydedilmesi ya da finansal bilgilerin tespit edilmesi, aynı şekilde şüpheli haricindeki kişiler aleyhine, bu maddenin 1. fıkrası 1.1. bendindeki koşulun şüpheli için geçerli olduğu ve bu maddenin 1. fıkrası 1.2. bendindeki önkoşulun yerine getirildiği ve aşağıdakilere dair esas dayalı şüphenin bulunması durumda emredilebilir:

2.1. ilgili kişinin şüpheliden kaynaklanan ya da şüpheliye özel iletişimleri kabul etmesi ya da yayınlaması veya şüphelinin finansal işlemlerinde yer alması; veya

2.2. şüpheli ilgili bu kişinin telefonunu kullanması.

3. Özel mekanlarda konuşmaların gizlice dinlenmesi, posta gönderilerinin kontrol edilmesi, telekomünikasyonların dinlenmesi, bilgisayar şebekesi yardımıyla telekomünikasyonlara müdahale edilmesi, posta gönderilerinin kontrollü gönderilmesi, bulunma yerinin tespit edilmesi için araçların kullanılması, herhangi bir nesnenin muvazaadan satın alımı, bir rüşvetçilik eyleminin uydurulması ya da gizli soruşturma, aşağıdaki durumlarda bir kişi, yer veya somut bir nesne aleyhine emredilebilir:

3.1. böyle bir yer veya nesnenin suç işlemi için kullanıldığına dair esasa dayalı şüphenin mevcut olması veya böyle bir kişinin suçu işlemesi ya da suç girişiminin cezalandırıldığı durumlarda işbu Kanunun 90. maddesinde belirtilen suç işlemi girişiminde bulunması;

5. Emrin veya onun uygulamasının yasadışı oluşuna ilişkin mahkeme kararının nihai hal alması halinde, usulü yöneten tek yargı hâkimi veya mahkeme heyeti başkanı, toplanan tüm malzemeleri tutanaktan kaldırır ve bu tür malzemeleri, tazminat kararına dair asliye mahkemesi başkanı aracılığıyla Takip ve Soruşturma Değerlendirme Mahkemesine[57] gönderir. KCMK m.98'e göre Takip ve Soruşturma Değerlendirme Mahkemesi, 2003 tarihli KCMK'da da yer alan (m.258), üç hâkimden oluşan, soruşturma aşamasında iletişimin denetlenmesi başta olmak üzere koruma tedbirleri ve diğer soruşturma işlemlerinden zarar görenlerin tazminat taleplerine bakmak için kurulmuş bir mahkemedir[58].

Gizli teknik soruşturma ve gözlem önlemlerinin uygulanmasıyla sağlanan delillerin yasallığı konusunda şüphenin olduğu her durumda, taraflar, yargılamanın yapıldığı mahkemedeki Soruşturma ve Gözlem Heyeti'ne başvurabilirler. Özel davalar için yetkili mahkeme hâkimleri tarafından oluşturulan bu heyet, davayı incelemeli ve tarafların talebi üzerine, gizli teknik soruşturma ve gözlem tedbirlerinin uygulanmasıyla sağlanan delillerin hukuka uygunluğu hakkında karar vermelidir ve bu, yargılamanın ilk aşamalarında kabul edilemez delilleri ortadan kaldırmak için yapılır.

Takip ve Soruşturma Değerlendirme Mahkemesi'nin görevleri KCMK m.98'e göre şu şekildedir:

3.2. emredilen önlemlerden alınabilecek bilginin suç işleminin soruşturulmasına yardım etme ihtimalinin bulunması ve diğerleri için gereksiz zorluk ya da olası tehlike oluşturmadan diğer soruşturma tedbirlerinin alınma imkanının bulunmaması.

4. Posta gönderilerinin kontrol edilmesi, telekomünikasyonların dinlenmesi ya da iletişimlerin bilgisayar şebekesi aracılığıyla dinlenmesi, aynı şekilde şüpheli haricindeki kişiler aleyhine, bu maddenin 3. fıkrası 3.1. bendindeki koşulun şüpheli için geçerli olduğu ve bu maddenin 3. fıkrası 3.2. bendindeki önkoşulun yerine getirildiği ve aşağıdakilere dair esas dayalı şüphenin bulunması durumda emredilebilir:

4.1. böyle bir kişinin şüpheliden kaynaklanan ya da şüpheliye özel iletişimleri kabul etmesi ya da yayınlaması veya şüphelinin finansal işlemlerinde yer alması; veya

4.2. şüpheli ilgili bu kişinin telefonunu kullanması ya da bilgisayar sistemine erişimi bulunması".

[57]Bu Mahkeme, 5271 sayılı CMK m.141 ve devamında koruma tedbirleri dahil soruşturma işlemlerinden zarar görenlerin dava açtıkları bir mahkeme olup, Türk hukukunda CMK m.141 ve devamı maddelerinde koruma tedbirlerinden zarar görenlerin ağır ceza mahkemesine açması usulüne benzemektedir, bkz. Rexhep Murati, Protection of Human Rights under Kosovo's Criminal Code and Criminal Procedure Code, Chicago Kent-Law Review, 80 (1), 2004, s.111, 114.

[58]Murati, s.99, 114.

"*1.1. bu bölüm kapsamındaki önleme ya da önlem emriyle ilgili olan, bu maddenin 5. fıkrası kapsamında uyarınca yapılan itiraza dair karar alır ve ilgili tazminat hakkında karar verir; veya*

1.2. Emrin veya onun uygulamasının yasadışı olduğuyla ilgili olarak, hâkimin işbu Kanunun 97. maddesi 3. fıkrası uyarınca nihai mahkeme kararı alması halinde, bu bölüm uyarınca emre tabi olan kişi ya da kişilere tazminat verilmesi hakkında karar alır.

2. Takip ve Soruşturma Değerlendirme Mahkemesi, işbu Kanunun 97. Maddesi 3. Fıkrasında belirtilen somut bir mahkeme kararına karşı somut bir itiraz ya da tazminat hakkında karar alması için asliye mahkemesi başkanı tarafından tayin edilecek üç hâkimden oluşur. Takip ve Soruşturma Değerlendirme Mahkemesi üyelerinden hiçbiri, itiraza tabi olan kişiyle ya da işbu Kanunun 97. maddesinin 3. fıkrasında belirtilen mahkeme kararına tabi olan toplanmış maddi delil ve olgularla profesyonel anlamda ilişkisi olmamalıdır.

3. Yetkili polis görevlileri ve devlet savcıları, Takip ve Soruşturma Değerlendirme Mahkemesine, kendi görevlerini yerine getirmesi için bu mahkemenin isteyebileceği evrakları temin ederken, ilaveten bu mahkemenin talebi üzerine, sözlü beyanatları da temin eder.

4. Esasına göre, önlem emrinin ya da onun uygulanmasının bu bölüm kapsamında yasadışı olduğu yönündeki mahkeme kararının nihai hal alması ardından, böyle bir mahkeme kararı Takip ve Soruşturma Değerlendirme Mahkemesi için bağlayıcıdır.

5. Kişi, bu bölüm çerçevesinde yasadışı bir önleme ya da bu bölüm kapsamındaki bir önleme dair yasadışı bir emre tabi olduğunu değerlendirmesi durumunda, kendisi, herhangi bir yasal ihlalin mevcut olduğunu iddia etmesi halinde, karar alması için Takip ve Soruşturma Değerlendirme Mahkemesini tayin eden asliye mahkemesi başkanına itirazda bulunabilir.

6. İtiraz hakkında karar alma durumunda, Takip ve Soruşturma Değerlendirme Mahkemesinin bu bölüm kapsamındaki önlemin yasadışı olduğu ya da böyle bir önleme dair emrin yasadışı olduğunu belirlemesi halinde, aşağıdaki şekilde karar alabilir:

6.1. halen yürürlükte olması halinde durdurmak;

6.2. toplanan malzemelerin yok edilmesini emretmek; ve

6.3. emre tabi olan kişi veya kişileri tazmin etmek."[59]

Ceza muhakemesi sırasında, sırasıyla asıl yargılama başlamadan önce, Savcılık tarafından asıl yargılama için sunulan ve önerilen tüm delillerin hukuka uygunluğu bir kez daha değerlendirilecektir. Sanık ve müdafii, tek hâkime veya mahkeme başkanına delillerin değerlendirilmesi ve onların yasallığı için talep yazma hakkına sahiptir ve mahkeme delillerin yasaya aykırı olarak elde edildiğini tespit ederse iddianameyi reddedebilir.

1. Asıl duruşma öncesinde, sanık aşağıdaki nedenlere dayanarak iddianame kapsamındaki belirli delillere karşı itiraz başvurusunda bulunabilir:

1.1. delillerin polis, devlet savcısı ya da diğer devlet organı tarafından meşru bir şekilde alınmamış olması;

1.2. delillerin işbu Kanunun XVI. Bölümü kapsamındaki kurallara aykırı olması; veya

1.3. mahkemenin delilleri esasen savunulamaz olarak değerlendirmeye dair açıkça ifade edilebilir esaslarının bulunması.

2. Devlet savcısına, itiraza sözlü ya da yazılı olarak yanıt verme imkânı verilmek zorundadır.

3. İtirazın yapıldığı tüm deliller için, tek yargı hâkimi ya da mahkeme heyeti başkanı delilin izin verilmesi ya da hariç tutulmasına ilişkin yazılı gerekçeli karar alır.

4. Kabul edilemez deliller, yazılarda ayrı tutulur ve kapatılır. Bu tür deliller, mahkeme tarafından yazılardan ve diğer delillerden ayrı tutulur. Kabul edilemez deliller, kabul edilebilirliğe ilişkin mahkeme kararına karşı itiraz durumları haricinde, ceza usulünde gözden geçirilemez ya da kullanılamaz.

5. Aleyhine itirazın yapılmadığı tüm deliller, belirli bir delilin kabul edilebilirliğinin Kosova Cumhuriyeti Anayasası ile garanti edilen sanık haklarını tehlikeye atacağını re'sen belirlemesi haricinde, adli incelemede kabul edilebilir delildir.

[59]Kosova Ceza Muhakemesi Kanunu, Madde 98.

6. Her taraf, bu maddenin 3. fıkrası kapsamında belirtilen mahkeme kararına karşı itirazda bulunabilir. İtiraz, yazılı mahkeme kararının kabul edilmesinden sonraki beş (5) gün içerisinde yapılmak zorundadır.[60]

Mahkeme, delillerin hukuka aykırı olarak elde edildiğini tespit ederse, bir karar verir ve bu delili dava dosyasından ayırır ve hiçbir şekilde yargılamanın hiçbir aşamasında herhangi bir taraf bu delilleri kullanamaz. Bu, taraflar için daha fazla güvenlik sağlar ve devlet kurumları tarafından ihmal ve hatta suiistimal olasılığını büyük ölçüde sınırlar.

Türk hukukunda dayasak ifade ve sorgu yöntemleri delil yasaklarının kapsamına alınmıştır (CMK m. 148/3-4, 75/1, 76/1). Yine ortaya konulacak bir delil, yasaya aykırı şekilde ele geçirilmişse reddolunacaktır (CMK m.206/2-a). Ayrıca, failie atılı suç, hukuki biçimde ele geçirilmiş delillerle ispatlanmalıdır (CMK m.217/2). Kararın hukuka aykırı usullerle elde edilen delillere dayanması da kesin hukuka aykırılık hali olarak kabul edilip temyiz nedeni olarak gösterilmiştir (CMK m.289/1-i)[61].

2.1.5. Delil Türleri

Ceza muhakemesinde delillerin çok önemli rolü vardır ve maddi gerçekliğe onlar üzerinden somut gerçekler onlar üzerinden doğrulanır. Sadece bu şekilde bir kişinin suçlu olup olmadığı belirlenebilir. Cezai suçun soruşturması kapsamında, muhakeme usulünün değişik aşamalarında, muhakeme kurumları olarak devlet kurumları çeşitli deliller talep eder, toplar ve sorumlu mahkemeye sunar.

İşlenmiş olan suçun türüne ya da suçun işlenmesinde kullanılan araçlara bağlı olarak, olay yerinde veya başka yerlerde çeşitli delil türleri elde edilir veya toplanır. Ayrıca, mağdurun kendisinin bile bir şekilde farklı delil türleri ürettiği veya büyük bir kaynak oluşturduğunu belirtmek gerekir.

Deliller, fiziksel biçimlerine, elde edilme şekillerine, bunları sağlayan ve toplayan makama ve aynı zamanda önleyici önem veya değerlerine bağlı olarak birkaç türe veya gruba ayrılır. Ceza hukuku araştırmalarına ve aynı zamanda adli bilimler araştırmalarına katılan farklı

[60]Neni 248 I Kodit te Procedures Penale te Kosoves

[61]Gökcen- Çakır, s.2933, 2936, 2940,

akademisyenler, delil türleri ve onların farklı türlere veya gruplara bölünmeleri hakkında görüş bildirmişlerdir[62].

Tomaseviç, delillerin çeşitleri ve sınıflandırılması hakkında konuşurken, bunları öncelikle maddi veya gerçek delillerin ile kişisel veya bireysel deliller olarak sınıflandırır. Maddi deliller, muhakemedeki gerçekleri (örneğin belgeler, teknik kayıtlar, cezai suçun izleri, suçun işlendiği araçlar, parmak izleri vb.) kanıtlayan nesneler iken, kişisel kanıtlar, kanıt araçları olarak sunulan kişilerin ifadelerinden oluşmaktadır[63]

Başka bir kanıt ayrımı da, bu kanıtları kimin önerdiğini ve sunduğunu ve de bu delillerle ne iddia edildiği, yani suçlama delilleri ve savunma delilleri şeklinde olabilir. Kosova hukukunda iddia makamı tarafından sunulan deliller aracılığıyla suçun kanıtlanması amaçlanırken, savunma tarafından sunulan deliller ile sanığın masumiyeti kanıtlanması hedeflenir. Deliller, suçlama ve savunma delillerine, sonradan ise doğrudan ve dolaylı delillere, orijinal ve türetilmiş delillere, kişisel ve maddi delillere ve eksiksiz ve eksik delillere ayrılmıştır.[64]

Yukarıda da belirtildiği gibi doğrudan delil, tartışmalı bir gerçeğin varlığını veya var olmayışını doğrudan kanıtlayan delil olarak kabul edilir. Örneğin doğrudan bir suçun işlendiğine tanık olan bir görgü tanığının ifadesi, doğrudan delil olarak kabul edilir. Ayrıca, gösterge olarak adlandırılan dolaylı deliller, tartışmalı gerçeğin dolaylı olarak doğrulanmasına katkıda bulunur[65].

2.1.5.1. Beyan Delili

Bir suçun işlenmesi halinde, ilgili taraflar olarak, suçun faili veya failleri, cezai suçun mağdurları, olay hakkında doğrudan veya dolaylı bilgi sahibi olan kişiler bulunmaktadır. Ceza muhakemesinin farklı aşamalarında tüm bu kişiler, olayın en iyi ve mümkün olduğunca doğru bir şekilde açıklığa kavuşturulması için ifade vermelidir. Bu kişilere ek

---

[62] Prof. dr.sc. HajrijaSijerçiq – ÇoliqMr. sc. Haris Haliloviq, asistentilartë E DREJTA E PROCEDURËS PENALE ME VËSHTRIM TË POSAÇËM NË PROCEDURËN PENALE TË KOSOVËS, Sayfa100 , 2007Priştine

[63]Sijerçiq –Haliloviq, a.g.e., s.100.

[64]Dr. AzemHjadari, E Drejta e ProceduresPenale, sayfa 191-193, 2010, Priştine,

[65]Ejup Sahiti, Rexhep Murati, E drejta e procedurespenale (Ceza Muhakemesi Kanunu), Priştine, 2016, s.235; Dr. AzemHjadari, E Drejta e ProceduresPenale, Priştine, 2010, s.236..

olarak bazı durumlarda, duruma bağlı olarak, diğer kişiler, devlet makamları tarafından davanın açıklığa kavuşturulması için bilgi vermeye davet edilebilirler ve bunlar çeşitli alanlardan uzmanlar olabilirler.

Davadaki tarafların ve diğer kişilerin beyanları büyük öneme sahiptir ve ceza muhakemesi düzenlemeleri, muhakemenin başlaması aşamasında onlara önem vermekte ve mahkemelerin nihai kararları da bu delillere dayandırılması bu önemi göstermektedir. Bu deliller, yani tarafların ve diğer kişilerin ifadeleri, kişisel delil olarak kabul edilir ve bireysel olarak değerlendirilmesinden sonra ve diğer delillerle ilgili olarak da kanıtlayıcı değere sahiptirler.

Ancak, devlet organları bu delilin ele alınmasının son aşamasında çok dikkatli olmalıdır. Bu, delilin değerlendirilmesinin yüksek derecede profesyonellik ile yapılması gerektiği anlamına gelir. Çünkü pek çok nedenden dolayı bu delillerin doğru olmaması, eksik ve yanlış olması sıklıkla görülmektedir.

Delillerin, özellikle kişisel olanların değerlendirilmesi karmaşık bir zihinsel süreçtir ve bu değerlendirmenin yapılması için, muhakemenin taraflarında farkındalığın oluşumu ve yargı psikolojisi gibi unsurlar devreye girmektedir. Delillerin kesin değerlendirmesi, mahkemedeki oturumlarda veya müzakerelerde tartışılması vesilesiyle yapılır. Ancak, bu aşamadan önce, mahkeme her bir delili belirli bir ölçüde değerlendirir. Bu nedenle, somut delil elde etme ve aydınlatma sürecinde mahkeme, her bir delili analiz etmeli ve doğrulamalıdır. Böylece, eğer gerekirse, herhangi bir delil için bu yönde izleme yapılabilir[66].

Türk hukukunda delillerin serbestçe değerlendirilmesi ilkesi kapsamında tarafların ispat hususunda anlaşmaları ya da ikrar etmeleri hâkimi bağlamaz[67]. Tarafların iradesinden bağımsız şekilde hâkim, delilleri değerlendirir.

CMK'ya göre, şüphelinin ifadesi veya sanık beyanı, bu kişilerin özgür iradelerine istinat etmelidir (m.148/1). Bunu engelleyebilecek olan kötü muamele, işkence, cebir veya tehdit eylemleri gibi bedeni ya da ruhi müdahaleler yapılamayacaktır. Ayrıca sanık veya

[66]Dr. EjupSahiti, Psikologjiagjyqesore (Adli Psikoloji), Priştine, 2007, s.107.

[67] Ünver/Hakeri, s. 62; Devrim Aydın, Ceza Muhakemesinde Deliller, Ankara 2014, s. 148.

şüpheliye yasaya bir menfaat de vaat edilemeyecektir (m.148/2) Hatta, bu yasak yöntemlerle elde edilen ifade ve beyanlar, yani ikrarlar şüpheli veya sanıklar rızalarıyla vermiş olsalar da delil şeklinde kabul görmez (CMK m.148/3).

Bununla birlikte kolluk tarafından şüpheli müdafii hazır olmaksızın alınan ve suç ikrarı içeren ifadeler, soruşturma aşamasında şüpheli tarafından sulh ceza hakimi karşısında veya dava açıldıktan sonra sanığın mahkeme huzurunda doğrulamaması halinde hükme esas alınabilecek deliller olmayacaklardır[68].

Şüpheli ya da sanığın suçu kabullenmesi bulunsa da, bu kabullenme diğer delillerle de desteklenmelidir. Burada önemli olan şey, ifadenin şüpheli ya da sanığın özgür iradesiyle elde edilip edilmediği ve ikrarın somut deliller ile desteklenip desteklenmediğidir[69]. Örneğin şüpheli avukatı hazır olmadan kollukça alınan ifaden, hakim veya mahkeme huzurunda doğrulanmazsa karara esas alınamayacaktır.

2.1.5.1.1. Şüpheli/ Sanığın Beyanı

Ceza muhakemesinin tüm aşamalarda şüpheli ya da sanığın beyanlarına büyük önem verilmektedir. Bu ifade, suçu kabul ederek bir bütün olarak onaylayıcı, suçu reddederek inkâr ifadesi ve aynı zamanda, soruşturmayı yönlendirmek ve devlet organlarının yanlış yöne yönlendirmek için gerçekleri çarpıtmaya ve yanlış bilgi vermeye çalışarak başka şekillerde ortaya çıkabilir. Ancak, ne olursa olsun, sanığın beyanlarını değerlendirmek yargılama makamının görevidir. Beyanlar ayrıca diğer delillerle ilişkili şekilde değerlendirilmeli ve analiz edilmelidir. Ancak bundan sonra uygun sonuçlar çıkarılmalıdır.

Kosova Ceza Muhakemesi Kanunu'nda Türk hukukundan farklı olarak sanığın suçluluğunu kabul etmesine ilişkin açık düzenlemeler getirmiştir. Mahkemenin, sanığın ikrarının yasaya ve diğer mevcut koşullara uygun olup olmadığını kanıtlama konusunda katı yasal yükümlülüğü vardır.

Sanığın suçluluk kabulü, mahkeme tarafından ancak şu durumlarda onaylanabilir:

- sanık suçluluğu kabul etmenin doğasını ve sonuçlarını anlamış olması

---

[68] Ersan Şen, Şüpheli veya Sanık İkrarının Delil Değeri, https://www.hukukihaber.net/supheli-veya-sanik-ikrarinin-delil-degeri-makale,6082.html, erişim tarih: 07.06.2022.

[69] Şen, Şüpheli veya Sanık İkrarının Delil Değeri.

- suçluluk kabulü, savunma avukatıyla yeterli istişareden sonra gönüllü olarak yapılmışsa, bir savunma avukatı varsa ve sanığın suçu kabul etmek için hiçbir şekilde zorlanmamış veya mecbur bırakılmamış olması;

- suçluluk kabulü iddianamede sunulan somut durumun gerçeklerine ve maddi delillerine ya da iddianamenin tamamlanmasında savcının sunduğu ve sanıkça kabul edilen maddi delillerle ve savcı ya da sanıkça gösterilen tanıkların beyanları gibi diğer delillere dayanması.[70]

Yukarıda belirtilenlerden, sanığın ikrarına ilişkin ifadesini onaylamak için, diğer bazı yasal koşulların yerine getirilmesi gerektiği çok açıktır. Çünkü sadece sanık tarafından suçluluk kabulü, yeterli delil olarak alınamaz. Suçluluğun kabulü, sanığın suçlandığı suçun niteliği ve suçluluğun kabulü durumunda taşıyacağı sonuçlar, ayrıntılı olarak açıklandıktan sonra yapılmalıdır. Bu çok önemlidir, çünkü sanığın suçlu olduğunu iddia etmenin sonuçlarının farkında olmadığı ya da sonuçları en aza indirerek hiçbir sonuç olmayacağına dair yanlış söz vererek, sanığın iradesine kötü yönde etki edildiği durumlar bulunmaktadır.

Genellikle sanığa şartlı ceza veya küçük para cezası verildiğinde ortaya çıkar ve o hapis cezasına çarptırılmayacağını anlayarak suçluluğu, cezai suç işlemediği durumlarda bile kabul eder. Bu ve diğer nedenlerden ötürü, sanığın suçu kabul ettiği her durumda yanında savunma avukatının da bulunması gerekmektedir. Avukat, sanığa,bu durumu ve suçluluk kabul ettikten sonra karşılaşacağı sonuçları ayrıntılı olarak açıklayacaktır.

Öte yandan, mahkeme böyle bir durumdan kaçınmak için çok daha dikkatli olmalıdır ve aynısı her ne pahasına olursa olsun, sanık tarafından suçluluk kabulünün kendisine tam hukuki destek sağlandıktan sonra verildiğine ve savcılığın sunduğu diğer delillerin bu ikrarı desteklediğine ikna olduktan sonra onaylamalıdır. Hiçbir koşulda ve herhangi bir nedenle mahkeme, bu kabulün diğer deliller ve ifadelerle güçlü bir şekilde desteklenmemesi halinde, sanığın suçluluk kabulünü onaylamamalıdır.

Sanığın ifade vermesi veya vermemesine bakılmaksızın, yasa koyucu, görüşme veya sorgulama sırasında sanığın beyanını ifade etme özgürlüğünün kötü davranış, yorgunluk, fiziki müdahale, uyuşturucu kullanımı, baskı ya da hipnoz yoluyla, sanığın yasalarca

[70]Kosova Ceza Muhakemesi Kanunu, Madde 233, paragraf 18, alt paragraf 18.1-18.3.

yasaklanmış tedbirlerle tehdit edilmesi, yasa tarafından sağlanmayan herhangi bir menfaat için söz vermesi, hafızasını ya da anlama yeteneğini zayıflatması gibi yollarda etkilenmesini kesinlikle yasaklamaktadır. Sorgulama, bu yasaklara aykırı olarak yapılırsa, sorgulama veya mülakat kaydı kabul edilemezdir[71].

2.1.5.1.2. Mağdur ve Tanık Beyanı

Davada sanık olan kişinin ifadesine ek olarak, suçun mağdurunun ifadesi de büyük önem taşımaktadır. Zarar gören taraf, ceza muhakemesinde taraftır ve ifadesinin önemli delillerden biri olduğu bir bilgi kaynağıdır. Mağdur taraf, yaptığı açıklamada, önemli gerçekler sunabilir ve olayın meydana geliş şekli ve koşullarını daha kesin hale getirebilir. Bu durumda, mağdur bulunduğu pozisyona ek olarak, olayın tanığı olarak da kabul edilir ve çifte rol üstlenir.[72]

Mağdur tarafın tanık olarak sorgulanması ihtiyacı, genellikle uygulamada kaçınılmaz şekilde görülmektedir. Böyle bir durum, özellikle, somut ceza gerektiren suç için, mağdurun ifadesi dışında, usul organlarının karar vereceği başka bir delil bulunmadığı durumlarda ortaya çıkacaktır. Bu tür durumlar mülkiyete karşı suçlar veya vücut bütünlüğüne karşı suçlar olabilir ve bu gibi durumlarda mağdur tarafın tanık olarak sorgulanması kaçınılmazdır. Bu durum failin bilinmediği durumlarda bile ortaya çıkabilir.[73]

Diğer birçok vakada mağdurun ifadesi, mağdurun aynı zamanda tek tanık olabileceğinden, olayı aydınlatmak için tek delildir. Mağdurun derhal ölmediği veya ölüm olayı açıklığa kavuşturulmadan önce cinayet suçlarında bile, mağdurun önemli ifadelerine dair örnekler vardır. Ancak her durumda, mağdurun ifadesine dikkat edilmelidir, çünkü cezai suçu ve bu suçun neden olduğu hasarı tanımlarken çeşitli nedenlerle, sanıktan daha güvenilir değildir.[74]

Mağdurun ifadesinin, işlenen suça ilişkin soruşturmalarda daha önce görev almış, nitelikli olan ve dikkatli kişiler tarafından alınması çok önemlidir. Çünkü sorgulayan resmi kişinin nitelikli olması, cinsel istismar gibi bazı suçlarda çok hassas olabilmektedir. Çocuk

[71]Ejup Sahiti, Rexhep Murati, E drejta e procedures penale (Ceza Muhakemesi Kanunu), Priştine, 2016, s.262.

[72]Sahiti, Psikologjiagjyqesore (Adli Psikoloji), s.128.

[73]Sahiti, Psikologjiagjyqesore (Adli Psikoloji), s.128.

[74]Sahiti, Psikologjiagjyqesore (Adli Psikoloji), s.129.

mağdurların ifadeleri, doğaları ve duyarlılıkları nedeniyle çok dikkatli bir şekilde alınmalıdır. Çocuk mağdurlar söz konusu olduğunda usul hükümleri, çocuğun kişiliğini korumak ve kendisinin diğer duygusal yüklerine neden olmamak için daha da fazla kısıtlama getirmektedir.

Mağdur beyanı, gerek soruşturma gerekse kovuşturma safhasında gidilebilen ve beyan delili niteliğine sahip bir ispat aracı şeklinde kabul görmektedir. Mağdur, tanık olarak dinlenecekse, yemin dışında tanıklara dair düzenlemelerin tatbik edileceği ifade edilmiştir (CMK m. 50, 236). Bunun yanında, hukuksal konumuna bakıldığında mağdurun şüpheli ya da sanık gibi yargılama aşamasında uyuşmazlığa konu olayın bir parçası olan bir süje olduğu dikkate alınmalıdır. Mağdur ve katılan, açıklamaları suç oluşturmazsa beyanları nedeniyle cezalandırılamazlar[75]. Kosova Ceza Muhakemesi Kanunu m.62'de mağdurların taraf sıfatına sahip olduğu ifade edilmiştir. Yine m.77'ye göre polis, mağdurları, m.62'de yer alan hakları konusunda bilgilendirecektir. Mağdurun, m.124/2 kapsamında tanık olarak ifadesi alınabilir ve mağdur, m.340'da yer alan yemin etme yükümlülüğünden muaf tutulmamıştır.

Yargılama sırasında bir suçun işlenmesine tanık olan kişi, gerçeğin açıklığa kavuşturulması için çok önemlidir ve delil olarak çok büyük bir ağırlığa sahiptir. Tanıklar, olay yerinde ve duyuları aracılığıyla bu olayı yaşarken, suçun işlenmesini görebilen kişilerdir. Doğrudan gözlerinde tamamen ya da kısmen neler olduğunu gören, devlet otoriteleri nezdindeki deneyimlerini netleştirebilen görgü tanıkları da bulunabilir. Ayrıca, tanıklar olayı başka kaynaklardan da duymuş olabilirler ve aynı zamanda kovuşturma veya mahkemeye yönelik ceza davası hakkında önemli bilgiler verebilirler.

Duruşma sırasında da tanık ifadeleri bile dikkatle alınmalıdır, çünkü tanıklar etkilenebilir, koşulları yanlış anlayabilir, psikolojik doğasının yansımaları ortaya çıkabilir, yargılama sırasında ifade verdiği ilgili gerçeklere ilişkin ifadesinin doğruluğunu da etkileyebilecek davalarda herhangi bir tarafa sempati veya antipati oluşturabilir[76].

---

[75] Öztürk, s. 321; Aydın, 2014, s.77; Ahmet Bozdağ- Kader Sarıusta, Ceza Yargılamasında Mağdurun Beyanı Ve Delil Değeri, İnönü Üniversitesi Hukuk Fakültesi Dergisi –İnÜHFD- C:8 S:2, 2017, s.585.

[76]Sahiti, Psikologjiagjyqesore (Adli Psikoloji), s.131

Türk doktrininde tanıklık, ceza muhakemesindeki uyuşmazlığa konu eylemin beş duyuyla algılanması ve bunların muhakeme safhasında mahkeme önünde anlatılmasıdır[77]. Tanığın beyanı delildir, kendisi ise delil kaynağıdır[78]. Tanık beyanı, tanığın beş duyu organıyla algıladığı olaylara dayanmalıdır. Tanık sıfatını kazanabilmek için beş duyu organı vasıtasıyla olayı algılama haricinde fiziki ya da ruhi bir olgunluk aranmamaktadır[79].

CMK "Tanığın Dinlenilmesi" başlıklı m. 52'de yer aldığı üzere tanık beyanı, sözlü beyandır. Tanığın dinlenilmesinden söz eden CMK'ya göre tanık beyanını verirken daha önce yazdıklarını okuyamaz[80].

Mağdurun tanık olarak dinlenilmesi durumunda yemin dışında tanıklığa dair düzenlemelerin uygulanacağı hüküm altına alınmıştır (CMK m. 236/1). Bazı yazarlar, mağdur ve şikâyetçinin davanın tarafı olmaları nedeniyle tanık vasfıyla yeminsiz şekilde beyanlarının alınabileceğini fakat bu beyanların tanık beyanı olmayıp sanık harici diğer taraf beyanı olarak adlandırmaktadır[81]. Bazı yazarlar, katılanın tanık olabilse de, mağdur ya da şikâyetçinin tanık vasfıyla dinlenirken yeminsiz dinlenmesi gerektiğini ifade etmektedir. Bazı yazarlar, mağdur, şikâyetçi ve katılanın beyanları farklı delillerle desteklenmediği sürece mahkumiyet kararı verilemeyeceğini ifade etmektedirler[82].

Tanıklığa ilişkin bir başka sorunlu alan, suç ortaklarının tanık olmasıdır. CMK'da "m. 50'de ceza muhakemesinde suç ortağının tanıklığına olanak sağlanmıştır. Suç ortağı kişi de şüpheli veya sanık gibi uyuşmazlığın tarafıdır. Bu nedenle şeriklerin birbirlerine karşı tanıklık yapması doğru değildir ve bu yüzden bu hüküm hatalıdır. Bazı yazarlara göre, bu halde sanıklar açısından kendini suçlayıcı beyan verme yasağı tatbik edilmelidir (CMK m. 48)[83].

---

[77]Yenisey / Nuhoğlu, s.518; Metin Feyzioğlu, Ceza Hukuku Muhakemesinde Tanıklık, Ankara 1996, s. 28.

[78] Şahin / Göktürk, s.182.

[79] Osman Yaşar, Yeni İçtihatlarla Uygulamalı e Yorumlu Ceza Muhakemesi Kanunu I. Cilt, 7. Baskı, Seçkin Yayıncılık, Ankara, Nisan 2017, s.649.

[80]Yenisey/Nuhoğlu, s. 519.

[81]Centel/Zafer, a.g.e., s. 287 vd

[82] Bıçak, s.478.

[83] Şahin/Göktürk, s. 184

2.1.5.1.3. Beyanların Delil Değeri

Nihai bir karar verilmesi durumunda, gerek savcı tarafından soruşturma aşamasında ve iddianamenin sunulması sırasında gerekse mahkeme tarafından beyanların delil değeri belirlenmelidir. Bu nedenle, beyanların usul hükümlerine ve diğer yasal mevzuat hükümlerine uygun olarak alınması çok önemlidir, aksi takdirde bu ifadeler mahkeme tarafından delil kabul edilemezler[84].

Polis ve savcı tarafından toplanan delil niteliğindeki ifadeler, ancak mahkeme tarafından incelendikten ve doğrulandıktan sonra delil değeri kazanır. Aynı durum, anayasal ve yasal haklarına uygun olarak usul hükümlerine göre alınması gereken sanık ifadesi için de geçerlidir.

Usul hükümleri, tanığın ifadelerinin ne zaman kabul edilemez olduğunu belirler. Örneğin tanıklıktan çekinme hakkı bulunanların, bu hakları hatırlatılmadan beyanlarının alınması halinde, bu tanıkları ifadeleri hiçbir koşul altında delil olarak kabul edilemez ve mahkemenin kararı bu delillere dayanamaz. Ayrıca, tanıklık etmeyi reddetme hakkını anlamayan bir çocuğun ve tanığın (çocuklar özellikle polis ve kovuşturma tarafından manipüle edilme eğilimindedir) ifadesinin zorla, tehditle veya diğer yasaklanmış yollarla elde edildiği durumda alınan ifade, yargılamalarda delil olarak kabul edilemez.[85].

Hukuka aykırı yollarla ele geçirilen delil araçları, "delil" olamaz ve hükme esas alınamaz[86]. CMK m. 217/2'de[87] yer alan düzenlemede, delillerin ele geçirilmesinin doğrudan ve dolaylı etkisi şeklinde bir ayrım gözetilmemiştir. "*Hukuka uygun bir şekilde elde edilmiş her türlü delil*" ifadesiyle şekilde hukuka aykırı olmama durumları ifade edilmiştir[88]. Örneğin

---

[84]EjupSahiti, RexhepMurati, XhevdetElshani, Kosova Cumhuriyeti Ceza Muhakemesi Kanunu Şerhi, Baskı I, 2014, Priştine, 2014, s.676.

[85]Kosova Ceza Muhakemesi Kanunu, Madde 128.

[86] Nevzat Toroslu, "Hukuka Aykırı Deliller Sorunu", Prof. Dr. Hamide Topçuoğlu'na Armağan, Ankara 1995, s. 58,

[87] CMK m.217/2: *"Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir"*

[88] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, AÜSBF Yayınları, Ankara 1995, s.33.

soruşturma aşamasında CMK m.148 yasak usullerle ele geçirilen ifadeler açısından değerlendirme yasağı öngörmektedir[89].

Yine tanıklar için CMK md. 45,46 ve 48'de getirilen tanıklıktan çekinme hakkı ile sanıkla belirli derecede akrabalığa sahip şahıslar tanıklık yapmaya mecbur bırakılmamakta, bu şekilde akrabalarını suçlayan beyanda bulunma ile yalan söyleme ikilemini yaşamaları önlenmektedir[90]. Ayrıca belli meslekleri icra edenlere de tanıklıktan çekinme hakkı tanınmıştır. Meslekleri sebebiyle tanıklıktan çekinme hakkı olanlar ise avukatlar ve stajyerleri ile sağlık mesleğine mensup olanlardır[91].

2.1.6. Maddi Deliller

Delil, çok sayıda ceza muhakemesi usulü kuralının uygulanmasıyla elde edilebilir. Delil elde etme uygulamaları arasında, olay yerinin incelenmesi büyük önem taşımaktadır. Olay yerinin incelenmesi faaliyetinin, öneminden dolayı, en kısa zamanda ve alana ilişkin uzmanlığın gereklerinin yerine getirilmesi suretiyle gerçekleştirilmesi gerekmektedir[92]. Maddi delillerin çoğu veya en azından bir kısmı, suçun işlendiği yerde kalır.

Olay yerinin maddi delil sağlama açısından önemi tartışılmazdır. Aslında, olay yeri, suçun niteliğine ev işleniş şekline göre suçun varlığını, bir sanığın suçluluğunu veya masumiyetini belirleyen ve maddi delil sağlamak için ana kaynaklardan biridir. Bu nedenle, olay yeri hem cezai hem de yasal ve usuli anlamda geniş çapta ele alınmaktadır.

Olay yerinin incelenmesi, işlemi yapan organının suçun işlendiği ortamı algıladığı, maddi delilleri tespit ettiği, etkin bir şekilde iz ve maddi delil topladığı ve konuyla ilgili koşulları açıklığa kavuşturduğu bir soruşturma eylemidir. Olay yerinin incelenmesi, etkinliğin, bulunan izlere ve incelenen kişinin kişiliğine dayanan mekanizmasını açıklayan önemli bir bilgi kaynağını ortaya koymaktadır. Diğer işlemlerle karşılaştırıldığında inceleme, yeri

---

[89] Pervin Aksoy İpekçioğlu, Gözaltında Alınan İfadenin Önemi Ve Delil Değeri, AÜHFD , C.57 S.3, 2008, s.63.

[90] Feyzioğlu, s.197.

[91] Devrim Güngör, Ceza Muhakemesinde Tanık Beyanının Delil Değeri Üzerine Bazı Tespit Ve Değerlendirmeler, İnönü Üniversitesi Hukuk Fakültesi Dergisi, C:6, S. 2, 2015, s. 309, 312; Semiyet Badem, Ceza Muhakemesi Hukukunda Tanık, TAAD, Yıl: 12, Sayı: 45, Ocak 2021, s.308

[92]AzemHajdari, Komentari I Kodit te PorceduresPenale te Kosoves, sayfa 180, 2016, Priştine

doldurulamayan bir işlemdir ve kural olarak işlenen herhangi bir somut suç için yapılabilir[93].

Delil ve olay yeri ile ilgilenen birçok araştırmacı, olay yerinin anlamı ile ilgili birçok tanım sağlamıştır. Olay yerini anlamak sadece teorik değil aynı zamanda pratik açıdan büyük öneme sahiptir, zira suçun işlendiği yere bağlı olarak mahkemenin yargı yetkisini de değişir.

Olay yeri, suçun meydana geldiği yerdir. Bu yerde, olay ile ilgili olası maddi izler ve deliller bulunabilir. Olay yerinde ayrıca olayın gelişimi ile ilgili koşullarının açıklığa kavuşması için incelemeler yapılmalıdır ve bunlar üzerinden olayın meydana gelmesi nedenleri, mekanizmaları, sonuçları ve failleri belirlenmelidir[94].Bu yüzden olay yeri, o olayla ilgili iz ve maddi delil bulmak için gerçek bir fırsatın bulunduğu bir yer olarak anlaşılmalıdır. "Yer" terimi ile, tam olarak o olayın meydana geldiği ya da sonucun tam olarak meydana geldiği yer kastedilirken, "olay" terimi ile belirli bir ortamda gerçekleşen olayı veya değişimi kastetmekteyiz. Böylece, yer, olayın gerçekleştiği somut yeri anlamına gelirken, olay suçu, yani suçun işlenmesi anlamına gelmektedir[95].

Ceza hukuku açısından, suçun işlendiği yerin belirlenmesi büyük önem taşımaktadır, çünkü mahkemenin bölgesel yargı yetkisi, işlenme yeri tarafından belirlenir. Bazı suçlarda işlenmenin yeri temel bir unsur olarak kabul edilir. Bazı durumlarda uluslararası ceza hukuku açısından, suçun işlendiği yeri belirlemek önemlidir, çünkü suç bir ülkede işlenmiş olabilir ve sonuç diğer ülkede ortaya çıkabilir[96].

Olay yeri bir suçun işlendiği ve onun içinde veya etrafında meydana gelen suç ile ilgili iz, araç veya delillerin bulunabileceği bir yer olarak kabul edilmektedir. Bu nedenden dolayı inceleme, detaylı arama, fotoğraf çekme, tespit, durumun belgelerinin belgelere yansıtılması, olay ile ilgili olabilecek veya suçun nedenlerini, koşullarını, yollarını,

---

[93]AzemHjadari, Komentari I Kodit te ProceduresPnelae te Kosoves, sayfa 402, 2016, Priştine

[94]EshrefMyftari, Keqyrja e vendit te ngajres, Tiran, 1984, s.9

[95]CrimeSceneandForensicTechniqueseğitiminden materyal, SHSHPK, Vushtri, 2002.

[96]IsmetSalihu&Hilmi Zhitia&FejzullahHasani, Komentar i KoditPenaltëRepublikëssëKosovës, Sayı I, Priştine 2014, s.40

potansiyel faillerini veya failini bulmak için bir temel oluşturabilecek materyal ve araçların toplanması organize edilmesi talep edilir.[97]

Suçun meydana geldiğine inanılan yerde, suç, işlenme mekanizması, işlenme aracı, fail veya potansiyel failler ile ilgili çoğu sayıda iz ve materyal delil kalmış olabilir. Bunlar, suç eyleminin yasal olarak belgelenmesine veya failin bulunmasına yol açabilir. Olay yerinin incelenmesi bir soruşturma yöntemidir. Bununla muhakeme organı direk olarak suçun meydana geldiği ortamı algılar ve ayrıca, olay ile ilgili önem taşıyan koşulları açığa kavuşturur ve maddi delilleri bulur, toplar ve tespit eder.[98]

Olay yeri; bir ev veya bir bina, bir araba veya herhangi bir açık ya da kapalı yer olabilir[99]. Olay yeri, suçun işlendiği veya suçun işlenmesinin kanıtlandığı ve failin bulunmasını sağlayabilecek izlerin veya delillerin bulunabildiği yerdir. Ceza muhakemesi yönünden, olay yeri veya suçun işlendiği yer, eylemin gerçekleştirildiği ve sonucun ortaya çıktığı yer olarak kabul edilmektedir. Daha da kesin olarak, cezai bir suçun işlendiği yer, KCMK'nın 10. maddesinde belirtilmiştir[100]. Suçun işlendiği yer, failin bir fiilde bulunduğu veya bulunmaya zorunlu olduğu ya da zararların meydana geldiği yeri temsil etmektedir. Suç, failin hareket ettiği veya zararın meydana gelmesini istediği yerde hazırlanmıştır veya işlenmesi denenmiştir[101].

Bu çalışmanın amaçlarından biri, olay yerinin kriminalistik anlamında ele alınması ve sırasıyla materyal delillerin sağlanması ve toplanması olduğu için bizim odak noktamız bu anlamda olacaktır. Ancak, olay yerini en doğru şekilde anlamak için bazı ek açıklamalar sağlayacağız.

Eğer bir cezai suçun meydana geldiği yeri göz önüne bulundurursak o zaman olay yerlerini devamdaki gruplara ayırırız: kapalı olay yerleri ve açık olay yerleri:

- Kapalı olay yerleri, cezai suçun bir ev, bir yaşam binası, bir bina veya bir apartman vb. gibi fiziki anlamda kapalı olan yerler sayılır.

---

[97]Mr. Sc. Besim Arifi, Keqyrja e vendit te ngjarjes, Priştine 2012, s. 27

[98] Dr. Vesel Latifi, Kriminalistika, zbulimidhe te provuarit e krimit, 2009,s.171.

[99]Dr. AzemHjadari, Komentari I ProcduresPenale, Priştine 2010, sayfa 379

[100]AfrimShala, Hyrje ne te drejtenPenale, Priştine 2019, s.60-61

[101]Kosovoa Cumhuriyeti Ceza Kanunu, Madde 10, Fıkra 1,2

- Açık olay yerleri cezai suçun açık olan bir alanda işlendiği yerlerdir. Bunlar cezai suçun doğada, yolda, ev bahçesinde, otopark vb. gibi yerlerde işlendiği durumlardır.[102]

Olay yerinin araba olduğu hallerde bazı araştırmacılar, bu olay yerini ayrı bir kategori içinde görmektedir. Dolayısıyla bu olay yerini inceleyenler suçun (cinsel saldırı, cinayet vb.) araba içinde meydana geldiğinde sadece arabayı olay yeri olarak görmektedir[103].

Maddi delillerin bulunduğu yere gelince olay yerlerini birincil ve ikincil olay yerleri olarak ayırırız.

Birincil olay yerleri suçun işlenildiğinden şüphe olan ve ana delillerin ya da suçun orada işlendiğini doğrulayan delillerin bulunduğu yerlerdir. Ayrıca, birincil olay yerleri, olay ile ilgili ana delillerin bulunup bulunmasına bakılmaksızın ilk incelenen sahne olarak de düşünülebilir.

İkincil olay yeri, doğrudan birincil olay yeri ile ilgili olan maddi delillerin bulunduğu yer olarak kabul edilir. Aşağıdakiler bu tür yerler olarak kabul edilir:

- vücudun hareket edildiği yerden;

- ölüme neden olan saldırının gerçekleştiği yer;

- suç ile ilgili herhangi bir fiziksel kanıtının bulunduğu yer (beden parçaları);

- cesedin bulunduğu yere kadar taşınması için kullanılan araç.[104]

Ayrıca, failin olay yerinden ayrılması sırasında (olay yerinin ana noktasından kaçış yolu) yakın mesafelerde maddi deliller bıraktığı bulunduğu durumlar da vardır[105]. İkincil olay yerleri, arama sırasında suçun hazırlandığını kanıtlayan delillerin veya çalınan ve o yere getirilen nesneler gibi cezai suçun işlenmesini kanıtlayan delillerin bulunduğu yerlerdir.

---

[102]Crime Scene and Forensic Techniques eğitiminden materyal, SHSHPKVushtri, 2002.

[103]Gökcen- Çakır, s.2920.

[104]NedzadKorajlic, TaktikaKriminalistike, Priştine, 2007, s. 225.

[105]Vincent J.M. Dimao, ManagingDeathInvestigation, FBI Handbook, s. 98.

- Olay yerinin incelenmesi, yargı makamının, suçun meydana geldiği ortamı doğrudan algıladığı, maddi delilleri tespit ettiği, topladığı, düzelttiği ve dava ile ilgili koşulları açıkladığı bir soruşturma eylemidir[106].

- Olay yeri incelenmesi, suçun meydana geldiği ortamda değişikliklerin meydana geldiği her durumda gerçekleştirilebilir[107]. Kural olarak, hiçbir maddi iz bırakmayan suç yoktur ve bu nedenle olay yeri ile ilgili temel teori Locard'ın "bir şey bulunmalıdır" ilkesi olur[108].

- İnceleme sürecinde uzmanlar, koşulları belirlemek ve olayın gelişimini açıklamak için özel önem taşıyan delilleri keşfeder, gözlemler ve toplar. Bu nedenle, incelemenin mümkün olduğunca verimli olması için onu yapan ekibin, inceleme sırasında olay yerinde karşılaşılan tüm izleri ve maddi delilleri tespit etmeye, gözlemlemeye ve toplamaya dikkat etmesi gerekmektedir[109].

- İncelemenin özel önemi, delillerin ve delil kavramının genişletilmesi gerektiği gerçeği ile ilgilidir. Örneğin parmak, ayakkabı ve lastik izlerini delil olarak saymanın yanında bazen çok az veya hiç görülmeyen mikro izleri de kanıt olarak sayılmalıdır. Bu kanıtların, görülen kanıtlar kadar önemi vardır. Eğer bir uzman ekip incelemeyi yapar ve buna gerekli önemi verirse, o zaman bu delillerin kendi aralarında ve diğer koşullarla arasında bir bağlantı kurularak bilinmeyen birçok konu aydınlatılacaktır.

- "İz" kelimesi Fransızca "le trace" kelimesinden türetilmiştir. Bu kelimeye bilim veya çalışma anlamına gelen logos kelimesi eklenir ve her ikisi de Traseoloji bilimi olarak da adlandırılan izler üzerinde araştırma yapar. Böylece, Traseoloji izleri araştıran bir Kriminalistik dalıdır[110]. İz, faili tespit etmeye veya belirli bireysel durumları tespit etmeye

---

[106]Vesel Latifi, Kriminalistika, zbulimidhetëprovuarit e krimit, Priştine, 2011, s.229.

[107]XhemajlAdemaj, EkspertizatKriminalistike, Priştine, 2010, s. 89.

[108]Ademaj, s. 72.

[109]Öğrenci el kitabı, Mbrojtjadhekëqyrja e vendittëngjarjes, SHSHPK, Vushtri, 2002.

[110] Besim Arifi, Këqyrja e vendittëngjarjes, Priştine, 2012, s. 8.

yardımcı olabilecek insan, hayvan, nesne veya araç tarafından bırakılan herhangi bir şeydir[111].

- Olay yerinin incelenmesi, faili keşfetmek ve suçu işlediğini kanıtlamak için büyük bir bilgi kaynağıdır. İzler, suç olayıyla ilgilidir, ancak fiili durumu gizlemek veya failden şüpheyi kaldırmak için de izlerin bırakılabileceği akılda tutulmalıdır[112].

Suçun işlendiği yerde, en sık devamdaki izler bulunabilir:

1. traseolojik izler (el, ayakkabı, ateşli silah vb. izleri)

2. malzeme izleri (insan biyolojik izleri, tekstil, cam, metaller, vb.).)

3. nesnelerde (eşyalarda) izler vb. [113]

Her bir cinayetin gerçekleşme biçiminin özelliklerinden bağımsız olarak, her durumda, olay yeri inceleme biriminin çözülmesi gereken bazı problemler önüne çıkar.[114]

Bunlardan bazıları aşağıdakilerdir:

1. Olayın meydana geldiği yer;
2. Olayın meydana geldiği zaman;
3. Suç araçları;
4. Araştırmacı sayısı;
5. Mağdurun kimliği;
6. Faili güdüleyen şey vb.

Olayın ne zaman gerçekleştiğinin belirlenmesi, failin kovuşturulmasını ve yakalanmasını sağlamakla ilgilidir. Kural olarak, bir kişinin ölüm zamanı, olayın gerçekleştiği zamanla

[111]Aynı yerde, s. 85.

[112]Ademaj, s. 208.

[113]Ademaj, s. 208.

[114]EstrefMiftari, Kriminalistika, s. 174.

çakışmalıdır. Mağdurun vücuda verdiği hasar derecesi ne kadar şiddetli ve ölümcül olursa, olayın meydana gelmesiyle ölümün meydana gelmesi neredeyse aynı anda olur.[115]

Suçun işlendiği zaman; ceset lekelerinin (erken ve geç), atmosferik olayların (yağmur, kar) ve olay yerini ve cesedi incelerken tespit edilebilecek diğer durumlar ve olgular keşfi ve incelenmesi gibi bilgilerin toplanmasından anlaşılır. Bununla birlikte, olay yerinin de dış etkilerden etkilenmesi önlenmelidir ve gerekli koruyucu tedbirler alınmalıdır[116].İnceleme sırasında günlük gazeteler, seyahat biletleri vs. gibi çeşitli belgeler bulunabilir. Ardından, masaüstü bilgisayar, dizüstü bilgisayar, son aramaların istendiği yerlerde telefon, mesajlar, e-posta gönderileri, etkinleştirilirse telefon alarmları ve varsa hangi saate ve tarihinde yapıldığı gibi verileri elde etmek için elektronik cihazlar kontrol edilir.

Örneğin olay bir bina içinde meydana gelmişse ve ışıklar açık ise, olayın gece meydana geldiği anlaşılabilir. Ayrıca kurbanın üstünde pijamalarsa varsa, bu, olayın gece meydana geldiğini gösterebilir. Masaüstünde taze yemek de olayın yeni gerçekleştiğinin bir göstergesidir. Çiçek saksılarına, içlerindeki toprağın durumuna ve onların sulanmış olup olmamalarına da bakmak gerekmektedir.

Olay doğada meydana gelmişse, cesedin ne tür kıyafetleri giydiğine, yani yaz ve kış giysileri olup olmadığına bakılır. Maktulün üzerinde yağışın üzerindeki etkisine, maktulün vücudun yağmurdan ıslanıp ıslanmadığına, eğer ıslanmışsa bulunduğu yere göre zemine bakılır. Mağdurun kıyafetlerinin ayrışması, böcek etkileri, cesedin vahşi hayvanlar tarafından zarara uğraması vb. bilgiler olayın gerçekleştiği zamana ilişkin bilgi verebilmektedir.

Suçun işlendiği zamana, kriminalistik boyutu dışında ceza mevzuatı da özel önem vermiştir. Kosova Cumhuriyeti Ceza Kanununa göre, suç, onun meydana gelme zamanına bakılmaksızın failin harekete geçtiği ya da harekete geçme zorunluluğu olduğu durumda işlenmektedir[117].

[115]Sokrat Meksi&FlamurBlakaj, s. 40.

[116]Gökcen-Çakır, s.2920; Polat, s.340; Kaygısız, s.43.

[117]Kosova Cumhuriyeti Ceza Kanunu, Madde 9, fıkra 1.

Tabii ki, bu göstergelerin kaydedilmesi ve düzeltilmesi olayın zamanını belirlemenin bir yönünü oluşturmaktadır, fakat en önemlisi de olayın zamanlamasını belirlemek için her bulgunun değerlendirilmesi ve bilimsel yorumlanmasıdır.[118]

Ölümcül yaralanmalara neden olabilecek olan silahlar ve sert cisimler gibi bütün nesne türleri cezai suçun işlenmesinde araç olarak kullanılabilir[119]. Suçun işlendiği cisim, ceset üzerinde yaralanma özelliklerine göre belirlenebilir. Bu yaralanma özellikleri çoğu zaman kullanılan cismin şeklini ve büyüklüğünü gösterir. Bereleme, hematom, yara, kırılma, yırtık, beden kısımlarının kopması, keskin aletlerle kesme, yanık, zehirleme izleri, ateşli silahlar ve diğer araçlardan yara izlerine, yani yaralanmaların türüne bağlı olarak ölüm şekli ve hangi aracın ölüme neden olduğu belirtilmesi gerekebilir[120]. Yaralanmanın türüne bağlı olarak, kırma veya çizilme, hematom, yaralar, kırıklar, vücut parçalarının ayrılması, keskin aletlerle kesmesi, yanma, zehirlenme izlerinin, ateşli silahlardan veya diğer yollardan yara izlerinin, ölüm şeklini ve ölüme neden olan araçlar belirlenmelidir[121].

Olay yerinin incelenmesi, önemli bir muhakeme eylemi olarak KCMK'de öngörülmektedir. Burada, olay yeri incelemesi sırasında uyulması gereken bazı kurallar bulunmaktadır. Devlet savcısı, toplanan delilleri gözden geçirmek veya ceza muhakemesi için önemli olan gerçekleri aydınlatmak için olay yerinin incelenmesinin veya aynısının yeniden yapılandırılmasını emredebilir[122]. Bu hükümden, olay yerinin incelenmesini (ve yeniden yapılandırılmasını) emreden kurumun Devlet Savcısı olduğunu anlamaktayız. Bu eylemin temel amacı, ceza muhakemesinde soruşturma aşamasında delil toplamak ve önemli gerçekleri açıklığa kavuşturmaktır. Bu sürecin, suçun varlığını doğrulama, türünü belirleme, fail bulma, mağdurun kimliğini tespit etme, zararın varlığını ve yüksekliğini doğrulama, belirlenen kişileri kontrol etme vb. gibi nihai bir amacı vardır[123].Devlet Savcısının, incelemeyi yerine getirmesi için sırasıyla eğitimli ve nitelikli polis birimlerine emir verdiği anlaşılmaktadır.

---

[118]EstrefMiftari, s. 177.

[119]NedzadKorajlic, Metodika,..,s. 37.

[120]EstrefMiftari,s.177.

[121]SokratMeksi&FlamurBlakaj, s.54

[122]Kosova Ceza Muhakemeleri Kanunu, Madde 150.

[123]AzemHajdari, Kometari I Kodit te PorcddduresPenale te Kosoves, Priştine, 2016, s. 402.

Devlet savcısı olay yerini polis ile birlikte veya kendisi yalnız inceleyebilir, çünkü KCMK Devlet Savcısına bunu yalnız yapma hakkını vermektedir. Ancak, Devlet Savcısının böyle bir inceleme için yeterli bilgiye sahip olmadığı göz önüne alındığında, bu metin ile bu hükmün uygulanamayacağını düşünüyoruz. Bununla birlikte, Devlet Savcısının, olay yeri incelemesinin yapılması konusunda sıkı usul sınırlamaları da vardır. Olay yerinin incelenmesi veya yeniden yapılandırılması, devlet savcısı veya polis tarafından gerçekleştirilir. Devlet savcısı ve polis durumla ilgili kendileri bilgi almak için sözü edilen incelemeyi veya yeniden yapılandırılmayı gerçekleştirilebilir. Bu onların güvenirliği belirleme veya delillerin bulunmasını sağlayacaktır. Fakat, bu durumlarda, bu maddenin 3 veya 4. fıkraları ile uyumlu olmadıkça sonuçlar kabul edilmeyecektir. Devlet savcısı bu tür bir incelemeyi veya yeniden yapılandırılmayı bir bildirim ile yeniden gerçekleştirilebilir ve bu durumda atıfta bulunan sonuçlar kabul edilir olacaktır[124]. Bu hüküm, muhakemede taraflar arasında bir tür tarafsızlığı korumak için konulmuştur, çünkü olay yerinin sadece savcının ve polisin katılımıyla incelenmesi, taraf tutma veya muhakemede sanık olan kişinin çıkarlarına ve haklarına aykırı olan delillerle oynama ile ilgili şüphelere sebep olabilir. Savcı ve polis tarafından yapılan, sanık ve savunma avukatına bildirilmeden bu tür bir inceleme yapıldıysa, incelemenin sonuçları mahkeme tarafından kabul edilebilir sayılmayacaktır[125].

Bu tür durumların önüne geçmek için yasama organı ayrıca olay yerinin incelenmesi ile ilgili bir kaç ilave kriter öngörmüştür. Bu kapsamında eğer olay yerinin incelenmesinden önce failin belli olduğunda durumlar öngörülmüştür. Şüpheli, olay yerinin incelenmesinden önce tespit edilip tutuklanmışsa, o zaman devlet savcısının bazı yasal sınırlamaları olacaktır. Kimlikleri bilindiği durumlarda, devlet savcısı, şüpheliyi, sanığı veya savunma avukatını inceleme veya yeniden yapılandırma ile ilgili bilgilendirecektir. Sanığın savunma avukatı, olay yerinin incelemesinde veya yeniden yapılandırılmasında bulunma hakkına sahiptir.[126]

---

[124]Kosova Ceza Muhakemeleri Kodu, Madde 150, fıkra 2

[125]Hajdari, s. 403.

[126]Kosova Cumhuriyeti Ceza Muhakemeleri Kanunu, Madde 150, fıkra 3.

Çoğu durumda olay yeri incelemesi yapıldığında suçu işleyen kişi bilinmeyebilir çünkü gerçekten inceleme işlemleri suçun işlendiği zamandan sonra ilk saatlerde yapılmaktadır ve böylece fail tespit edilmemiş olabilir, ya da kaçması ya da başka nedenlerden dolayı emniyet kurumları ve savcılık tarafından bilinmeyebilir. Bu gibi durumlarda muhakemenin taraf tutmaması yani tarafsızlığını koruması için yasama organı çok özel bir kural koymuştur. Bu kural uyarınca olay yeri incelenmesinin gözlemi ve denetiminde ön duruşma hâkimine büyük bir rol vermektedir[127]. Şüpheli, sanık veya savunma avukatı devlet savcısı tarafından bilinmiyorsa, ön duruşma hâkimi incelemeye ve yeniden yapılandırmaya katılır ve onları ayrıca gözlemler[128].

Bazı suçların karmaşıklığı göz önüne alındığında, farklı alanlardan uzmanlar olay yeri incelemesi kapsamında çalışma yapabilir. Bu tür vakalar, örneğin balistik, adli tıp veya bomba patlaması soruşturmasında bir uzmana ihtiyaç olduğunda olabilir. Bu tür durumlarda uzmanların incelemeye dahil edilmesi için olanaklar sağlanır. Olay yerinin incelenmesi veya yeniden yapılandırılması, delilleri korumak veya açıklamak, gerekli ölçümleri ve kayıtları yapmak, çizimleri çizmek ve ayrıca diğer bilgiler toplamak için yardım edilebilir[129]. Son olarak, olay yerinin incelenmesi için temel eylemler, girme, kontrol, fotoğraflama, ölçme, belgeleme, delil paketleme gibi işlemlerdir.

2.1.6.1. Suç Aletlerinden Elde Edilen Deliller

Suçlar en sık ateşli silahlar, keskin aletler (bıçak, tornavida, makas, iğne, balta), ağır cisimler (tuğla, çubuk, iş aletleri, taş, yumruk), zehir, yanma (ateş), normal boğma ve suda boğma ve diğer birçok aletle ve birçok şekilde işlenebilmektedir. Kuşkusuz, ateşli silahların yaygınlığını göz önüne aldığımızda, pratikte çoğu zaman, cezai kullanımları sonucu veya ihmal sonucu kullanımları esnasında büyük zararlara neden olunabilir ve bazen bunlar ölüme de yol açabilmektedir[130]. Ateşli silahlarla işlenen suçların incelenmesinde,

[127]KCMK'nin 19. maddesi, 1 fıkrası, 1.23 bendi uyarınca ön duruşma hâkimi soruşturma aşamasında belirlenen hâkim olacaktır.

[128]Kosova Cumhuriyeti Ceza Muhakemeleri Kanunu, Madde 150, fıkra 4.

[129]Kosova Cumhuriyeti Ceza Muhakemeleri Kanunu, Madde 150, fıkra 7.

[130]GramozYlli, Kontributi i ekspertitmjekoligjornëdëmtimetngaarmët e zjarrit, ''Justiniani I'' bilimsel dergide yayınlanmıştır, No.1, Aralık 2009, s. 66; FadilKajtazi, Pisatoletatdherevolveret, 2015, s.13; Ademaj, s.347.

laboratuarların balistik bölümleri önemli rol oynamaktadır[131]. Örneğin bu kapsamda değerlendirilen deliller çıkış yarası, maktülün olayda günlük hayatta kullandığı eli kullanıp kullanmadığı veya olayda biden çok atış olup olmadığı gibi delil ve belirtilerdir[132]. Yaralamada kesici ve delici alet kullanılması, bunların açtığı yaraların büyüklüğü, iz ve yönleri de yaralamanın bıçak ve benzeri aletlerle gerçekleştirildiğini göstermektedir.

Yine failin temas ettiği yüzey ile temas sırasında parmaklarda bulunan ve bu yüzeyde bırakılan, ter-yağ katmanlarından oluşan görünür, yarı-görünür veya görünmez bütün çizgiler de failin parmak izlerinin bırakıldığı anlamına gelmektedir[133]. Parmak izleri, bu özellikleri dolayısıyla eğitilmiş personel tarafından olay yerinde dikkatle aranır, çünkü parmak izleri benzersiz bir delildir

Olay yerinde ele geçirilen el yazısı belgeler de laboratuarlarda grafoloji dairelerinde incelenmektedir. El yazısının da parmak izlerinde olduğu gibi kişiye has benzersiz özellikleri bulunabilmektedir ve failin el yazısı ile karşılaştırıldığında bunlar eşleşebilmektedir[134].

Bunların yanında olay yerinde başka fiziki deliller de bulunabilir. Örneğin olay yerinde şekil izleri; yani kırılmış eşyanın parça şekli veya sıçrama, leke izleri bulunabilir. Yine olay yerinde aralarında organik, inorganik ve zehirler gibi materyal izleri olabilir. Materyal izlerinden kasıt; katı, sıvı ya da gaz biçiminde olabilen ve miktar olarak az veya çok hacme sahip olabilen izlerdir[135].

2.1.6.2. Beden Muayenesi ve Vücuttan Örnek Alma (Biyolojik Delil)

Birçok durumda, olay yerinin araştırırken, araştırmacılar, biyolojik doğası olan izlerin araştırılması, bulunması, düzeltilmesi ve izlenmesi üzerine odaklanırlar. Bu, genellikle

---

[131]Gökcen- Çakır, s.2925; Fadil Batalli, Mjekesia Ligjore, Priştine 1987, s.46

[132]Fadil Batalli, Mjekesia Ligjore, Priştine 1987, s.46; Artur E. Westveer, "Behavioral Science Unit, FBI", "Managing Death Investigation 1997,U.S. Department of Justice, Federal Bureau of Investigation, s. 425; No. 03/L-187Adli Tıp Yasası, Madde 4, fıkra 2

[133]Mr.Sc. Besim Arifi, Keqyrja e vendittengajres, Sayı I, Priştine 2012, s.97; Edward Hueske, Essentials of Forensics Science- Firearms and fingerprints, Set Editor, Suzane Bell PhD, 2009, s. 115; Dr. Xhemajl Ademaj, Ekspertizat Kriminalistike, Priştine 2010, s. 263-268

[134]Luan Veliqoti, Kriminoloji, Cilt I, Tiran 2015, s. 221.

[135] Prof. Dr. SkenderBegeja, Kriminalistika, Cilt I, Tiran 2001, s.136; Gökcen- Çakır, s.2920.

hayata ve vücuda yönelik suçlar, cinsel bütünlüğe karşı suçlar, terörist saldırılar, insan kaçırma, çeşitli hırsızlık vb. vakalarda meydana gelir.

Son yıllarda DNA analizi teknikleri büyük gelişme kaydetmiştir ve dünyanın birçok ülkesi "veri tabanlarını" (database) kurmuştur. Bu veri tabanlarında suç işleyen bireylerin genetik profilleri ve çözülmemiş davalar için olay yerlerinde bulunan izler arşivlenir. Soruşturma ve kovuşturma aşamasında bu veri tabanlarındaki veriler ile failin saç, tükürük, kıl veya kanından elde edilen DNA'sı karşılaştırılır[136].

Cinsel suçlar işlendiğinde, olay yerinde bulunan spermden de DNA analizi yapılmakta ve diğer delillerle birlikte failin bu suçu işleyip işlemediği anlaşılabilmektedir. Sperm ve sperm lekeleri, mağdurun giysilerinde veya vücut boşluklarında zorla cinsel ilişki durumunda bulunabilir[137].

2.1.6.3. Delil Toplama Usulü ve KCMK Uyarınca Yasal Kısıtlamalar

Yukarıda açıklandığı gibi, usul hükümleri genel olarak ceza yargılamaları sırasında delillerin elde edilme ve ele alınma biçimini ele almaktadır. Ancak, aynı hükümler, delil elde etme şekli ve kaynağı gibi bazı kısıtlamaları öngörmektedirler. Bu kısıtlamalar yargı organlarını delil toplama ve inceleme usulü sırasında daha dikkatli ve profesyonel olmaya zorlamaktadır. Delillerin yürürlükteki yasalara uygun olarak ele alınması, diğer şeylerin yanı sıra, insan haklarına ve özgürlüklerine saygı anlamına gelir. Çünkü, kabul edilemez delillerle sanığın ceza muhakemesindeki haklarının açık bir şekilde ihlal edildiği davalar az sayıda değildir.

Yasal hükümlere uygun olarak elde edilmemiş olan delilleri kabul edilemez delil olarak ilan edecek ve dava dosyasından çıkartılması için öngörülen usullere uygun olarak yapılmasına dikkat etmesi gereken son makam, mahkemedir. Mahkeme hiçbir durumda ve hiçbir nedenle kararını, kabul edilemez deliller (KCMK m.111) temelinde desteklemesine izin vermelidir.

Kosova Ceza Muhakemesi Kanunu, delillerin gerçeği ortaya çıkarabilme imkânına bakmaksızın, delillerin kabul edilemez olarak ilan edileceği birkaç duruma öngörmüştür.

---

[136]Artur Gaxha, GjurmetBiologjikedheroli e rendesia e tyre ne procesinpenal, Tiran 2014, s.2; Prof. LuanMemushi: BiologjiaHumane, Tiran 2006.

[137]ArturGaxha, GjurmetBiologjikedheroli e rendesia e tyre ne procesinpenal, Tiran 2014, s.25.

Aşağıda, böyle bir eylemin gerçekleşmesi durumunda delillerin kabul edilemez olduğu delilleri almanın yasadışı yollarından bazılarını getireceğiz.

1. Sanığın, kendine garanti edilmiş hakların (ana dilini kullanması, sessiz kalma hakki, ücretsiz tercüme, avukat tarafından savunma hakkı, tıbbi muayene hakkı) ihlal edildiği durumlarda ifade vermesi ve onun ifadesi kötü muamele, gözdağı verme, kanunda öngörülemeyen herhangi bir fayda vaadi, hafıza kaybı veya anlama yeteneği olmadığı koşullar sonucu verildiğinde deliller kabul edilemez olur. Sanık sorguya alındığında, yasa, anayasa ve uluslararası eylemlerle güvence altına alınan belirli haklara sahiptir. Kendi dilini veya anladığı dili kullanma hakkı temel bir haktır ve hiçbir nedenle bir sanık anlamadığı bir dilde sorgulanamaz. İfade, anlamadığı bir dilde alınırsa, bir tercümanın bulunması zorunludur. Sessiz kalma ve kendini beyan etmeme hakkına da saygı duyulmalıdır. Bu hakkın ihlali veya her ne pahasına olursa olsun koşulsuz beyan etme yükümlülüğü, kimliğine ilişkin sadece kişisel veriler vermek zorunda olduğu ve daha fazlası olmayan ciddi bir ihlal teşkil etmektedir. Ayrıca, özellikle korumanın zorunlu olduğu suçlarda, sanığın koruma hakkına saygı duyulmalıdır. İfadenin zorla, tehditle, vaatlerle veya hafızasının zayıflamasıyla alınmasıyla ilgili olarak, böyle bir ifade hiçbir koşulda delil olarak kabul edilemez. Aksine, bu gibi durumlarda bir ifade alınırsa, resmi kişinin ceza gerektiren bir suç işlediğini sonucuna serbestçe varabiliriz.

2. Tanık olarak sorgulanamayacak bir kişinin tanık olarak beyanının alınması da kabul edilemez delildir. Bu gibi durumlarda bile, ifade delil olarak kabul edilemez, özellikle de tanık; aile üyeleri, çocuklar, zihinsel ve duygusal rahatsızlıkları olan insanlar gibi tanıklık etmek zorunda olmayan bir kişi olduğunda bu kişilerin beyanlarının alınması kabul edilemez (yasak) delil kapsamındadır.

3. Tanık olma yükümlülüğünden serbest bırakılmış ama bununla ilgili ona haber verilmemiş ya da bu hakkından açık bir şekilde vazgeçmemiş ya da talimat veya vazgeçme tutanakta yazılmadığı durumlarda tanık olarak bir kişi sorguya alınması da kabul edilemez delil kapsamındadır. Tanıklık etmek için serbest bırakılan tanıklar, sanığın eşi veya evlilik dışı eşi, en az beş yıl hapis cezası verilebileceği ve ceza gerektiren suç tarafından yaralanacağı bir ceza gerektiren cezai suç için uygulanması hariç, kan grubu, sanığın ataları ve soyundan gelenleri, erkek kardeşi, kız kardeşi, amcası ve teyzesi ve bu hatlardaki diğer

kişiler, cezai suçun en az on yıl cezalandırılabildiği durumlar veya sanığın birlikte yaşayan veya sanığa ilişkin bir çocuğa karşı cezai suç söz konusu olduğu durumlar hariç. Evlat edinen ebeveyn veya evlat edinilen çocuk, suçun 10 yıldan fazla cezalandırılabileceği durumlar veya bu kişinin birlikte yaşayan çocuğa karşı cezai suçun tanığı olduğu veya sanığa yakın olduğu durumlar dışında ifade veremez. Sanığın veya başka bir kişinin itirafta bulunduğu dindar kişi, görevlerini yerine getirirken ve öğrendikleri şeyleri gizli tutmak zorunda olduklarında bu gerçekleri öğrenmiş olan savunma avukatı, mağdurun savunma avukatı, doktor, sosyal hizmet uzmanı, psikolog vb. kişilerin tanık olarak beyanı alınamaz (KCMK. m.127/1).[138]

4. Tanıklık yapmayı reddetme hakkını anlamayan bir çocuk, tanık olarak sorguya alındığında, ya da çocuğun bir suça tanık olması halinde ifadelerini alma ve bunların delil olarak kullanılması, çocukların yaşı ve olgunlaşmamış olmasından ötürü usule dair neticeler doğurabilir. Devlet organları çocukların ifadelerine atıfta bulunamaz ve bunlara güvenemez ve bunları kabul edilebilir delil olarak sunamaz ve değerlendiremez.

5. Tanığın ifadesi, zorla, yıldırma ya da benzeri yasaklanmış başka yollarla elde edildiğinde kabul edilemez olur. Zorla, tehditle veya benzeri bir biçimde delilin alınması, ifadeyi tamamen kabul edilemez kılar. Bu yasadışı önlemlerin uygulanmasıyla, gerçeği açıklığa kavuşturmak için gerekli her türlü bilgi elde edilebilir, ancak buna rağmen şiddet, işkence, yıldırma, hipnoz vb. kullanımı haklı değildir[139].

6. Hukuk uzmanı olarak görevlendirilemediği durumlarda uzmanın ifadesidir. Yasal hükümler, tam olarak hangi kişilere ve hangi şekilde ceza davası için uzman atanabileceğini belirtir. Sadece ilgili niteliklere sahip kişiler veya kurumlar uzman olarak atanabilir, aksi takdirde delillerden herhangi biri kabul edilemez delil olarak kabul edilecektir.

7. Devlet savcısı veya polis tarafından olay yerinin incelenmesi veya yeniden yapılandırılması işleminin, sanık veya savunma avukatına böyle bir işlem bildirilmediğinde, elde edilen deliller kabul edilemez olacaktır. Bu kurallardan herhangi bir sapma, delilin kabul edilemez olarak beyan edilmesine neden olur. Uygulamada, ön

[138]Ejup Sahiti, Rexhep Murati, Cezai Usul Hakkı, Priştine, 2016, s.269.

[139]EjupSahiti, RexhepMurati, XhevdetElshani, Kosova Cumhuriyeti Ceza Muhakemesi Kanunu Yorumu, Priştine, 2014, s.680.

duruşma yargıcının veya savcının olay yerinde görünmediği sık görülen durumlar vardır. Sanığın savunma avukatının, bu işlemler yapıldığında çağrılmaması da genelde olabilmektedir. Yasal yükümlülüğü olan ve hazır bulunma zorunluluğu olan bu kişilerin olay yerinde bulunmaması, olay yerinin incelenmesine katılan polis, savcılık veya başka bir organ tarafından çok sayıda manipülasyon imkânı sağlar. Bu durumlarda, olay yerinde bulunan herhangi bir delil kabul edilemez delil olarak kabul edilecektir.

8. Ceza muhakemesi hükümlerine aykırı olarak kişinin, evin veya diğer binaların aranması yapıldığında (ön duruşma hâkimin emri olmadan, uygulanan emre aykırı kontrolün uygulanması vb.) Bir aramanın yapılması sırasında, özellikle faili doğrudan olay yeri ve suçla ilişkilendiren önemli deliller bulunabilir. Ancak, bu delillerin kabul edilebilir olması için, herhangi bir aramanın yasal kısıtlamalara uygun olarak yapılması yasal bir zorunluluktur. Çünkü, aramanın bir emir olmadan yapılması halinde, insan hakları ihlal edildiğinde, baskının kanunla belirlenen sürenin dışında sonuçlandığı gibi hallerde, bu yerde değerli bir delil bulunmasına rağmen, mahkemede kabul edilebilir delil olarak kabul edilemez.

9. Delil, hukuka aykırı bir karara dayanan gizli ve teknik bir gözetim ve soruşturmayla elde edildiğinde (KCMK m.88 ila 94), kabul edilemez hale gelebilir. Bu tedbirlerin uygulanması birçok suçun ve faillerinin bulunmasına yol açmaktadır, ancak bir suçun ortaya çıkarılmasında bu önlemlerin uygulanmasının önemine rağmen, yargı organları, mahkeme kararında belirtilen yasal hükümleri ve kısıtlamaları, uygulanacak tedbirin kesin olarak belirlenmesini, tedbiri uygulayacak ve tedbirin uygulanacağı kişileri, süre sınırlamasını ve herhangi diğer yasal kısıtlamaları kesinlikle uygulanmalıdırlar. Bu hükümlerin her ihlali, bu delillerin yetkili mahkeme tarafından dava dosyasından ayrılacak kabul edilemez delil olarak beyan edilmesine neden olur.

Ayrıca kanun koyucu KCMK'nin257. maddesinin 4. paragrafı uyarınca aşağıda belirlenenlere yol açan her tür sorguyu yasaklamıştır:

1. Sanığın görüşünü oluşturma ve ifade etme özgürlüğü kötü muamele, yorgunluk, uyuşturucu kullanımı, işkence, baskı ya da hipnozdan etkilendiğinde.

2. Sanık, yasa uyarınca yasak tedbirlerle tehdit edildiğinde;

3. Yasalarca öngörülmeyen herhangi bir fayda vaat edildiğinde ve

4. Sanığın hafızası veya anlama yeteneği zayıfladığında.

Bu yasadışı eylemler, sanığın kabulü olduğu durumlarda bile delili hukuki hale getirmez (KCMK 257. maddesinin 5 ve 6. paragrafları). Yasa, sanıklara aslında kabul etmediği bir şeyi kabul ettiği varsayımına dayanarak soruların sorulmasını da yasaklamaktadır.

2.2. Dijital Delillere İlişkin Kosova ve Türkiye Uygulamalarının Karşılaştırılması

2.2.1. Dijital Delil Kavramı

Türk ceza muhakemesi sisteminde delil serbestisi ilkesi egemen olduğundan, hukuka uygun her türlü delil hâkimin vicdani kanaatinin oluşmasına yardımcı olabilecektir. Bu kapsamda delil serbestisi ilkesi dikkate alındığında dijital delillerin de delil değerine sahip olduğu söylenebilir. Teknolojinin gelişmesiyle birlikte bilişim teknolojisinin çeşitlenmesi, özellikle de bilgisayar teknolojilerinin gelişimi ile birlikte dijital delillerin ulaşma ve bunları hukuka uygun şekilde elde etmenin önemi ortaya çıkmıştır. Modern dünyada başta bilgisayar, akıllı telefon, tablet gibi araçlarla işlenen suçların da bu teknolojinin ilerlemesiyle bir değişim geçirdiği dikkate alındığında, dijital deliller gittikçe artan şekilde hukuk âleminde kendilerine daha fazla yer bulmaktadırlar. Bilhassa "bilişim suçları"nın sayısal olarak artması ve çeşitlilik göstermesinin yanında, geleneksel suçların da bilişim yöntemleri kullanılarak işlendiği görülmektedir. Bu kapsamda her tür suça ilişkin olarak dijital delil elde edilebileceği akla gelmektedir[140].

Bununla birlikte, bu noktada değinilmesi gereken bir başka husus ise bilişim suçları kavramından ne anlaşılması gerektiğidir. Bilişim suçu kavramına ilişkin doktrinde bir tartışma bulunmaktadır. *Yazıcıoğlu*[141]bilgisayar suçları kavramını kullanırken, *Sınar* ve *Ergün*[142] ise "siber suç" terimini kullanmaktadır. Ancak doktrinde baskın görüş "bilişim suçları" terimini kullanmaktadır[143].Türk Ceza Kanunu (TCK) m.243 ila 245 arasındaki

---

[140] Uğur Kaynakçıoğlu, Ceza Muhakemesinde Dijital Deliller, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2015, s.21

[141]Bilgisayar suçları kavramı için bkz. Yılmaz Yazıcıoğlu, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul: Alfa Yayınevi, 1997.

[142]Siber suç kavramı için bkz. Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul: Beta Yayınevi, 2001; İsmail Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara: Adalet Yayınevi, 2008.

[143] Bilişim suçları kavramı için bkz. Caner Yenidünya/Olgun Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişm Suçları, İstanbul: Legal Yayıncılık, 2003; Hatice Akıncı/A. Emre Alıç/Cüneyd Er, "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk, Yeşim Atamer (der.), İstanbul: İstanbul Bilgi

suçlar da bilişim suçları olarak tanımladığından, bu tanımın kullanılmasının doğru olduğu kanaatindeyiz. Kosova Ceza Kanunu'nun "Bilgisayar sistemlerine girme" başlıklı m.327'de yetkisiz ve kendisine veya başka bir şahsa yasadışı kazanç elde etmek veya diğer bir şahsa zarar vermek maksadıyla bilgisayar verilerini değiştirmesi, yayımlaması, silmesi, imha etmesi veya tahrip etmesi veyahut başka şekilde diğer herhangi bir kişinin bilgisayarına girmesi eylemleri cezalandırılmıştır. Bununla birlikte, yetkili olmayan bir kişinin bilgisayar veri tabanına müdahale etmesi veya bu verileri kullanması veyahut başka birisine vermesi eylemleri suç olarak kabul edilmiştir. Yine KCMK m.203/3'te "bilgisayar ağı" kavramı kullanılmış olup, bu maddelerde bilişim suçları gibi genel bir kavram yer almamıştır.

Öte yandan, dijital delillerin kullanıldığı olaylarda, hâkimin suça ilişkin sorunları çözmesi de daha kolay hale gelmektedir. Bazen somut olayın, örneğin sosyal medya üzerinden hakaret ve cinsel taciz gibi, dijital delillere ulaşılmadan çözülmesi olanaklı değildir. Bu sebeple bu deliller, zaman içinde geleneksel delillere oranla daha ulaşılabilir duruma gelmişlerdir. Her geçen gün soruşturma ve yargılama makamlarının ceza muhakemesi alanındaki dijital delil barındıran suçlarla karşılaşma sıklığı da yükselmektedir[144]. Bu bağlamda dijital delilin ne olduğunun belirlenmesi de önem kazanmaktadır.

Dijital delil kavramı, henüz hukuken ayrıntılı şekilde tanımlanmasa da doktrinde çeşitli tanımlar yapılmıştır. Doktrinde bir görüş dijital delilleri, *adli bilişime ilişkin bir çalışma sırasında, bilgisayarlar, akıllı telefon, dijital fotoğraf makineleri ve bu çerçevedeki depolama aletleri üstünden ele geçirilen adli deliller* şeklinde tanımlamıştır[145].

Bazı eserlerde dijital delil yerine elektronik delil[146] kavramının kullanıldığı görülmektedir. Bu görüşü savunanlar elektronik delili, bir elektronik aygıt üstünde yer alan ya da bu aygıtlar vasıtasıyla iletilen, ceza muhakemesi bakımında değeri olan veriler şeklinde

---

Üniversitesi Yayınları, 2004; Muammer Ketizmen, Türk Ceza Hukuku'nda Bilişim Suçları, Ankara: Adalet Yayınevi, 2008; Zakir Avşar/Gürsel Öngören, Bilişim Hukuku, İstanbul: Pasifik Ofset, 2010; Ali Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014 ve Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 6. Baskı, Ankara: Seçkin Yayıncılık, 2015 (Bilişim Suçları).

[144]EoghanCasey, DigitalEvidenceandComputerCrime: ForensicScience, Computersandthe Internet, 3. Edition, Londra: AcademicPress, 2011, s. 9 (DigitalEvidence).

[145] Türkay Henkoğlu, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, 2. Baskı, İstanbul: Pusula Yayıncılık, 2014, s. 5.

[146] Dijital deliller ile elektronik deliller arasında fark bulunup bulunmadığı aşağıda açıklanacaktır.

adlandırmıştır[147]. Yabancı doktrindeki eserlerde de hem elektronik delil hem de dijital delil kavramının değişken şekilde kullanıldığı anlaşılmaktadır[148]. Doktrindeki bu çalışmalara bakıldığında dijital delili kavramı üzerinde uzlaşı olmadığı ve bu kavram yerine elektronik delil kavramının kullanıldığı görülmektedir.

2.2.1.1. Dijital Delil ve Elektronik Delil Kavramların Arasında Benzerlik ve Farklılıklar

Dijital delil ile elektronik delil terimleri, birbirlerinin yerine ve gerekli özen gösterilmeksizin kullanılmakta olup, bu deliller arasındaki benzerlik ve farklarının anlaşılabilmesi amacıyla dijital ve elektronik kavramlarının açıklanması gerekmektedir[149].

2.2.1.1.1. Elektronik Kavramı

"Elektronik" kavramı maddenin eksi yüklü elektronların hareketlerinden faydalanarak farklı donanımları meydana getirme bilimi anlamına gelmektedir. "Elektronik", maddenin elektriksel özelliklerini kullanan bilgisayar, radyo, televizyon gibi birçok aygıtın esasını oluşturur[150]. Bu nedenle elektronik deliller elektronik bir araç vasıtasıyla işlenen, depolanan ya da gönderilebilen ve adli anlamda değeri olan verilerdir[151].

Yine elektronik kavramı ile iç içe olan sinyal terimi ise, bütün elektronik hareketlerin matematiksel fonksiyon şeklinde gösterilmesidir. Başka bir deyişle sinyal, elektronik veri hareketini sembollerle gösterir. Bu veriler, analog ve dijital şeklinde ikiye ayrılır ve dijital veriler de elektronik aygıtlar içinde kullanılan bir çeşit sinyal türüdür. Bu açıklamalardan anlaşıldığı gibi, elektronik terimi, dijital terimine oranla daha kapsamlı ve daha üst bir ifadedir[152].

---

[147] Leyla Keser Berber, Adli Bilişim, Ankara: Yetkin Yayınları, 2004, s. 46; Aynı görüş için bkz. Ergün, s.49; Karagülmez, s.443.

[148] Dijital delili tercih edenler için Bkz. s. 279 EoghanCasey ve Orin S. Kerr, "DigitalEvidenceandthe New CriminalProcedure", Columbia LawReview, Ocak 2005, vd.; her iki kavramı da aynı anda kullananlar için bkz. Stephen Mason, "Introduction", Stephen Mason (ed.), International Electronic Evidence, Londra: British Institute of International andComparativeLaw, 2008.

[149] Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil. Ankara: Seçkin Yayıncılık, 2014, (Dijital Delil), s. 453.

[150]Karagülmez, s.38.

[151]Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk, Ankara: Ankara Barosu Yayınları, 2009, s. 173.

[152] Yusuf Başlar, Ceza Yargılamasında Elektronik Delil, Yetkin Yayınları, Ankara 2016, s.63.

Analog kelime anlamı olarak benzer eş anlamına gelmekle birlikte, "analog sinyaller", girişe yarayan sinyalinin diğer sinyallerle elektriksel aşamalardan geçirilmesiyle elde edilir. Giren ve çıkan sinyaller arasında süreklilik ve çok çabuk değişim olduğundan, sonsuz sayıda ara değer bulunabilir. Bu yüzden, analog verilerle oynama, olanaksız olmasa da çok zordur[153].

2.2.1.1.2. Dijital Kavramı

"Dijital" kelimesi sözlükte "sayısal" anlamına gelmektedir[154].Elektronik cihazlar içindeki elektronik veriler, ikili sayı sistemi olan 0 ve 1'lerden oluşmakta olup,dijital sinyal ise, bu ikili kod sisteminin kullanılmasıyla meydana getirilir[155]. Bu sistemde veriler sayıların ardışık dizilmesiyle elde edildiğinden üzerlerinde kolayca değişiklik gerçekleştirilebilir. Buna ilave olarak, hata düzeltme kodları eklenerek bir dijital veri, bozulsa dahi tamiri temin edilebilir. Ayrıca, bir dijital veri nakledilirken farklı bir dijital veriyle aynı yere konulup nakledilebilir ve şifrelenebilir.

Dijital verilerin sadece yalnızca belirli değerlerden meydana gelen, sayılarla sınırlı olan, süreksiz olan bir ölçekte ve kesikli şekilde var olan verilerdir. Günümüz imkânları ile analog veriler dijitale, dijital veriler analoğa kolayca dönüştürülebilmektedir[156].

2.2.1.1.3. Dijital Delil ve Elektronik Delil Kavramının Karşılaştırılması

Bir suçun açığa çıkarılmasına yönelen delil ele geçirme çabaları dijital ortamdaki verilerin okunmasını gerektirir. Diğer bir deyişle arama sırasında veya olay mahallinde elde edilen bir USB bellek değil de, bu bellek içindeki sayısal veriler adli anlamda incelemenin esas konusunu oluşturur. Öte yandan, bir adli kolluk görevlisi olay mahalline vardığında, verilen adli emir doğrultusunda toplayacağı deliller içinde sayısal verileri de içeren elektronik aygıtlar da bulunacaktır. Bu kapsamda adli soruşturmada ele geçirilen ve suçla ilişkisi incelenecek USB bellek elektronik delil niteliğindedir[157].

---

[153]Karagülmez, a.g.e. , s. 41.

[154]https://sozluk.gov.tr/, erişim tarihi: 04.03.2022.

[155]Karagülmez, a.g.e. , s. 41.

[156] Fatoş Tünay Yarman-Vural, / Yusuf Murat Erten, Bilgisayar Sistemleri, 5. Baskı, Ankara: Akademi Yayıncılık, 2000, s. 281 .

[157] Hakan Aydoğan, "Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri", Yayınlanmamış Yüksek Lisans Tezi. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara 2009., s.30.

Yukarıda açıklandığı üzere bazı yazarlar, hem analog hem de dijital kavramını kapsadığı için dijital yerine elektronik ve elektronik delil kavramlarını kullanmayı tercih etmektedirler[158]. Ancak, analog delillerin, dijital delil sayılması mümkün olmadığından, bu deliller açısından farklı hukuki düzenlemeler yapılması gerekmektedir[159].

Daha önce de ifade edildiği üzere, elektronik yapısı olan her aygıtın dijital verisinin bulunduğundan söz edilemez[160]. Dijital delillerin; elektronik yapıda bulunduğu bir gerçek olsa da, yalnızca dijital durumda bulundukları hallerde dijital delil anlamında değerleri olacaktır. Başka bir deyişle, bu açıklamalar karşısında teknik anlamda bu çeşit delillerin de elektronik delil şeklinde değil, dijital delil şeklinde tanımlanmaları daha isabetli olacaktır. Bu şekilde elektronik delil-dijital delil karmaşası sona erecektir. Kaldı ki doktrinde elektronik delil kavramı kullanılsa bile, burada bahsedilen elektronik aygıtın içindeki dijital teknolojiye yönelik olacaktır.

Elbette dijital delil kavramının şimdilik dezavantajı, yasalarda açıkça bu terimin kullanılmamasıdır. Türkiye'de yürürlükteki hukuki düzenlemeler içinde elektronik, analog ve dijital terimlerinin yer alıp almadığına hem elektronik hem de az olmakla birlikte dijital kavramlarının kullanıldığı kanunlar bulunmaktadır.

CMK'de genellikle "elektronik" kavramının tercih edildiği görülmektedir. Örneğin CMK m.38/A'da UYAP üstünden gerçekleştirilecek elektronik işlemler yer almıştır. Yine CMK m. 43/2'de tanıkların çağrı usullerinde elektronik posta gibi araçlardan yararlanılabileceğinden söz edilmektedir. "Analog" ve "dijital" kavramlarına CMK'da yer verilmediği görülmektedir. Ayrıca TCK'da "elektronik" kavramının yer aldığı anlaşılmaktadır (m. 6/1-g, m.297/1). Bu Kanunda da "analog" ve "dijital" kelimeleri kullanılmamıştır.

Kosova hukukunda KCMK m.19/1.27, m.89, m.91/2 ve m.105/8'e bakıldığında "dijital" kavramı yerine "elektronik" kavramının tercih edildiği görülmektedir. Ancak Sibernetik Suçla Mücadele ve Önlenmesine Dair Kanun'da elektronik veya dijital kavramlarına yer verilmemiştir.

---

[158] Başlar, s.64.

[159] Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk, s. 173

[160] Karagülmez, s. 41.

Öte yandan, Türk hukukunda 5651 sayılı Kanun m. 3/3, m. 6/A-5 ve Ek Madde 1'de "elektronik" kavramının kullanıldığı, "analog" ve "dijital" kelimelerinin kullanılmadığı görülmektedir[161].

2.2.1.2. Veri Kavramı

Dijital delil kavramını oluşturan temel unsur veri kavramı olduğundan, dijital delili ile veri arasında yakın bir ilişki vardır. Bu ilişkinin esas nedenlerinden biri de, veri kavramının, gerek dijital delilin çekirdeğini oluşturması, gerekse ulusal ve uluslararası hukuk düzenleri tarafından kabul gören yerleşmiş bir kavram olmasıdır.

Sözlük anlamı olarak veri, "bilgi, data" anlamlarına gelmekle birlikte[162], bilişim sözlüğü açısından "*Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*" şeklinde tanımlanmıştır[163].

Türk mevzuatına bakıldığında bazı kanunlarda veri ve elektronik verinin tanımının yapıldığı görülmektedir. Örneğin 5651 sayılı Kanun m.2'de veri, "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer; bilgi ise, verilerin anlam kazanmış biçimi*" şeklinde ifade edilmiştir[164].

Veri, farklı kanunlarda niteliği gereği değişik şekillerde tanımlanmış olmakla birlikte, bütün tanımlarda verinin bir kayıt veya bilgi anlamına gelmesinin yanı sıra çoğunlukla hukuksal bir terim ve çekirdek değer olduğu görülmektedir. Çekirdek değere sahip olan

---

[161] "Elektronik" kelimesi 5070 sayılı Elektronik İmza Kanunu'nun gerek adında gerekse içeriğinde kullanılmış, "analog" ve "dijital" kelimeleri ise yer almamıştır. 5809 sayılı Elektronik Haberleşme Kanunu ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da da "elektronik" kavramı temel alınmıştır.

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 5. maddesinde "elektronik" kelimesi yer almışken, 25. ve 72/1. maddelerinde "dijital" kelimesi bulunmaktadır ve "analog" kelimesi de yoktur. 6502 sayılı Tüketicinin Korunması Hakkındaki Kanun'un 3/f, 3/h, 6/1, 49/2, 77/17 ve 80 maddelerinde de "elektronik" kelimesiner yer verilmişken, "analog" ve "dijital" yine yer almamıştır. Sonuç olarak Türkiye'deki yasal düzenlemelerinde elektronik kavramının kullanıldığı ve "dijital" kelimesinin çok az yer aldığı görülmektedir.

[162] https://sozluk.gov.tr/, erişim tarihi: 04.03.2022.

[163] https://sozluk.gov.tr/, erişim tarihi: 04.03.2022.

[164] 5070 sayılı Elektronik İmza Kanunu m.3. maddesinde elektronik veri; "elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar" şeklinde tanımlanmıştır. Ayrıca 6698 sayılı Kişisel Verilerin Korunması Kanunu m.3/1-d'de kişisel veri; "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi (…) ifade eder" biçiminde tanımlanmıştır.

veriler, hem dijital hem de elektronik delillerin esas unsurunu meydana getirmektedir. Hukuki düzenlemelerde debu ortak çekirdek değer,atıf yapılacak temel kavram olmalıdır[165].

2.2.1.3. Bilişim Kavramı

Bilişim kavramı[166] bir endüstrinin bütününü içinde barındıran bir üst kavram olmasa da, kelimenin türetilmesinde bilgi-işlem ve iletişim terimlerinin birleştirildiği anlaşılmaktadır. Bu nedenle bilişim, bilgi-işlem ve iletişime ilişkin işlevlerin birlikte bulunduğu elektroniğin ifadesi de olmaktadır[167].

Ayrıca bilişim bilimi, hukukta dijital delillerin anlamının anlaşılabilmesi için gereken yardımı sağlayacaktır. Bilişim bilimi sayesinde, elektronik aygıtlardan elde edilen bilgi veriler, beş duyuyla algılanabilir ve mantıksal şekilde düzenlenerek anlamlandırılabilir duruma getirilir. Bu şekilde yargılama makamları, bilgi, belge ve izlerden meydana gelen dijital delilleri yorumlayabilir duruma geleceklerdir. Tıp biliminin hukuk alanındaki yorumlayan adli tıp bilimlerinde olduğu gibi, dijital delillerin de elde edilmeleri, incelenmeleri ve yorumlanmaları bakımından kullanılan yöntemler konusunda yardım alınan bilim dalı adli bilişim olarak adlandırılmıştır[168]. Bu şekilde adli bilişimin de adli bilimler içinde bir alt dal haline geldiği söylenebilir[169].

2.2.2. Dijital Delillerin Kendine Özgü Özellikleri

2.2.2.1. Gizli Bir Yapılarının Olması

Dijital deliller, parmak izi veya DNA gibi gizli bir yapıda bulunurlar[170]. Klasik delillerden farklı olarak, bu delillerin tespitlerinin ilk anda yapılması olanağı bulunmamaktadır. Başka bir deyişle, dijital deliller bazı vasıtalar ya da usullerle somut, duyularıyla algılanabilecek

---

[165]Kaynakçıoğlu, s.30

[166] Sözlük anlamı ile bilişim, "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" şeklinde tanımlanır.

[167] Akıncı, Alıç, Er, s. 170; Değirmenci, Dijital Delil, s.53.

[168] Keser Berber, a.g.e. , s. 39

[169] Değirmenci, Dijital Delil, s.65.

[170] Kubilay Say, "Data İncelemeleri", Oğuz Karakuş (ed.), Kriminalistik, Ankara: Adalet Yayınevi, 2. Baskı, 2013, s. 521; Mustafa Göksu, Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayınevi, 2011, s. 30; Keser Berber, s. 44; Council of Europe (CoE), Electronic Evidence Guide, 2013, s. 11, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/2467_EEG_v18protected.pdf (Erişim tarihi: 01.04.2022).

bir hale getirilmeye gereksinim duyulur[171]. Bunu gerçekleştirecek aygıtlar, elektronik aygıtlardır.

Elektronik aygıtlar, somut yapıya sahip olduklarından olay mahallinde dijital deliller toplanırken bu aygıtlar önemli olacak ve bu aygıtların kullandığı dijital uygulamalar ve veriler de dijital delillerin somutlaştırılmasını sağlamaktadır. Bazı durumlarda aygıtın kendisi, bazen de verinin özelliği sebebiyle, dijital delillerin elde edilmesi belirli bir süre ya da özel bir usulün kullanılmasını gerektirmektedir. Bu yüzden dijital delilin bu gizli yapısını meydana çıkaracak belirli kişilere gereksinim duyulmaktadır. Bu şahıslar yasalarda delil toplamada yetkili kılınmış adli kolluk ve onlara teknik uzmanlıkları ile yardımcı olacak adli bilişim uzmanlarıdır. Bu adli bilişim uzmanlarının raporları, dijital delilin gizli yapısının açığa çıkarılmasında önemli olacak ve hâkimlerin vicdani kanaat oluşturmasına yardımcı olmaktadır[172]. Uygulamada adli bilişim uzmanları, hazırladıkları raporların başlangıcında adli bilişim konusunda üniversite eğitimleri, aldıkları eğitimler ve kursları, rapor hazırladıkları adli dosyalara ilişkin bilgi vermektedirler. Bu kapsamda adli kolluk uzmanlarının da raporlarında bu bilgilerin yer alması, bu alandaki yetkinliklerini göstermeleri açısından önemli olacaktır.

2.2.2.2. Kopyalanabilir Olma

Dijital delillerin geleneksel delillere oranla en önemli özelliklerinden biri de kopyalanabilir olmalarıdır[173]. Dijital veriyi oluşturan kod dizilimini aygıt içine ya da dışına aynı şekilde nakledebilmek amacıyla bir komut sistemi vardır. Bu şekilde dijital verilerin, sonsuz sayıda kopyalanabilmesi mümkündür. Bilgisayar, cep telefonu gibi bazı aygıtlar yedekleme olarak adlandırılan bir özellik ile otomatik bir kopyalama sistemine de sahip olabilirler. Bu özellik dijital delillerin incelenmesini hızlandırabilir. Çünkü birden fazla bilişim uzmanının aynı anda orijinal verinin içeriğinin aynısını barındıran kopya veriyi[174] inceleme olanağına sahiptirler ve bu deliller bu özelliğiyle mahkemeye de kolay şekilde sunulabilirler

---

[171] Göksu, a.g.e. , s. 30; Dülger, Bilişim Suçları, s. 751.

[172]Kaynakçıoğlu, a.g.e., s.38.

[173]CoE Electronic Evidence Guide, s. 12.

[174] Değirmenci, Dijital Delil, s. 140.

2.2.2.3. Kolaylıkla Değiştirilme, Bozulma ve Yok Edilebilir Olma

Dijital deliller, yapılarından ötürü kolayca değiştirilebilir, bozulabilir ve yok edilebilir özelliktedirler[175]. Bilgisayar gibi depolama birime sahip bazı elektronik aygıtlarda, gerçekleştirilen işlemler dijital veri şeklinde önceden kaydedilen dijital verinin üstüne yazılabilmektedir. Bu hal elektrik gücünün kesilmesine karşı önlem olmakta veya aygıtın bir özelliği de olabilmektedir.

Ayrıca dijital veriler, bu alanda uzman olmayan kişilerce dek olaylıkla değiştirilebilir, bozulabilir ve yok edilebilirler. Bu özellik dijital delillere daha özenli davranılmasını gerektirse de, değiştirme, bozma ve yok etmeye ilişkin eylemlerin belirlenmesinin uzmanlar tarafından yapılabileceğini göstermektedir. Öte yandan, bir verinin içeriği aynı olsa dahi, değişik elektronik aygıtlardan ya da farklı dijital usullerle somut hale getirildiğinde, çok değişik biçimlerde açığa çıkabilmektedir[176].

2.2.2.4. Yaygın ve Uluslararası Olabilme

Dijital deliller, dünya çapında bir alana dağılmış olabilirler[177]. Bilhassa bilgisayar ve cep telefonları gibi elektronik aygıtların internet aracılığıyla birbirleriyle bağlantılı olması, dijital delillerin çok geniş alana yayılabileceğini göstermektedir. Bu durum, dijital delilin elde edileceği kaynağın tespitinde sorun yaratmaktadır. Öte yandan delilin kaynak yeri tespit edilse dahi, bu yerin muhakeme işleminin yapıldığı ülkenin yetki alanı dışında bulunması hali de sorun oluşturmaktadır. Örneğin internet ağları veya bulut teknolojileri gibi uluslararası niteliği olan teknolojilerin içinde olan verilerin kaydedildiği aygıtlar,farklı bir ülkede bulunabilir. Bu halde delillerin ele geçirilmesi sorunu da uluslararası bir niteliğe sahip olmaktadır. Bu gibi durumlarda uluslararası adli yardımlaşma taleplerinin karşılanma yetersizliği, dijital delillerin elde etmeye ilişkin de olumsuz neticeler meydana getirmektedir.

---

[175] Keser Berber, a.g.e. , s. 46; CoE Electronic Evidence Guide, s. 11.

[176] Göksu, a.g.e. , s. 33.

[177] Say, a.g.e., s.521; John Ashcroft (Ed.), "Electronic CrimeSceneInvestigation: A Guide for First Responders", Washington: PhotoDisc, Inc, 2001, s.6, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (erişim tarihi 25.03.2022).

2.2.2.5. Kime Ait Olduğunun Belirlenmesinin Zorluğu

Dijital delillerin dünyaya yayılmış olmasının nedeni, herkesçe kolayca üretilebilmesidir. Fakat üreten kişinin tespiti kolay değildir. Çünkü dijital verilerin,bilhassa internet ağında anonimlik temelinde büyüdüğü ve üretildiği görülmektedir. Bilgi kaynağındaki bu anonimlik kavramı ile dijital verilerin kime ait olduğunun tespiti zorlaşmaktadır[178]. Bilginin üretildiği kaynağa ulaşılsa da bilgi veya delili üreten kişinin, kaynağın sahibi olduğunu ispatlamak zordur. Bu sebeple ceza muhakemesinde bazı karineler oluşturma ihtiyacı hissedilecek ve aidiyetin kanıtlanması bakımından, güvenli elektronik imza gibi yeni kurumlar meydana çıkmaktadır[179].

2.2.3. Dijital Delillerin Elde Edilmesi ve İspat Gücü

2.2.3.1. Delillerin Elde Edilmesi

2.2.3.1.1. Genel Olarak Delillerin Elde Edilmesi

Dijital delillerin ele geçirilmesi ve kanıt kuvveti sorunu, ceza muhakemesindeki teknik ve sorunlu alanlardan ikisini meydana getirmektedir. Dijital delillerin elde edilmesi esnasında meydana çıkan sorunlar, bu delillerine ispat kuvvetini de doğrudan etkilemektedir.

İlk olarak ceza muhakemesinde delilin ne zaman toplanmaya başlanacağı meselesi halen tartışmalıdır. Bir görüş, yalnızca soruşturma safhasında delil toplamanın olanaklı olduğunu ve soruşturma safhasında gerçekleştirilen işlemlerle hukuka uygun şekilde toplanan kanıt araçlarının delil niteliğine sahip olduğunu ifade etmektedir[180]. Bir başka görüş ise, deliller, soruşturma safhasında elde edilse de, kovuşturma safhasında da delil toplanmasının önünde engel bulunmamaktadır[181]. Bu görüşü destekleyen başka bir yazar ise, soruşturma safhasında ele geçirilen ispat araçları sadece şüphe sebepleri şeklinde tanımlanabilirler. Bu şekilde ispat araçlarının delil şeklinde tanımlanabilmesi sadece mahkeme yargılaması safhasında olanaklı olacaktır[182].

---

[178] Göksu, a.g.e. , ss. 31-32.

[179] Göksu, a.g.e. , s. 32.

[180] Ali Parlar/ Muzaffer Hatipoğlu/ Erol Güngör Yüksel, Açıklamalı-İçtihatlı Ceza Muhakemesi Hukukunda Deliller, Çapraz Sorgu ve İspat, Ankara: Yayın Matbaacılık, 2008, s. 512.

[181] Centel/Zafer, a.g.e. , s. 75, 597.

[182] Kunter/Yenisey/Nuhoğlu, a.g.e. , s. 1338.

Ceza muhakemesinde delil elde etmeye başlanabilmesi için, ilk olarak kanunda yer alan durum meydana gelmelidir. Bu durum; savcının, ihbar ya da farklı şekilde bir suçun işlendiği halini öğrenmesi, diğer bir deyişle, bir suç şüphesinin oluşmasıdır. Savcının soruşturmayı başlatabilmesi amacıyla ilk olarak önüne gelen olayda basit suç şüphesinin var olduğunu belirlemesi gerekecektir. Fakat doktrinde, suç şüphesinin öğrenilmesi ile soruşturmanın başlangıcı arasında da delillerin araştırılmasında bilgi toplama süreci olarak adlandırılan bir geçiş sürecinin de olabileceğinden söz edilmiştir[183].

Soruşturma işlemlerini başlatan savcı, dava açıp açmayacağına karar vermek üzere gerçeğin araştırılması için kolluk görevlileri vasıtasıyla, şüphelinin leh ve aleyhindeki delilleri elde etmekle mükelleftir (CMK m.160). Elde edilen deliller, suçun işlendiği hususunda yeterli şüphe meydana getiriyorsa, savcı iddianame düzenler. Diğer bir deyişle, kamu davası açılabilmesi için, suç işlendiğine dair basit şüphenin, toplanan deliller sayesinde yeterli şüpheye oluşması gerekir. Savcının emrinde olan adli kolluk görevlileri, delillerin toplanmasına ilişkin görevleri icra edecek şahıslardır. Bu durum, delil toplama işlemlerini icra edecek kişilerin kimler olduğunu göstermektedir. Adli kolluk, kendi kuruluş yasaları ve ilgili yasalara göre polis, jandarma ve sahil güvenlikten meydana gelmektedir (CMK m.164)[184]. Fakat delil toplanması teknik bir işlem olduğundan adli kolluk görevlisi de işin niteliğine uygun olarak farklı meslek gruplarındaki şahıslardan seçilmelidir[185]. Bilhassa dijital deliller gündeme geldiğinde bu durum bir gereksinim olmaktadır.

Yeterli şüphe oluşmasıyla hazırlanan iddianamenin kabulü sonucu başlayan kovuşturma safhasında da delil toplanması olanaklıdır (CMK 177). Bu safhada delil toplama işlemlerinin idaresi, hâkime aittir. Fakat hem soruşturma hem de kovuşturma safhasında dijital delillerin toplanmasında diğer delil elde etme yöntemlerinden yararlanılabilir.

Beyan delillerinin kaynağı kişiler olup, CMK m.2 uyarınca, şüphelinin kolluk görevlileri ya da savcısı tarafından suça ilişkin dinlenmesi ifade alma şeklinde tanımlanırken, sorgu ise

---

[183]Centel/Zafer, a.g.e. , s. 76.

[184] CMK m.164/1: "Adlî kolluk; 4.6.1937 tarihli ve 3201 sayılı Emniyet Teşkilatı Kanununun 8, 9 ve 12 nci maddeleri, 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun 7 nci maddesi, 2.7.1993 tarihli ve 485 sayılı Gümrük Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8 inci maddesi ve 9.7.1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanununun 4 üncü maddesinde belirtilen soruşturma işlemlerini yapan güvenlik görevlilerini ifade eder".

[185] Yıldızhan Yayla, İdare Hukuku, 2. Basım, İstanbul: Beta Yayınevi, 2010, s. 42

şüpheli ya da sanığın mahkeme ya da hâkim tarafından muhakemeye konu suça ilişkin olarak dinlenmesini ifade etmektedir[186].

Ceza yargılamasındaki uyuşmazlığın taraflarından birisi olmasa da, suça konu olayı gören veya duyan, bu olaya ilişkin duyu organlarının bir ya da birkaçı vasıtası ile bilgi edinen ve elde ettiği bilgileri yargılama makamlarına ifade eden üçüncü kişilere tanık, tanığın söylediklerine ise tanık beyanı adı verilir[187]. Beyan delilinin elde edildiği bir diğer kişi mağdur veya şikayetçidir. Mağdur ve şikâyetçinin beyanına dair olarak, yemin dışında, tanıklığa ilişkin CMK hükümlerinin uygulanacağı ifade edilmektedir (m.236). Fakat suça konu olayın tarafı olmaları sebebiyle bu kişilerin açıklamalarının temkinli şekilde değerlendirilmesi gerekir. Çünkü zarar görenin açıklamaları objektif şekilde gerçeği yansıtmayabilir[188].

Beyan delilleri haricinde belge delillerinin kaynağını eşya yani nesneler oluşturmaktadır. Belge, somut bir olaya ilişkin bir bilginin kâğıt veya kayıt özelliğine sahip bir eşyanın üzerine aktarılmış halidir[189]. Olayın ve belge delilinin kaynağına ilişkin olarak, bunların delil olabilmesi için elde edilmeleri gerekir. Belirti (emare) delillerinin kaynağını da hem kişiler hem de nesneler oluşturabilmektedir. Belge ve belirtiler elde edilirken yalnızca basit suç şüphesi var denilerek usul kurallarına uyulmadan, doğrudan incelenmez. Zira yalnızca muhakemenin yürütülmesi sırasında keyfi bir şekilde şüpheli kişilerin mülkiyetinde bulunan eşyaya erişmekle, kişilerin AİHS m.8 ve Anayasa m.20'de yer alan en temel hak ve özgürlüklerinden biri olan özel hayatın gizliliği hakkı ihlal edilmiş olur. Bu sebeple bu delillere erişimin sağlanırken yapılacak uygulamalara yönelik önlemler de yasalarda düzenlenmektedir.

---

[186]Centel ve Zafer, s. 201.

[187] Süheyl Donay, Ceza Yargılama Hukuku, İstanbul: Beta Yayınevi, 2012, s. 67; Metin Feyzioğlu, Ceza Muhakemesi Hukukunda Tanıklık, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1996, s. 28.

[188] Öztürk, s.324; Şüpheli ve sanık beyanı için ifade alma ve sorgu (CMK m.145), şüpheli ve sanık haricindekilerin (tanık mağdur gibi) beyanı için bilgi alma (Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği m.4- Resmi Gazete, Tarih: 01.06.2005, Sayı: 25832), yer gösterme (CMK m.85), teşhis (PVSK Ek m.6/9) ve doğrudan soru yöneltme (CMK m.201) gibi usuller vasıtasıyla beyan delilleri alınabilir. bkz Mahmut Koca, Ceza Muhakemesi Hukukunda Deliller, Ceza Hukuku Dergisi (CHD), Sayı. 2, Aralık 2006, s. 216

[189] Şahin ve Göktürk, s. 44.

Günümüzde sıkça kullanılan elektronik cihazlar, özellikle iletişim ve bilişim cihazlarının, kişilerin kullandığı suç vasıtaları arasında önemli bir yere sahiptir. Bir kişinin işlediği suçun sonrasında delil özelliğinde bir iz ve emare bırakmamaya çalışsa da bu kendi elinde olmadığı gibi, bilişim suçlarında da deliller, işlenen suç akabinde farklı şekillerde dijital delil olarak elde edilebilmektedir[190].

Ceza muhakemesinde belge ve belirti delillerinin elde edilmesinde kullanılan önlemler ise; arama ve elkoyma (CMK m.116 ve 127), bilirkişi incelemesi (CMK m.63), olay yeri incelemesi, fiziki kimliğin belirlenmesi (CMK m.81), keşif (CMK m.83), bilgi isteme (CMK m.332) şeklinde sayılabilir.

Bu konuda uygulanacak özel muhakeme önlemlerine ise ilgili madde içinde belirtilen suçların işlendiğine dair somut delillere dayalı kuvvetli şüphe nedenlerinin bulunması ve farklı şekilde delil elde edilmesi olanağının olmaması halinde, diğer bir deyişle, bu delile bir son çare olma (*ultima ratio*) ve zorunluluk hallerinde gidilebilecektir. Bu tedbirler bilgisayarlarda arama, kopyalama ve elkoyma (CMK m.134), iletişimin tespiti, dinlenmesi ve kayda alınması (CMK m.135), gizli soruşturmacı atanması (CMK m.139) ve teknik aletlerle izleme (CMK m.140) şeklinde gösterilebilir. Tesadüfi olarak ele geçirilen deliller (CMK 138) ise bu ikili ayrım haricinde kalan kendine özgü bir kurumdur.

2.2.3.1.2. Dijital Delillerin Elde Edilmesi

Dijital delilin elde edilmesinden anlaşılması gereken yöntemler; yukarıda sayılan özel muhakeme tedbirleri ile bunların kullanımı esnasında meydana çıkan, yasanın kullanılmasına izin verdiği ve tesadüfi olarak ele geçirilen deliller anlaşılmalıdır. Fakat gizli soruşturmacı atanması bu usullerin haricinde tutulmaktadır. Bunun sebebi, gizli soruşturmacı dijital delil ele geçirebileceği usulleri, hâkim kararına ihtiyaç duyulan önlemleri re'sen tatbik edemeyecek olmasıdır. Gizli soruşturmacı CMK m.134 kapsamında bilgisayarlarda bilgisayarlardaki delillerin elde edilmesi, CMK m.135'e göre iletişimin tespitine ilişkin tedbirleri re'sen tatbik edemez[191].

---

[190] Hüseyin Çakır ve Ercan Sert, "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler, Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010), Oğuzhan Ömer Demir ve Murat Sever (dr.), Ankara, 2011, s. 145-146.

[191] Kunter/Yenisey/Nuhoğlu, a.g.e. , s. 1546.

Öte yandan, ceza muhakemesi işlemlerinde dijital teknoloji kullanımı ve dijital delil ele geçirilmesi arasında bir fark vadır. Örnek olarak ifade alınırken ve el koyma işlemi yapılırken bilgisayarda tutanak hazırlanması, bu tutanağı dijital delil haline getirmektedir. Ancak bu tutanak saklanırken dijital teknoloji kullanılmaktadır.

Dijital delillerin elektronik aygıt içinde olmaları, delil elde etme safhasında onları geleneksel delillere göre daha özel duruma getirmektedir. Ayrıca somut varlığı olan bu aygıtlar dijital delil barındırdıklarından, dijital delil incelemesinde klasik usullerden farklı yöntemler kullanılmaktadır. Fakat dijital delillerin kolayca değiştirilebilmesi, bozulabilmesi ve yok edilebilmesi göz önüne alındığında geleneksel yöntemlerle araştırma yapacak kişilerin de dijital delillere dair bilgisiolankişiler olması gerekir[192].

Dijital delillerin incelemesi ve çözümlemesi yapılmış hali hâkim tarafından anlaşılabilse de, bu delillerin sağlamlığı ve güvenilirliğine ilişkin bölümünün teknik uzmanlığa ihtiyaç duyan noktalarının uzman kişiler tarafından belirlenmesi gerekecektir. Bu tespitleri gerçekleştirerek hâkime sunacak kurum, bilirkişiliktir. CMK'ya göre bilirkişi; çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hallerde oy ve görüşü alınacak kişidir[193].

Dijital delillerin incelenmesinde tek değişiklik, bilirkişilerin adli bilişim uzmanlarından seçilmesi gerekecektir. Dijital delili toplayacak kolluk kuvveti ya da yargı organınca belirlenen bilirkişi, adli bilişime dair sertifika sahibi olacak şekilde bilgi ve tecrübe seviyesine sahip olmalıdır[194]. Adli bilişim uzmanlarının yardımı ile dijital delillerin kendilerine mahsus nitelikleri sebebiyle, delil elde etme safhasında geleneksel delillere oranla daha sistematik ve modern usullerin uygulanması da irdelenecektir.

---

[192]Kaynakçıoğlu, s.51.

[193]Centel ve Zafer, s. 245; Bilirkişinin oy ve görüşünün alınmasına hâkim ya da mahkeme tarafından kendiliğinden veya savcı, katılan, vekil, şüpheli veya sanık, müdafii veya yasal temsilcinin talebi üzerine karar verilebilir (CMK m.63). Soruşturma safhasında bilirkişi, savcı tarafından da görevlendirilebilir (CMK m.63/3). Bilirkişi olarak atanabilecekler, kanunların belirli konularda görevlendirdiği resmi bilirkişiler (CMK m.64/3) dışında il adli yargı adalet komisyonları tarafından her yıl düzenlenen bir listede yer alan gerçek veya tüzel kişilerdir (CMK m.64). Fakat bu bilirkişiler haricinde de bilirkişi seçmek olanaklıdır (CMK m.64/2).CMK'nın lafzında da görüldüğü gibi bilirkişiye başvurma takdiridir.

[194] Değirmenci, Dijital Delil, s. 121; Keser Berber, a.g.e. , s. 46.

2.2.3.1.2.1. Adli Bilişim

Adli bilişim (veya bilgisayar kriminalistiği); hukuka uygun biçimde delillerin ele geçirilmesi için bilgisayar inceleme ve değerlendirme usullerine başvurularak yapılan uygulamaları anlamına gelmektedir[195]. Doktrinde adli bilişim kavramına ilişkin yapılan bir başka tanım iseşu şekildedir: "*Soruşturma ve/veya yargılamada, sürecin tarafların iddia ve/veya savunmalarını destekleyecek veya çürütecek gerçeklerin ortaya çıkartılması amacıyla bilişim aygıtlarının kayıtlarının incelenmesidir*"[196].

Henkoğlu ise adli bilişimi "*Bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığının tespiti amacıyla yapılan çalışmaların tümüdür*" şeklinde tanımlamaktadır[197]. Son olarak adli bilişim, olası hukuki delillerin ele geçirilmesi için bilgisayar inceleme ve değerlendirme yöntemlerine başvurularak yapılan bir uygulama biçiminde ifade edilmiştir[198].

Bu tanımlar incelendiğinde adli bilişimin, hukuki anlamda geçerli delil elde etmek için bilişimle ilgili sorunlar hususunda yardım alınacak uygulamaların tümü olduğu ifade edilebilir. Bu kapsamda adli bilişimin kaynakları da çok farklı ve çeşitlidir. İnternet kullanımları, bilişim suçları, fikri haklar, şirket sırlarına yönelik ihlaller, internet aracılığıyla hakaret suçları, sistem suiistimalleri gibi haller adli bilişimde kullanabilecek kaynaklardır[199]. Adli bilişim incelemesinde toplanan deliller salt ceza muhakemesi hukukunda kullanılmaz, özel hukuktaki uyuşmazlıklarda da kullanılabilmektedir[200].

2.2.3.1.2.2. Adli Bilişimin Aşamaları

Elektronik aygıtlar içinde bulunan dijital delillerin, ilk bakışta var olup olmadığı belirlenememektedir. Bu nedenle dijital delil elde etmede ilk önemli sorun, içinde delil barındırdığı zannedilen aygıtların suçun kanıtlanmasında ispat aracı olarak kullanılıp

---

[195] Dülger, Bilişim Suçları. , s. 738.

[196] Dülger, Bilişim Suçları, s. 739.

[197] Henkoğlu, a.g.e. , s. 1.

[198] Keser Berber, a.g.e. , s. 39.

[199] Keser Berber, s. 40.

[200] Keser Berber, s. 76-77.

kullanılmayacakları konusundaki belirsizliktir. Bu yüzden farklı suç tiplerine bakılarak farklı adli bilişim uygulamaları kullanılmakta ve aygıt incelemeleri de suç türüne göre gerçekleştirilmektedir[201]. Buna karşın, genel olarak bir adli bilişim aşamalarının kullanıldığı ve bilişim tekniklerinin de bu aşamalarda değişkenlik gösterdiği ifade edilebilir. Adli bilişimin aşamalarının neler olduğu konusunda doktrinde tartışmalar olsa da[202], adli bilişimin dört aşamadan oluştuğu kabul edilmektedir. Bu aşamalar; toplama, inceleme, analiz ve raporlamadır.

2.2.3.1.2.2.1. Toplama

Adli bilişim aşamalarının ilki, toplama, yani dijital delillerin ele geçirilmesidir. Bu aşamada; dijital delillerin aranması, belirlenmesi, toplanması ve listelenmesinin oluşturulması temin edilmelidir. Bu aşama, olay yeri veya arama yapılan yerde gereken tedbirler alınmadığında kaybolabilecek bilgilerin saklanmasını da kapsayabilir[203].

Toplama safhasının başarılı olması için olay yeri veya arama yapılan yer iyi bir şekilde korunmalıdır ve bunu adli kolluk sağlar. Bu sebeple adli kolluk, adli bilişim aşamaları ve

---

[201] Albert J. Marcella – Doug Menendez, Cyber Forensics: A Field Manual for Collecting,Examining,and Preserving Evidence of Computer Crimes, Auerbach Publications, 2007, s..51; Debra Littlejohn Shinder- Ed Tittel, Scene of the Cybercrime: Computer Forensics Handbook, Syngress, 2007, s.28.Michael A. Caloyannides, Privacy Protection and Computer Forensics(Artech House Computer Security Series) [2 ed.], Artech House Publishers, 2004, s.23; John R. Vacca, Computer Forensics: Computer Crime Scene Investigation *[1st ed.]*, Charles River Media, 2002, s.44; Jasmin Cosıc- Miroslav Baca, (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO. 2010, ss: 1226-1230, s.1227; Nicole Beebe. Digital Forensic Research: The Good, The Bad And The Unaddressed. IFIP Int. Conf. Digital Forensics, 2009, ss.17-36, s:30; Alastair Irons , Peter Stephens, Ian Ferguson. Digital Investigation As A Distinct Discipline: A Pedagogic Perspective. Digital Investigation, 6(1-2), ss.82-90. 2009, s84; Rick Ayers, Sam Brothers, Wayne Jansen. Guidelines on Mobile Device Forensics, NIST Special Publication Revision 1, (800-101), 2014, ss.1-85, s27; Adam Gordon (Ed.). Official (ISC)2 Guide to the CISSP CBK. 4. Baskı, CRC Press, 2015, s,798; Moniphia Orlease Hewling, Digital Forensics: An Integrated Approach For The Investigation Of Cyber/Computer Related Crimes, Bedfordshire University, Phd Thesis, 2013, s.106; Henkoğlu, s. 9-12;

[202] Keser Berber, s. 45 Say, s. 531; Karagülmez, s. 454 Değirmenci, Dijital Delil, s. 165 vd.

[203] Keser Berber, s. 45; Dülger, Bilişim Suçları, s. 746.

dijital delillerin toplanmasına dair bilgilendirilmelidir. Olay yeri iyi şekilde korunursa olay yeri incelemesi sağlıklı yapılır ve dijital delillerin kaybolması önlenir. Bu koşullar sağlandıktan sonra adli bilişim uzmanları toplama aşamasını başlatılabilirler. Toplama aşaması dijital delillerin aranmasıyla başlasa da, aramadan önce olay yerinin fotoğraflanması, toplamaya dair gereken teknik malzemelerin hazırlanması gibi işlemler yapılmalıdır[204].

Arama işlemi başladığında aygıtların durumlarına ya da özelliklerine bakılarak yapılması ve yapılmaması gereken eylemler olacaktır. Genelde adli bilişim uzmanları elektronik aygıt açık halde iken çalışmak durumundadırlar. Diğer durumunda ise elektronik aygıt kapalı haldedir ve çalışmamaktadır. Her iki durumda da yapılacak iş, dijital delillerin sonradan analiz edilmek için muhafaza altına almak olduğu görülmektedir[205]. Bu yüzden iki durumda da adli bilişim uzmanının yapacağı işlem, imaj alma şeklinde tanımlanan bir tür kopyalama işlemidir[206]. Fakat olay yeri incelemesi esnasında imaj alma işlemin yapılması zaman almakta ve yanlış bir işlem veri kaybına yol açabilmektedir. Bu yüzden imaj alma işleminin, inceleme anında elde edilmesi gereken ve erişilebilir verilerle sınırlı tutulmalı, inceleme bir sonraki aşama olan inceleme aşamasına bırakılmalıdır[207].

Aramada elde edilen elektronik aygıtlar ve dijital delillerin tespiti yapılmış olur. Belirlenen eşyaya etiket konulması ve delil vasfıyla kaydının yapılması gerekir. Tespiti yapılmış dijital deliller ve aygıtların toplanması çalışması daha sonra başlar. Toplanan eşya inceleme amacıyla laboratuvara götürülür. Bunlar yapılırken elektronik aygıtların dış etkenlere olan hassasiyetine dikkat edilmelidir, çünkü bu aygıtlar kolayca zarar görebilir. Toplama aşamasında yapılan her işlem mutlak surette listelenmelidir. Bu aşamadaki bütün işlemler sırasıyla yazılmalı ve buna ilişkinbelgelerde şüpheli ya da müdafinin imzası olmalıdır. Bu şekilde, yapılan işlemlerin hukuka uygun ve denetime açık olması sağlanır[208].

---

[204] Dülger, Bilişim Suçları, s. 747.

[205]Karagülmez, s. 456.

[206] Değirmenci, s. 373-374.

[207] Dülger, Bilişim Suçları, s. 750.

[208] Dülger, Bilişim Suçları, s. 748, 750.

İnternet bağlantısı gibi geleneksel olay yerininifiziki şekilde bulunmadığı hallerde toplama safhasının hizmet temin eden belirli kurumlardan yapıldığı haller meydana gelebilmektedir. Bu halde görevli adli bilişim uzmanının toplama işlemi, ilgili kurumdabulunan kayıtlar üzerinden yapılmalıdır. Fakat dijital verilerin sağlıklı ve güvenilir bir şekilde toplanması ve denetimi için ilgili kurumların da adli bilişim uzmanı çalıştırmaları gerektiği akla gelebilir. Ancak bu yönde bir yasal yükümlülük bulunmadığı da hatırlatılmalıdır. Adli bilişim uzmanı istihdam edildiğinde toplama safhası daha sağlıklı yapılabilecek olsa da hizmet sağlayan kurum içinde bir adli bilişim desteği almadan yapılan işlemlerin hatalı olması ve düzgün kayıt elde edilememesi olanağı da vardır.

2.2.3.1.2.2.2. İnceleme

Toplama aşamasından sonraki aşama olan inceleme aşamasında; dijital delillerin somut hale getirilmesi ile bu delillerin orijinal hali ve soruşturmadaki önemi açıklanır. Bu aşama, adli bilişim sürecinde en önemli aşamalardan biridir. Bu safhadaki ön hazırlık işlemi, ele geçirilen delillerin imajının alınmasıdır. Bu şekilde inceleme, orijinalinin aynısı olan imaj üstünde gerçekleştirilecek, orijinal delil üstünde bir tahrifat yapılmamış olacak ve delil bütünlüğü korunmuş olacaktır[209]. Bu şekilde inceleme esnasında oluşabilecek sorunlarda zarar görecek olan, delilin imajı olur. Bu halde delil zarar görmeyeceğinden en kötü durumda dahi tekrar imaj alma işleminin gerçekleştirilmesi olanaklı olacaktır.

Toplama işleminde diğer bir önemli konu ise dijital delillerin "*hash*" değerinin belirlenmesi konusudur. Hash değeri, dijital verinin bütünlük ve bozulmamışlık denetiminde başvurulan bir değerdir[210]. Yargılama aşamasında da yapılacak denetimin geçerliliği için kopyalama esnasında hash değerinin de yazılması gerekmektedir. İncelemeden önce alınan hash değerinin, daha sonraki safhalarda elde edilen hash değeri ile farklılığının olması durumunda veri üstünde değişiklik gerçekleştirildiği kanıtlanabilmektedir[211].

---

[209] Dülger, Bilişim Suçları, s. 752.

[210] Marcella –Menendez, s..53; Shinder- Tittel, s.30; Caloyannides, s.26; Vacca, s.46; Cosıc- Baca, s.1228; Beebe. s:31; Irons- Stephens- Ferguson. s.85; Ayers- Brothers- Jansen. s.29; Gordon s,799; Hewling, s.107; Henkoğlu, s. 56.

[211] Semih Dokurer, Adli Bilişim", Ses Görüntü ve Data İncelemeleri, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008, s. 244.

Bu aşamada dijital delilin zarar görmesi önlenmekte, delil bütünlüğü ve sağlamlığınında korunması hedeflenmektedir. İnceleme aşamasında delilin içeriği ve durumu listelenir. Bu listeleme delilin içinde ne olduğunu tarafların, bilmelerine imkanverir. Ayrıca inceleme aşamasında şifreleme yüzünden saklı kalmış ya da erişilememiş bilgilerin araştırılmasıdır[212].

2.2.3.1.2.2.3. Analiz

Analiz aşamasında, incelemede elde edilen neticelere hukuksal önemleri ve davadaki ispat değerleri bakımından yaklaşılmaktadır[213]. İnceleme aşaması, adli bilişim alanında teknik bir inceleme iken, analiz safhasında ise delillendirmenin hukuksal yönü de göz önüne alınarak bir inceleme yapılır. Bu aşamadaki inceleme, çoğunlukla elde edilen verilerin hukuki önemlerine göre sınıflandırma yapılmaktadır.

Analiz aşamasında, soruşturma konusu olmayan olayla ilişkisi olmayan veriler bir tarafa bırakılacaktır. Bu işlem gerçekleştirilirken dijital delilin ele geçirildiği aygıtların farklılığına göre kullanılacak birçok yazılım vardır[214]. Analiz aşamasında varılan neticeler son safha olan raporlama aşamasında kullanılacaktır.

2.2.3.1.2.2.4. Raporlama

Dosyada bilirkişi olan adli bilişim uzmanı, incelemesi bittiğinde, gerçekleştirdiği işlemleri ve ulaştığı neticeleri gösteren bir raporu, talep edilen incelemeleri de yerine getirdiğini belirtip, imzalayarak ilgili adli makama verir (CMK m.67). Bu aşamada belirti delilleri bilirkişi raporuna gelerek belge haline getirilmektedir[215]. Dosyada birden çok bilirkişi görevlendirilmişse, bilirkişilerin arasında ortak sonuçlar ve hatta farklı görüşler gerekçesiyle beraber raporda ifade edilir (CMKm.67/2). Fakat bilirkişi raporunun hâkimde yeterli vicdani kanaat oluşturmaması halinde yeni bir bilirkişi atayarak inceleme gerçekleştirilebilir. Bu bilirkişi incelemesine de itiraz edilebilir.

Adli bilişimin bütün aşamalarında yapılan işlemler, belgelenip kayıt altına alınmalı ve raporlama aşamasında bütün bu işlemler mahkemeye sunulmalıdır. Raporun içinde yapılan

---

[212] Keser Berber, s. 45.

[213] Keser Berber, a.g.e. , s. 45.

[214] Dülger, Bilişim Suçları, s. 756 vd; Karagülmez, a.g.e. , s. 464 vd

[215]Centel/Zafer, a.g.e. , s. 246.

işlemlerin içerikleri, işlemlerin başladığı ve son bulduğu tarih gibi unsurlar yer almalıdır. Bu unsurlardaki belirsizlikler, delil koruma zincirine menfi olarak etki eder[216]. Delil koruma zinciri, delilin ele geçirilme zamanından başlayarak mahkemeye iletilmesine kadarki süreçte, delil sağlamlığı ve bütünlüğünün bozulmadığının kanıtlayan çok önemli bir araçtır[217].

Raporlama aşamasında; toplama ve inceleme değerlendirmelerini de kapsayan ve analiz safhasının dökümantasyonunun yapıldığı ve özetlendiği, bu raporla incelemeyi gerçekleştiren adli bilişim uzmanlarının suça konu olaya yalnızca şekli olarak ve nitelikleri bakımından tanıklığı da temin edilmektedir[218]. Ayrıca, delil koruma zincir sağlanarak delillerin bütünlüğü ve sağlamlığı daha iyi şekilde korunmuş olur.

2.2.3.2. Dijital Delillerin İspat Gücü

Dijital deliller, ceza hukukundaki delillerin sınıflandırılması açısından belirti delilleri içinde sınıflandırıldığı söylenebilir. Bu nedenle dijital delillerin, belirti delillerinin sahip olduğu ispat gücüne sahip oldukları ifade edilebilir. Ancak belirti delilleri, beyan ya da belge delillerine oranla zayıf bir ispat kuvvetine sahiptir[219]. Bu nedenle bir belirti (emare) delili, mahkûmiyet hükmüne ulaşılması için yeterli olmayacaktır. Örneğin, olay yerinde şüpheliye ait parmak izinin bulunması, tek başına şüphelinin suçu işlediğini göstermez; yalnızca şüphelinin olayın meydana geldiği mahalde bulunduğunu kanıtlar. Bununla birlikte birden fazla ve birbirini tamamlayan belirtinin bir araya gelmesi durumunda mahkûmiyet kararı verilebilmesi olanaklıdır[220].

Hem Anayasa Mahkemesi[221]hem de Yargıtay tarafından verilen kararlarda[222] belirtilerin, delil anlamında tek başlarına suçu kanıtlamaya yeterli olamayacakları ve başka delillerle

---

[216] https://consultations.pefc.org/consult.ti/PEFCsChainOfCustody/viewCompoundDoc?docid=7826164&partId=7826324&sessionid=&voteid (Et. 09/02/2019)

[217] Peter Sommer, Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers, 3. Edition, Information Assurance AdvisoryCouncil, 2012, s. 30, https://cryptome.org/2014/03/digital-investigations.pdf, (Erişim tarihi: 07.03.2022).

[218] Keser Berber, a.g.e. , s. 45

[219]Centel/Zafer, a.g.e. , s. 245.

[220]Centel/Zafer, a.g.e. , s. 246; Kunter/Yenisey/Nuhoğlu (2013), s. 1375.

[221] AYM 19.08.1971-41/67, Resmi Gazete, Tarih: 15.01.1972, Sayı: 14073: "Başkaca inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının ve gizli ajan raporlarının, bir yurttaşa yapılan "Türkiye

desteklenmeleri gerektiği ifade edilmiştir. Yani belirti delili kapsamındaki tek bir delilin bulunması, suçu kanıtlamaya yeterli olmayacak ve mahkûmiyet hükmü verilemeyecektir. Fakat bu türde birbirini destekleyen farklı delillerin de bulunması durumunda mahkûmiyet kararı verilebilmektedir. Kaldı ki, bir nesnenin delil olması ile delil olan nesnenin belli bir olguyu kanıtlama gücü farklı şeylerdir[223].

Bir delil türü olarak dijital deliller, ceza muhakemesinde birçok sorunu beraberinde getirmektedir. İlk olarak dağınık ve farklı bir yapıya sahip olan dijital delili ele geçirmek zor olabilmektedir. Örnek olarak bir sabit disk, bilgi parçaları birbirine karışmış, diskin üstüne başka veriler kaydedilmiş ve zaman içinde katman hale gelmiş dağınık bir veri alaşımına sahip olabilmektedir. Bu alaşımında yalnızca küçük bir bölümünün soruşturma veya kovuşturmayla ilgilisi bulunabilmektedir. Bu açıdan, bu verilerden delile anlamında kullanışlı olanlarını çıkartılmalı, uygun ve değerlendirilebilir bir şekle sokulmalıdır[224].

Dijital delillerin kolayca manipüle edilebilecek yapıda olması ceza muhakemesinde başka sorunlara da yol açmaktadır. Olay mahallinde ele geçirilen dijital verilerin, mahkemeye verilene kadar korunmasının temin edilmesi, hâkimin vicdani kanaatinin doğru ve kesin delillere istinaden meydana getirilmesi bakımından önemlidir[225]. Dijital delil, suçlular tarafından ya da elde edilmesi esnasında yanlışlıkla, bozulmaya dair belirgin herhangi bir iz bırakılmaksızın değiştirilebilir. Örneğin malware gibi kötü niyetli yazılımlar kullanılarak bir bilişim aygıtı suçun işlenirken araç şeklinde kullanılabilir. Bu gibi hallerde suçun asıl zanlı ya da zanlılarını yakalamak sadece bilişim sistemindeki veriyle zanlı ya da zanlılar arasındaki ilişkinin kurulmasıyla olanaklı olacaktır[226].

Cumhuriyeti Anayasasını teğyir ve tebdile ve bu yasa ile kurulmuş Türkiye Büyük Millet Meclisini İskata veya görevini yapmaktan men'e cebren teşebbüs gayesiyle gizlice ittifak kurmak" gibi çok ağır bir isnada yasama dokunulmazlığının kaldırılması yönünden ciddilik kazandırabilmesi bir hukuk Devletinde düşünülemez."

[222] Ali Kemal Yıldız, Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu, Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, Aralık 2006, ss. 259-260.

[223]Centel/Zafer, s. 245.

[224]Casey, Digital Evidence and Computer Crime, s. 25.

[225] Değirmenci, Dijital Delil, s. 188-189.

[226] Değirmenci, Dijital Delil, s. 176.

Dijital delillerin ispat güçlerine ilişkin bir başka önemli konu, bu delillerin ceza yargılamasında geçerli kabul edilebilmesi hukuka uygun olmaları yanında, adli bilişim incelemesi yapılırken ve yapıldıktan sonra sağlam ve güvenilir oldukları da belirlenmelidir. Bu denetim, vicdani ispat sisteminin olduğu Türk ceza hukuku sisteminde hâkim tarafından gerçekleştirilmelidir. Bu aşamalardan geçen belirtinin delil olup olmayacağı da açığa çıkmış olur. Adli bilişim bilirkişilerinin raporu, hâkime ışık tutsa da raporun içeriğinin de denetlenmesi gerekmektedir. Denetlenmesi gereken hususlar; dijital delillerin elde edilme aşamasında hukuka uygun davranılıp davranılmadığı, söz konusu delil toplanırken soruşturma aşamasındaki hash değeri, zaman damgası ve delil koruma zincirine uyulup uyulmadığı ve örneğin hash değerinin kovuşturma sırasında alınan bilirkişi raporu iel uyumlu olup olmadığı, verilerde tahrifat olup olmadığı gibi kurallardır.

Bu kapsamda Türkiye'de dijital delillerin incelenmesine ilişkin çok detaylı kurallar bulunmasa da[227], ABD[228], İngiltere[229] gibi bazı ülkelerde adli bilişim uygulamalarına hukuki düzenlemeler ve kolluk ve adli makamlara yol gösterici rehberler yayınlandığı görülmektedir. Türkiye'de adli bilişim incelemeleri; Adli Tıp Kurumu'nuu yapısı içinde yer alan Adli Bilişim İhtisas Dairesi Başkanlığı[230] ve il adli yargı adalet komisyonlarınca her yıl hazırlanan bilirkişi listesine giren kişiler tarafından yapılmaktadır.

2.2.3.3. Dijital Delillerin Geçerliliğinin Denetimi

Elde edilen delillerin hukuki anlamda geçerli kabul edilebilmesi için bazı usullerin yerine getirilmesi ve standartlara uygun olması önem taşımaktadır. Bilhassa dijital deliller yapıları sebebiyle başka suçlarda el konulan fiziki delillere oranla daha hassas ve kolay bozulabilir

---

[227] CMK m.134 ve Adli ve Önleme Araması Yönetmeliği m.17'de bu konuda bazı hükümler olsa da yeterli de

[228] Paul Marcus/VickyWaye, "Australiaandthe United States: TwoCommonCriminalJusticeSystemsUncommonly at Odds", College of William & Mary Law School Faculty Publications, 2004, s. 32, http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1245&context=facpubs. (Erişim tarihi: 08.03.2022); Department of Justice of USA, SearchingandSeizingComputersandObtaining Electronic Evidence in CriminalInvestigations, https://www.justice.gov/file/442111/download, (Erişim tarihi: 08.03.2022).

[229] ACPO GoodPractice Guide forComputerBasedEvidence, https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf, Erişim tarihi: 08.03.2022; Murat Volkan Dülger, Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması, TAAD, Yıl:8, Sayı:31, Temmuz 2017, s.141 vd (Karşılaştırmalı Hukuk).

[230] https://www.atk.gov.tr/adli-tip-ihtisas-daireleri.html, Erişim tarihi: 08.03.2022.

niteliktedirler. Dijital delillerin ele geçirilmesi esnasında olay yerinde gerçekleştirilecek en ufak hata, veri ve dolayısıyla delillerin zarara uğramasına ve kaybolmasına yol açabilir[231]. Bu nedenle dijital delilin toplanması aşamasında olay yerini inceleyen ekipten, incelemenin yapıldığı yere kadar tüm sonuçların mahkemeye sunulması aşamaları önem taşımaktadır[232].

2.2.3.4. Hukuki Geçerliliğinin Denetimi

Dijital delilin hukuki geçerliliğinin denetlenmesinde, ilk olarak delillerde olması gerekli temel özellikler; olan gerçekçi, akılcı, erişebilir, olayı temsil eden, müştereklik ve hukuka uygunluk özellikleri ile yukarıda sayılan dijital delillere özgü özelliklerdir. Bu kapsamda delilin müştereklik özelliği uyarınca, soruşturma veya kovuşturmada ileri sürülen dijital delilin, taraflarca bilinmesi ve tartışılabilir olması gerekir. Dijital delil, müştereklik ilkesi açısından başka delillere oranla daha üstün bir pozisyona sahiptir. Çünkü soruşturma safhasında bile dijital delilller barındıran ve imajı alınan elektronik verilerin bir örneği veya elektronik aygıtın kendisi şüpheliye verilir. Dijital delili çoğaltılabilme niteliğine sahip olduğundan bu durum bu delilller bakımından bir avantaj oluşturmaktadır[233]. Öte yandan, Türkiye uygulamasında kriminal laboratuvarlar haricinde CMK kapsamında izin verilen uzman mütalaası adı verilen ve yargılama makamlarına arz edilen raporların çoğunlukla göz önüne alınmaması müştereklik ilkesine zarar vermektedir[234].

Dijital delil, aynı zamanda akılcı, gerçekçi ve olayı temsil ediyor olmalıdır. Delilin akılcı olması, bilimsel bakımdan da kabul edilebilir olmasını gerektirir[235]. Aynı zamanda dijital delili toplayacak görevli, kolluk kuvveti ya da adli makamca atanan bilirkişi, adli bilişim konusunda sertifika sahibi de olacak şekilde bilgi ve deneyim düzeyine sahip olmalıdır[236].

---

[231] Yusuf Uzunay , "Dijital Delil Araştırma Süreci", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, s. 46-47.

[232] Çakır ve Sert, s. 148.

[233] Hüseyin Akarslan, Bilişim Suçları, Ankara: Seçkin Yayıncılık, 2012, s. 132-133.

[234] Halid Özkan, "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği", Yener Ünver (Ed.), Ceza Muhakemesi Hukukunda Delil ve İspat içinde (265-287), Ankara: Seçkin Yayıncılık, 2014, s. 268.

[235] Özkan, s. 269.

[236] Değirmenci, Dijital Delil, s. 121.

"*Hukuka uygun elde edilmiş olması*", dijital delillerin ceza yargılaması açısından en önemli özelliğidir[237]. Hukuk kurallarına ve bu kurallarda belirtilen usullere uyulmaksızın dijital delil elde edilmesi durumunda bu delilin hukuka aykırılığı gündeme gelecek ve bu delil hükme esas alınmayacaktır. Ayrıca, hukuka aykırı ve hükme esas alınamayacak deliller, özel hayatın gizliliğini ihlal veya özel kişisel verilerin açıklanması gibi bazı mağduriyet ve temel hak ihlallerine neden olacaktır[238]. Örneğin Türk hukukunda 31.07.2018 tarihli ve 7145 sayılı Kanunla yapılan değişiklikten önce CMK m.134 kapsamında bilgisayarlara yürütülen soruşturma kapsamında el konulabilmesi için mahkeme kararı gerekmekteydi ve Cumhuriyet savcısının kararı veya daha sonra mahkemenin bu aramayı onaylaması ile bu deliller hukuka uygun hale gelmiyordu. Bu tarihten yani 31.7.2018 tarihinden evvel, önceden alınmış bir mahkeme kararı bulunmaksızın CMK m.134 kapsamındaki elektronik aygıtlara ve dolayısıyla dijital delillere el konulması, hukuka aykırı bir el koyma olacak ve bu deliler ceza muhakemesinde kullanılamayacaktır[239].

2.2.3.5. Teknolojik Geçerliliğinin Denetimi

Dijital delil açısından karşılaşılan en önemli problemlerden birisi, ele geçirilmesi ve yargılama bitene kadar korunması aşamasında bu *delillerin bütünlüğünün* korunmasıdır. Bu sorun dijital delillerle fiziki deliller arasındaki en esaslı farklardan biridir. Cumhuriyet savcısı, elektronik aygıttan ele geçirilen verilerinin ilk ele geçirildiği haliyle olduğunu, elektronik aygıtın tümüyle kolluk kuvvetleri veya kısmen ya da tamamen tanık veya sanıkça ele geçirildiği hususlarına bakılmaksızın, mahkemede doğru ve tam olarak meydana koymak zorundadır[240]. Çünkü dijital delilin niteliği gereği kasti olarak veya yanlışlıkla silinmesi, değiştirilmesi veya bozulması kolaydır ve olanaklıdır. Dijital delilin bütünlüğünün sağlanması, genelde kriptografi (şifreleme) yöntemleri kullanılarak yapılmaktadır.

Dijital delilin teknolojik denetimi, *dijital delilin doğrulanmasını* gerektirmektedir. Örneğin dava açıldığında hâkim tarafından dijital delille ilgili dikkate alınması gereken temel ilke,

---

[237] Akarslan, s.133.

[238] Değirmenci, Dijital Delil, s. 389.

[239] Yargıtay Ceza Genel Kurulu 2016/544 E. , 2020/127 K., T.25.2.2020,

[240] Başlar, s.99.

elektronik delilin niteliği gereği yeterince kişiselleştirilememesidir[241]. Dijital delil elde edildikten sonra ceza muhakemesi aşamasında isnat edilen suçla ya da şüpheliyle ilgili olup olmadığının kanıtlanması gerekmektedir. Ayrıca, dijital delilin gerçek delil özelliğine sahip olabilmesi için ilk elde edildiği andan başlayarak hiçbir şekilde biçimde değişime uğramadığının, hangi görevli ve uzmanlarca hangi yerde ve ne zaman elde edildiğinin teyit edilmesi gerekir[242]. Bununla birlikte, dijital delillerin inceleme ve analiz işlemlerinin yapıldığı laboratuvarın bu işlemleri yapmak için uygun standartlarda olup olmadığı, kullanılan ekipman ve usullerin yerinde olup olmadığı gibi birçok konunun da değerlendirilmesi gerekmektedir[243].

Yine tüm soruşturma işlemlerine ilişkin tutanak tutulması, bu tutanağın görevli, savcı (ya da sulh ceza hâkimi) ile hazır bulunan tutanak yazmanınca imza edilmesi (CMK m. 169/2) ve bilgisayar veya bilgisayar kütüklerine elkoyma işlemi esnasında bunlardaki tüm verilerin yedeklemesi gerektiği düzenlemiştir CMK m. 134/3. Bu açıdan, adli bilişim aşamalarında ele geçirilen dijital verilerin tutanağa geçirilerek imzalanması, *dijital delilin deyim yerindeyse inkâr edilememesi* bakımından çok önemlidir[244].

Bilişim sistemleri; girdi, süreç ve netice biçiminde işleyen sistemler olduğu dikkate alınmalı ve dijital delil açısından girdi, delillerin işleme tabi tutulması halinde işlemlerin doğruluğu ve çıktının önceki işlem aşamalarıyla uyumlu olup olmadığı denetlenmelidir[245] . Veriler ve bilgisayar sisteminde hata ve bozukluk olup olmadığı, bilişim sisteminin standart tipte olup olmadığı, bu sistemin çalışmasına güven duyulup duyulmayacağı gibi teknik

---

[241] Değirmenci, Dijital Delil, s. 121

[242] Yusuf Uzunay ve Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Delililer", AB'05 Akademik Bilişim Konferansı, Gaziantep, 31 Ocak - 4 Şubat 2005, https://9lib.net/article/teknolojik-ge%C3%A7erlili%C4%9Fin-denetlenmesi-elektronik-delilin-ge%C3%A7erlili%C4%9Finin-denetlenmesi.q7wx8xnd, Erişim tarihi: 08.02.2022.

[243] Yusuf Uzunay,ve Kemal Bıçakçı. "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu. İstanbul, 9-11 Haziran 2005, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. Pdf, Erişim tarihi: 08.02.2022.

[244] Başlar, s.101.

[245] Değirmenci, Dijital Delil, s. 139.

durumların da bilirkişilerce incelenip verinin kimliği belirlenebilir bir şahsa ait olup olmadığının tespiti gerekir[246].

Dijital delilin ele geçirilmesi aşamalarında bir bilirkişi tarafından yapılan inceleme ve bulgular farklı bir bilirkişi tarafından sonradan yeniden incelenebilir olmalıdır. Farklı bir uzman aynı usuller sonucunda aynı neticeye ulaşıyorsa delilden elde edilen neticelerin ve tatbik edilen usulün geçerliliği kanıtlanmış olur. Örneğin farklı kişiler tarafından uygulanan inceleme ve analiz yazılımları her defasında aynı sonucu vermelidir[247].

2.2.4. Kosova Hukukunda Dijital Delil Kavramı

Son yıllarda yaşanan teknik ve teknolojik gelişmeler, insanların günlük yaşamları üzerinde büyük bir etki yaratmıştır. Birçok teknik cihazın, özellikle de sayısallaştırımış bilgi ya da enformasyonun işlenmesini esa alan cihazların kullanılmaya başlanması, sosyal yaşamın çeşitli alanlarında muazzam kullanımlarına yol açmıştır. Yeni bilgi teknolojileri (BT) varlıkları ve programları, ulusal ve uluslararası taşımacılık, finans ve bankacılık sistemi, bilim, kültür, spor, üretim ve günlük yaşamı etkileyen diğer pek çok alanda yaşamın her alanında kullanım alanı bulmuştur.

Bu cihazların ve programların kullanımı hayatı daha kolay ve dinamik hale getirmekle birlikte, yeni teknolojinin kullanımına ilişkin bazı kurallar ve kısıtlamalar koymaya ihtiyacı da beraberinde gündeme gelmiştir çünkü BT cihazları elbette iyi niyetlere ek olarak, bazı yasadışı eylemleri gerçekleştirmek için sırasıyla kötü amaçlar için de kullanılabilirler.

Modern dünyada bilgisayarların ve uluslararası bilgi ağlarının kullanılması, iş ve insan yaşamındaki köklü değişiklikleri etkilemiştir. Artık bir kişinin daha önce sıkı çalışma gerektiren ve toplanması ve organize edilmesi için uzun bir süre gerektiren bilgi ve veriler elde etmesi daha kolay hale gelmiştir. Kişisel, kurumların bilgisayarları, eğitim, araştırma ve çalışma merkezleri büyük kolaylık ve fayda sağlamıştır. Bugün bilgisayar teknolojisi kullanımı olmadan birçok araştırma projesini düzenlemek, planlamak ve uygulamak neredeyse imkansızdır. Bilgisayarın uygulanması, bilimin gelişmesine ve insanlığın esenliğine büyük bir ivme kazandırdı. Bununla birlikte, günlük yaşamdaki geniş

[246] Kunter, Yenisey ve Nuhoğlu, s. 1104.

[247]Henkoğlu, s. 2, 7; Özkan, s. 268.

uygulaması, çağdaş toplumun gelişimi ve refahı lehine olmayan bazı zararlı unsurlara sahiptir.[248]

Bu nedenle, her bir devletin, kendi mevzuatı çerçevesinde, çeşitli BT açıklamalarının kullanımına, özellikle de belirli kişiler tarafından yasa dışı kazanç için kullanılabilenlere ilişkin bazı kilit hususları tanımlaması zorunludur. BT alanında gelişmelere yol açan küresel değişiklikler, her bir devletin en iyi yasal korumanın organizasyonunu göz önünde bulundurması gereken yüksek riskli diğer alanları ortaya çıkarmıştır. Çünkü BT cihaz ve programlarının kullanımıyla ceza gerektiren suçların yol açabileceği zararlar çok büyüktür.

Bilgi teknolojilerinin geliştirilmesinin hayatımıza, getirdiği yenilikler, bu teknolojik gelişmeler sadece iyi amaçlar için kullanılmadığı için çok tehlikeli bir suç sorununa maruz kalmıştır. Bu durum, devletleri tek tek değil, aynı zamanda çeşitli bölgesel ve dünya örgütlerini, BT'nin getirdiği yeniliklerin kullanımında güvenlik yaratmak için hızla harekete geçmeye itmiştir. Dünyanın her zamankinden daha fazla siber alanda yasal korumaya ihtiyacı bulunaktadır.

Yüksek sosyal riskli suç türlerinden biri olarak bilinen, teknolojinin suç unsurları tarafından kötüye kullanımı siber suç ‘(cybercrime) olarak bilinir. Burada bilgisayar dolandırıcılığı, bilgisayar sahteciliği, güvenlik sistemlerinin ihlali veya bilgisayar sisteminin bir ağa bağlı bir araç olarak dahil olduğu herhangi bir biçimde görünebilen, bir bilgisayar sistemindeki bir kişinin eylemidir. Bilgisayar suçları şu şekilde tanımlanır: Parasal kazanç, mağdurun imajına zarar verme veya modern teknolojiyi kullanarak doğrudan veya dolaylı olarak fiziksel veya zihinsel zarara yol açarak bireylere veya birey gruplarına karşı işlenen cezai suçlardır. Günlük uygulamada, siber suç olgusu karşısında iki tür davranış gözlenir.[249]

Özellikle bilgisayar devriminin getirdiği değişiklik, her bilgiyi ikili bir koda dönüştürerek, işleyerek ve yeni bilgiler üreterek her süreci otomasyonu olarak aynı zamanda suç davranışının daha da karmaşıklaşıklaştırarak bilgisayar sistemlerinin mevcut teknolojilere entegrasyonunu, bu teknolojidelerin kullanılması suretiyel kitlesel olarak zarar ortaya

[248]Dr. RagipHalili` Kriminoloji`, Dördüncü Baskı, Priştine 2016,s.211.

[249]Aldo Shkembi, `` Arnavut ve Avrupa Mevzuatının Uyumlaştırılması ", Sayfa 5, Yayın 1, Tiran 2015

çıkarma olasılığını da beraberinde getirmiştir. Bilgisayar, bilişim teknolojilerinin yoğun olarak kullanıldığı toplumlarda bir suç türleri de gündeme gelmiştir.[250]

2.2.4.1. Kosova Hukukunda Dijital Delillerin Elde Edilmesi

Siber suçları en geniş anlamıyla şu şekilde tanımlamak mümkündür. Buna göre siber suçlar, ekonomik değer kazanmak, mağdurun imajına zarar vermek veya modern teknolojiyi kullanarak veya başka bir şekilde doğrudan veya dolaylı olarak fiziksel veya zihinsel hasara neden olmak için bireylere veya birey gruplarına karşı işlenen cezai suç, amaçların sahtekarlık, güvenlik sistemlerinin ihlali, sömürü vb. yoluyla kazanılması olduğu bir komut sistemi aracılığıyla eylemlerin gerçekleştirilmesi olarak tanımlanır.[251]

Siber suçlar, çeşitli biçimlerde kendini gösterir; çoğunlukla sahtekârlık, korsanlık, program hırsızlığı, programlara izinsiz giriş, özel yazılıma izinsiz giriş ve özel samimi sırların tespiti, çeşitli diğer manipülasyonlar, siyasi ve endüstriyel casusluk ve kriminal faaliyetlerin diğer birçok şeklidir.[252]

Siber suçlara karşı başarılı bir şekilde korunmak için Kosova Cumhuriyeti, en azından şu anda bu tür suçları önlemek ve bunlarla mücadele etmek için yeterli kabul edilen bir mevzuatı uyarlamıştır.

Kosova Cumhuriyeti Ceza Kanunu'na göre KCK'nın 327. maddesi uyarınca bu nitelikteki sadece bir suç öngörülmektedir; “Bilgisayar Sistemlerine Erişim ". Bu maddedeki tanıma göre, 1. fıkrada devamındaki gibi kabul edilmektedir Her kim yetkisiz ve kendisine veya başka bir şahsa yasadışı kazanç elde etmek veya diğer bir şahsa zarar vermek maksadıyla bilgisayar verilerini değiştirir, yayımlar, siler, imha eder veya tahrip ederse veya başka şekilde diğer herhangi bir kişinin bilgisayarına girmiş olursa, para cezasına ve üç (3) yıla kadar hapis cezasına çarptırılır.[253]

Bu yasal hüküm, bilgisayar sistemlerine erişim durumunda yasadışı eylemlerin, bu suçu işlemenin ciddi bir biçimi olarak kabul edilen on bin (10000) avrodan daha yüksek miktarlarda maddi hasara veya faydaya neden olduğu durumu da öngörmektedir. Bu

---

[250]Dr. RagipHalili` Kriminoloji`, Sayfa 69, Dördüncü Baskı, Priştine 2008

[251]AldoShkembi, “Arnavut ve Avrupa Mevzuatının Uyumlaştırılması ", Yayın 1, Tiran 2015,s.8

[252]Dr. RagipHalili,` Kriminoloji`, Dördüncü Baskı, Priştine 2008, s.212.

[253]Kosova Cumhuriyeti Ceza Kanunu, madde 327, fıkra 1, Bilgisayar Sistemine Giriş

maddenin 1. paragrafından suç eylemi on bin (10.000) Euro'yu aşan maddi kazançla sonuçlanırsa veya zarar on bin (10.000) Euro'yu aşmış olursa, sanık para cezasına ve altı aydan beş yıla kadar hapis cezasına çarptırılır.[254]

Ceza Muhakemesi Kanunu m.134'de yer alan hükme benzer şekilde, "Bilgisayar Analizleri" başlıklı Kosova Ceza Muhakemesi Kanunu m.147'de[255] bilgisayarlardan elde edilecek delillerle ilişkin usuller yer almıştır. Öncelikle bu düzenlemeye m.147/1'e göre, bilgisayarlarda yapılacak her incelemenin KCMK m.136 ila 142 düzenlenen bilirkişi incelemesi şeklinde yapılacağı ve inceleme sonucunda bilirkişi raporu hazırlanacağı belirtilmektedir.

Bilgisayara el konulması için, KCMK m.147/2'de bir mahkeme kararına gerek olduğu belirtilmiştir. Bununla birlikte, maddede, "verilen rıza üzerine meşru şekilde alınan"

---

[254]Kosova Cumhuriyeti Ceza Kanunu, madde 327, fıkra 2, Bilgisayar Sistemine Giriş

[255] KCMK "Madde 147

Bilgisayar Analizleri

1. Bu madde kapsamındaki her inceleme ya da analiz, işbu Kanunun 136-142. maddelerinde belirtilen bilirkişi görüşü bildirme kuralları ve bilirkişi ifadesine tabi tutulur.

2. Bir mahkeme emri ya da onay üzerine meşru bir şekilde alınan bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da benzer teçhizatlar için, devlet savcısı bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da benzer teçhizatlar içerisinde bulunan bilgi ya da verilerin gözden geçirmesi, analiz etmesi ve araması için polis görevlisi veya bilirkişiyi yetkili kılabilir.

3. Yetkili polis görevlisi ya da diğer bilirkişi, bilgisayar analiz ve aranmasına ilişkin eğitim veya deneyime sahip olmalıdır.

4. Yetkili polis görevlisi ya da diğer bilirkişi, aşağıdaki bilgileri içerecek olan, işbu Kanunun 138. maddesine uygun olarak kendi bulgularıyla ilgili bir bilirkişi raporu çıkartır:

4.1. yetkili polis görevlisi ya da diğer bilirkişi, delilleri teşhis edici herhangi bir isim, rakam ya da etiket de dahil olmak üzere, incelenen bilgisayar teçhizatı, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarını açıklar.

4.2. yetkili polis görevlisi ya da diğer bilirkişi, bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarını polisten nerede ve nasıl alındığını açıklar.

4.3. yetkili polis görevlisi ya da diğer bilirkişi, bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarının denetlenme sırasını açıklar.

4.4. yetkili polis görevlisi ya da diğer bilirkişi, bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarında araması için yetkili olduğu spesifik olgulara dayalı bilgiyi açıklar.
4.5. yetkili polis görevlisi ya da diğer bilirkişi, bilgisayar dosyaları veya elektronik postalardan dosyaların kaybolmasını önlemek, dosyaları deşifre etmek, silinen dosyaları geri dönüştürmek veya verilerin alınması için atılan adımlar dahil fakat bunlarla sınırlı kalmayacak şekilde, aramayı eksiksiz ve güvenilir bir biçimde gerçekleştirmek için adli bilişim alanında en aktüel uygulamalar uyarınca atılan adımları açıklar.

4.6. yetkili polis görevlisi ya da diğer bilirkişi, arama sonuçlarını açıklar ve arama için önemli olan bilgisayar dosyalarının elektronik kopyalarını ekler.

bilgisayarlardan da bahsedilmiştir. Yukarıda 5271 sayılı CMK m.123'de ispat aracı olan eşya ve kazancın "muhafaza altına alınması" olarak tanımlanan kurumun, KCMK'da "kontrol" olarak tanımlandığı belirtilmiştir. Kontrol kurumunun düzenlendiği KCMK m.105/8'de[256] bilgisayar ve elektronik eşya sahibinin rıza göstermesi halinde, bu nesnelere muhafaza altına almak amacıyla el konulabilecek ve mahkeme kararına ihtiyaç duyulmaksızın KCMK m.147/2 uyarınca inceleme yapılabilecektir. Bu fıkra uyarınca devlet savcısı, inceleme için bir polis görevlisi ya da bilirkişiyi yetkili kılabilecektir. Polis veya başkaca bilirkişisinin bilgisayar incelemesinde gerekli eğitim ve deneyime sahip olması gerektiği de açıkça belirtilmiştir (KCMK m.147/3).

Polis görevlisi veya bilirkişinin bilgisayarı inceleme raporu, KCMK m.138'de açıkça belirtilen bilirkişi raporunda yer alması gereken unsurları taşımalıdır. KCMK m.138 yanında bilgisayar inceleme raporunda polis görevlisi veya bilirkişi; herhangi bir isim, rakam ya da etiket de dahil olmak üzere, incelenen bilgisayar teçhizatı, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarını tanımlar[257]. Öte yandan, polis görevlisi veya bilirkişi; bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyaların polis tarafından nereden ve nasıl elde edildiğini açıklarlar[258]. Polis görevlisi veya diğer bilirkişi; bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarının delil zinciri sırasını (toplama, kontrol, transfer, analiz gibi) da açıklar[259]. Ayrıca, bu raporda polis görevlisi veya diğer bilirkişi, bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da özel bilgisayar dosyalarında araması için yetkili olduğu belirli olgulara dayalı bilgiyi açıklar[260]. Polis görevlisi veya diğer bilirkişi, bilgisayar dosyaları veya elektronik postalardan dosyaların kaybolmasını önlemek, dosyaları deşifre etmek, silinen dosyaları geri dönüştürmek veya verilerin alınması için atılan adımlar dahil fakat bunlarla sınırlı kalmayacak şekilde, aramayı eksiksiz ve güvenilir

---

[256]KCMK m.105/8: "Bilgisayar, kamera, cep telefonu, seyyar elektronik cihazlar ya da korunmaya yarayan seyyar elektronik teçhizatlar dahil fakat bunlarla sınırlı kalmayacak şekilde, elektronik teçhizatların kontrol edilmesi için esasa dayalı nedenlerin mevcut olması halinde, kontrol emri bu tür cihaz ya da cihazların geçici el konmasını yetkilendirmek ve yetkili polis görevlisinin kontrol edebileceği ve kopyalayabileceği elektronik veri türlerini tanımlamak zorundadır".

[257]KCMK m.147/f. 4.1.

[258] KCMK m.147/f. 4.2.

[259] KCMK m.147/f. 4.3

[260] KCMK m.147/f. 4.4

bir biçimde gerçekleştirmek için adli bilişim alanında en güncel uygulamaları takip ederek yaptıklarını açıklar[261].

Bununla birlikte, Kosova'da bu yasal hükmün tek başına siber suçları önlemek ve mücadele etmek için yeterli olmadığı dikkate alınarak, uluslararası sözleşmelere, gelişmiş ülkelerin en iyi uygulamalarına ve onu sadece Kosova'da değil ötesinde teknolojik gelişmeler düzeyine uyarlayan bu alan için özel bir yasa olan 03/l-166 Sayılı Sibernetik Suçla Mücadele ve Önlenmesi Yasası çıkarılmıştır.

Sibernetik Suçla Mücadele ve Önlenmesi Yasa'sına göre, bu yasa, sibernetik suçları somut yasal tedbirlerle önlemeyi ve bunlarla mücadele etmeyi, insan haklarına saygı gösterilmesi ve kişisel verilerin korunmasını sunarak, bilgisayar sistemleri yoluyla ihlallerin önlenmesi, tespiti ve yaptırımını amaçlamaktadır. Bu yasanın amacının, bu alandaki cezai fiillerin önlenmesi, daha sonra bu fiillerin faillerin ve faillerinin başarılı bir şekilde keşfedilmesidir ve elbette nihai amaç, eylemleri gereği bu nitelikteki suçları işleyen tüm bireylere yaptırım uygulamak olduğu açıktır.

Ayrıca, bu yasa daha kesin olarak hangi eylemlerin bu tür suçlar olarak kabul edildiğini belirtmekte ve cezai suçların unsurları, işleyiş şekli, cezai yaptırım ve diğer gerekli veriler hakkında daha kesin açıklamalar vermektedir. Daha doğrusu, cezai suç olarak öngörülmüşlerdir Bilgisayar sistemlerinde veri gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suç işleri; İzinsiz Durdurma; Yetkisiz transfer; Bilgisayar sistemlerinin işlevliğinin engellenmesi; Yetkisiz üretim, sahiplik ve girişimler; Bilgisayarla ilgili suç işleri; Mal varlığının kaybına neden olmak; Bilgisayar sistemleri aracılığıyla çocuk pornografisi.[262]

Sibernetik Suçla Mücadele ve Önlenmesi Yasası, ayrıca devlet organlarının doğası gereği daha usule dayalı olan ve soruşturmanın yürütülmesi sırasında uygulanması gereken bu suçların soruşturulması ile ilgili bazı eylemlerini sağlar. Bu yasaya dayanarak, bu suç alanı ile ilgili ifadelerin bazı temel tanımlarını sunmamız bu çalışma için çok önemlidir. Bu tanımlar şunlardır:

---

[261] KCMK m.147/f. 4.5.

[262] Sibernetik Suçla Mücadele ve Önlenmesi Yasası, Maddeler 9-16.

-Sibernetik suç – bilgisayar sistemleri ve bilgisayar verilerini kötüye kullanma gibi suçun işlenmesi şekli gibi ya da bilgisayar ağında yapılmış olan bir suç etkinliği.

-Bilgisayar sistemi – bilgisayar programları sayesiyle otomatik bilgi işlemi sunan bir ya da daha fazla operatif bağlantısı olan ya da herhangi bir araç ya da bağlantılı araçların montajı.

-Otomatik bilgi işlem – bilgisayar sisteminde verilerin bilgisayar programları ile işlem gördüğü süreç.

-Bilgisayar programı – belirli sonuçların elde edilmesi amacıyla bilgisayar sistemi yolu ile uygulanabilir olan talimatlar grubu.

-Bilgisayar verileri - bilgisayar sistemi ile işlem görebilecek şeklinde deliller, bilgiler ya da kavramların her temsil edilişi. Bu kategori belirli fonksiyonu yerine getirmek için bilgisayar sistemlerini teşvik edebilecek her bilgisayar programını kapsar.

-Hizmet sağlayıcıları - kullanıcılara bilgisayar sistemi ile iletişim imkanını sağlayan özel ya da tüzel kişi ve bu hizmet sağlayıcıları için ve onlar tarafından sunulan hizmet kullanıcıları için bilgileri toplayan ya da işleme sunan kişi.

-Veri trafiğiyle ilgili veriler - iletişim zincirinin bir bölümünü temsil ederek, iletişimin kaynağını, hedefi, hattı, zamanı, tarihi, boyutu, hacmi ve süreyi ve iletişim için kullanılan hizmet türünü göstererek, bilgisayar sistemi ve ürünleri üzerinden yapılan iletişim ile ilgili bilgisayar verileri.

-Kullanıcı hakkında veriler - kullanılan iletişim ve hizmet türü, posta adresi, coğrafi adres, IP adresi, telefon numaraları veya diğer erişim numaraları ve ilgili hizmet ve de kullanıcı kimliğine neden olabilecek diğer verileri dahil ederek kullanıcı kimliğine yol açabilecek her türlü bilgi.

-Güvenlik önlemleri – bilgisayar sistemine erişimin belirli kullanıcı kategorileri için kısıtlandığı veya yasaklandığı belirli prosedürlerin, araçların veya özel bilgisayar programlarının kullanımı.

-Reşit olmayanlarla pornografik materyalleri – gerçek bir kişiyi temsil etmemelerine rağmen, açık cinsel davranışlarla reşit olmayan bir kişiyi güvenilir bir şekilde teşvik eden açık cinsel davranış veya resimlerle reşit olmayan bir kişiyi veya reşit olmayan olarak gösterilen reşit olan bir kişiyi gösteren her malzeme.

-Durdurma - yetkisi olmayan kişiler tarafından verilerin ele geçirilmesi ve alınması.[263]

Dünyadaki diğer ülkeler gibi Kosova Cumhuriyeti de, devlet mekanizmaları ve bu devlet faaliyetinin başarılı bir şekilde geliştirilmesine uygulanabilecek diğer yasalar dahil olmak üzere kurumsal mekanizmalar arasında siber suçların önlenmesi için bir strateji oluşturulmuştur. Yukarıda belirtilen yasalara (Ceza Kanunu ve Sibernetik Suçla Mücadele ve Önlenmesi Yasası) ek olarak, aşağıdaki yasalar da bu alanda geçerlidir:

- Kosova Cumhuriyeti Anayasası;
- 03/L-050 Sayılı Kosova Güvenlik Konseyinin Kurulmasına Ait Yasa;
- 03/L –166 Sayılı Sibernetik Suçla Mücadele ve Önlenmesi Yasası;
- 04/L-145 Sayılı Bilgi Toplumu için Devlet Organları için Yasa;
- 04/L-094 Sayılı Enformatik Toplum Hizmetlerine Ait Yasa;
- 04/L-109 Sayılı Elektronik Haberleşme Yasası;
- 05/L-030 Sayılı Elektronik İletişim Dinlenmesine Dair Yasa;
- 03/L – 172 Sayılı Kişisel Verilerin Korunması için Yasa;
- 04/L-076 Sayılı Polis Yasası;
- 03/L-142 Sayılı Kamu Asayiş Üzerine Yasa;
- 03/L063 Sayılı Kosova İstihbarat Teşkilatı Yasası;
- 04/L-149 Sayılı Cezai Müeyyidler İcra Yasası;
- 04/L-065 Sayılı Telif Hakları ve İlgili Haklar Yasası;
- 03/ L-183 Sayılı Uluslararası Cezaların Uygulanmasına Ait Yasa;
- 04/L-213 Sayılı Ceza Hukukuna Dair Uluslararası Hukuki Yardım;
- 04/L-052 Sayılı Uluslararası Anlaşmalar Hakkında Yasa;
- 04/L-072 Sayılı Devlet Sınır Kontrolü ve Denetimi Hakkında Yasa;

[263]Sibernetik Suçla Mücadele ve Önlenmesi Yasası, madde 3 Tanımlar.

- 04/L-093 Sayılı Mikrofinans Kurumları, Bankaları ve Banka Dışı Mali Kuruluşlara Ait Yasa;
- 04/L-064 Sayılı Kosova Forenzik Ajansına Ait Yasa;
- 04/L-198 Sayılı Stratejik Mallar ile İlgili Ticaret Kanunu;
- 04/L –004 Sayılı Özel Güvenlik Hizmetleri Yasası;
- 03/L-046 Sayılı Kosova Güvenlik Gücü Yasası;
- 03/L-109 Sayılı Kosova Gümrük ve İstihlak Vergisi Yasası;
- 03/l-109 Sayılı Kosova'da Gümrük ve Tüketim Vergisinin Değişme ve Tamamlamalarına Ait 04/L-099 Sayılı Yasa;
- 03/L-178 Sayılı Bilgi Sınıflandırılması ve Güvenliğin Doğrulanması Üzerine Yasa ;
- 04/L-082 Sayılı Kosova Cumhuriyeti Ceza Kanunu;
- 04/L-123 Sayılı Ceza MuhakemeleriKanunu;
- 03/L-122 Sayılı Kosova Cumhuriyeti Dış Hizmetler Yasası;
- 03/L-193 Sayılı Reşit Olmayanlara Ait Adalet Kanunu;
- Sınıflandırılmış Bilgilerin Dağıtımı ve Transferi Hakkında 18/2011 Sayılı Yönetmenlik.[264]

2.2.5. Türk Hukukunda Dijital Deliller

2.2.5.1. Genel Olarak

Türk hukukunda da dijital deliller, özellikle bilgisayar ve bilgisayar kütüklerinin aranması, incelenmesi ve el konulması için Kosova hukukundakine benzer şekilde 5271 sayılı Ceza Muhakemesi Kanununda (CMK) 134. maddesinde dijital delillerin ele geçirilmesine dair özel bir hüküm bulunmaktadır.

Dijital delillerin elde edilmesine ilişkin, CMK'da özel bir düzenlemeye olarak yer verilmiştir. Bunun nedeni ise teknolojik gelişmelerle birlikte bilgisayar ve akıllı telefon kullanımının artması ve bunların hayatın her alanına girmesidir. Devletler, bu yeni

[264]Kosova Cumhuriyeti Siber Güvenliği Devlet Stratejisi, 2016-2020, sayfa 18.

teknolojiler karşısında kendilerini ve yurttaşlarını koruma gereksinimi hissetmişlerdir. Pekçok devlet, günümüzde yasal düzenlemelerinde bilgisayar aracılığıyla işlenen suçları düzenlemiş ve yaptırımlar öngörmüştür. Devletler suçlarla etkin mücadele edebilmek amacıyla bu sürece kayıtsız kalmamış ve bilgisayar ve benzeri aygıtlarda bulunan delillerden faydalanmaya başlamıştır.

Dijital delillerin ele geçirilmesi KCMK'nun arama ve elkoymaya ilişkin genel hükümleri ve bu verilerin incelenmesine dair mevzuat uyarınca gerçekleştirilmektedir. Kosova hukukunda bilgisayarların donanımları ve yazılım sistemleri de bu çerçevede elkoyma kapsamında eşya şeklinde değerlendirilmektedir. Yapılan arama neticesinde bulunan aygıtlara geçici şekilde incelenmek için el konulması olanaklıdır; bu aygıtların incelenmesi kâğıtların incelenmesine dair hükümler gereğince yapılmaktadır, mevzuatta geçen "kâğıt" kavramının geniş şekilde yorumunun yapılması gerekir. Bu kavram ile yazı ve veri tabanları üstünde işlenmek suretiyle oluşturulan tüm düşünce açıklamaları anlaşılmaktadır. Bu biçimde düşünce açıklaması içeren aygıtlar, bilirkişi incelemesi yapılabilecek belirti delili niteliğindedir.

Fakat Türk Ceza Muhakemesi Kanunu'nun 134.maddesinde düzenlenen tedbirlerin konusu bilgisayarlar, bilgisayar kütükleri ve bilgisayar programları şeklinde belirlenmiştir. Donanım ve yazılımdan oluşan[265] bir cihaz olan bilgisayar sözlükte, "*çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyi*n" şeklinde tanımlanmaktadır[266].

2.2.5.2. Türk Hukukunda Dijital Delillere İlişkin Yasal Düzenlemeler

2.2.5.2.1. Ceza Muhakemesi Kanunu'nda Dijital Delillere İlişkin Düzenlemeler

CMK m. 116 ve devamı maddelerinde arama, CMK 127 ve 128. maddelerinde elkoyma tedbirlerine dair genel hükümler olsa da dijital delillerin ele geçirilmesi özel bir arama ve elkoyma kararına ihtiyaç duymaktadır. Çünkü bir bilgisayarın içinde ya da birbirine ağla bağlanan bilgisayarların ağ sistemi içinde delil araması ve elkoyma işlemi ayrı bir işlem

[265]Yusuf Yaşar/İsmail Dursun, Bilgisayarlarda, "Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", MÜHF-HAD, C. 19, S. 3, Y. 2013, s. 17.

[266] Türk Dil Kurumu, Türkçe Sözlük, Ankara 2005, s. 268.

özelliğini taşımaktadır[267]. 1412 sayılı Ceza Muhakemeleri Kanunu (CMUK) döneminde dijital delillere ilişkin uygulamada ortaya çıkan sorunlar, özel bir düzenleme bulunmadığından genel hükümlere başvurularak çözülmekteydi. Bu nedenle CMK m.134'de dijital delillerin toplanmasına ilişkin özel bir hüküm getirilmiştir. CMK gerekçesinde de belirtildiği üzere, CMK m.134arama ve elkoyma önlemine ilişkin özel bir düzenlemedir. CMK içisinde bilgisayarlara ilişkin bir madde olduğundan dijital delillere ilişkin göze çarpan ilk düzenleme olmaktadır.

Maddenin başlığına bakıldığında, maddenin içeriğinin sadece bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymaya ilişkin olduğu ve bütün dijital delilleri kapsamadığı ileri sürülmüştür[268]. Madde başlığı ve içeriğinde yalnızca bilgisayarlar ve bilgisayar kütüklerine ilişkin olması sebebiyle dar yorum yapıldığında bilgisayar ve bilgisayar kütüğü özelliğini taşımayan aygıtlara ilişkin olarak CMK m.134'ün tatbik edilmesi olanaklı olmayacaktır[269]. Bu sorun CMK'daki düzenlemenin veri değil, bilgisayar merkezli düzenlenmesinden ileri gelmektedir. Bu durumda CMK m.134'ün bilgisayar ve bilgisayar kütükleri haricindeki aygıtlara yönelik olmayacak ve başka aygıtlar bakımından dijital delil, arama ve elkoyma önlemleri genel kurallar uyarınca yerine getirileceği ileri sürülebilir[270]. Kanaatimizce CMK m.134'de yer alan düzenlemenin, genel arama ve el koyma usullerine göre güvenli olması ve olabildiğince hâkim kararına dayanarak arama yapılması usulünün getirilmesi sebebiyle bilgisayar haricindeki aygıtlar bakımından da CMK m.134'ün uygulanabileceği açıktır. Uygulamada da bilgisayar haricindeki aygıtla bakımından da CMK m.134'ün uygulandığı anlaşılmaktadır[271].

CMK m.134'ün yalnızca depolanmış bilgisayar verilerine ilişkin olduğu görülmektedir. Verilerin akış halinde bulunduğu durumlar, CMK m.134'de düzenlenmemiştir. Türk hukukundaki bu boşluk CMK m.135 ile düzenlenen iletişimin tespiti, dinlenmesi, kayda

---

[267] Osman Gazi Ünal, "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma", Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011, s. 84-85.

[268] Dülger, Bilişim Suçları, s.726

[269] Dülger, Bilişim Suçları, s.726

[270]Kaynakçıoğlu, s.110.

[271] Cengiz Tanrıkulu, Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma, Ankara: Adalet Yayınevi, 2014, s. 358.

alınması ve sinyal bilgilerinin değerlendirilmesi[272] tedbirleri aracılığıyla karşılanmaktadır[273].

Ayrıca CMK m.116 ve devamı maddeleri uyarınca yapılan aramalarda, tesadüfi olarak elde edilen delillerde nasıl hareket edileceği CMK m.138'de düzenlenmiştir. Bu madde uyarınca olağan arama ve elkoyma tedbirlerinin tatbik edilmesi esnasında yürütülen soruşturma ya da kovuşturma ile ilgisi bulunmayan, başka bir suçun işlendiği şüphesi uyandıran bir dijital delil ele geçirilirse, bu delil koruma altına alınır ve bu durum hemen savcılığa iletilir. Bu maddede "*arama ve elkoyma tedbirlerinin uygulanması sırasında*" lafzını dar şekilde yorumlamamak gerektiği, tesadüfen delil etme durumunun CMK m.134 kapsamında yapılan aramalar için de geçerli olduğu belirtilmiştir[274]. Kanaatimizce tesadüfen elde edilen dijital delillerde de Cumhuriyet savcısına haber verildikten sonra, dijital verilere elkoyma tedbirinin CMK m.134/1 gereğince hâkim onayına sunulması gerekmektedir.

2.2.5.2.2. Diğer Düzenlemelerde Dijital Delillere İlişkin Hükümler

Elektronik haberleşmenin bir türü olan internet ortamlarında yapılan yayınlar, 5651 sayılı Kanun ile düzenlenmiştir. Bu yasa kapsamında bilhassa internet üzerindeki verilerin ele geçirilmesi bakımında önemli düzenlemeler bulunmaktadır. Dijital delil elde etme çalışmaları internete de uzandığı durumlardabu hükümlere ihtiyaç duyulmaktadır. Bu amaçla 5651 sayılı Kanun m.1'de internet servis sağlayıcılarının; erişim, içerik, yer ve toplu kullanım sağlayıcı olarakdört farklı sağlayıcıdan oluştuğu belirtilmiş ve 2. maddesinde bu sağlayıcıların tanımlarına yer verilmiştir[275].Özelikleinternet kafeler gibi

---

[272] CMK m.135'e ilişkin geniş bilgi için bkz.Kunter/Yenisey/Nuhoğlu (2013), a.g.e. , s. 1339 vd.; Seydi Kaymaz, İletişimin Denetlenmesi: Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan, 4. Baskı, Ankara: Seçkin Yayınevi, 2015; Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi", Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XI, Sayı: 1-2, 2007, ss. 1095-1112.

[273]CMK m.135'in uygulanma usulü, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik'in 17. maddesinin b fıkrasında düzenlenmiştir.

[274] Yaşar, Dursun, s.23.

[275] 5651 sayılı Kanun m.2: "…e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

toplu kullanım sağlayıcılar dışında özellikle yer ve erişim sağlayıcılara yönelikbazı yükümlülükler konulmuştur.

Kanun m.5/3'de. yer sağlayıcı kurum ve kişilere bilgi saklama yükümlülüğü konulmuştur. Bu kapsamda, belirtilen süre saklanan dijital verileri soruşturma veya kovuşturma organları talep edebilecektir. Erişim sağlayıcılar da m.6/1'de bilgi saklama ve depolama yükümlülüğü getirilmiştir[276].

Ayrıca 5809 sayılı Elektronik Haberleşme Kanunu m.12'de dijital delillere ilişkin önemli bir hüküm vardır. İşbu maddenin 2. Fıkrasına göre Bilgi Teknolojileri ve İletişim Kurumu, *sektörün gereksinimleri, uluslararası düzenlemeler, teknolojik gelişmeler gibi konular dikkate alarak işletmecilere*[277] *mevzuat kapsamında yükümlülükler getirebilecektir*[278].

Adli ve Önleme Aramaları Yönetmeliği m. 17/1-4 ile CMKm.134/1-4 neredeyse birebir aynıdır. Yönetmelik m.17/3 ve 17/5'de CMK m.134/3 ve 134/5'deki noksanlıkları giderecek ek maddeler düzenlenmiştir.

Yönetmelikm.17/3[279], CMKm.134/3 ile uyumlu hüküm getirmiş fakat devamında CMK'da bulunamayan yedekleme işleminin bilgisayar ağları ve diğer uzak bilgisayar kütükleri ve çıkarılabilir donanımlara yönelik uygulanabileceği düzenlemesi getirilmiştir. Yönetmeliğe getirilen bu ek ifade ile olay yerindeki bilgisayarlar dışında USB,SD kart, CD, çıkarılabilir hafıza aygıtları gibi veri depolama birimlerinde yedekleme yapılabileceği ifade edilmektedir. Öte yandan, bu hüküm ile WAN, LAN gibi ağlara bağlı bilgisayarlardan

---

m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri… ifade eder."

[276]İçerik, erişim ve yer sağlayıcıların BTK'nın talep ettiği bilgileri, bu kuruma iletmesinde ilişkin yükümlülüğünün yer aldığı 5651 sayılı Kanun m.4/3, m.5/5, 6/1-d Anayasa Mahkemesince iptal edilmiştir, bkz Anayasa Mahkemesi 8/12/2015 tarih ve E.: 2014/87, K.: 2015/112 sayılı Kararı.

[277] 5809 sayılı Kanun m.3/z: "İşletme: elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi…ifade eder"

[278]Anayasa Mahkemesi, dijital delile konu olabilecek ve BTK'ya, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisinin verildiği 5809 sayılı Kanun m.51'i, Anayasanın 20. Maddesine aykırı bularak iptal etmiştir, bkz.AYM E. 2013/122, K. 2014/74, T. 09.04.2014; Ayrıca m.12/2-g ile işletmecilere,"*Kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması.*" yükümlülüğü getirilmiştir

[279] CMKm.134/3: *"Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerinyedeklemesi yapılır".*

uzaktan yedekleme yapılabilmesi hükmü konuşmuştur. Yönetmelik'e yapılan bu ekleme ile CMK m. 134/3'deki eksiklikler giderilmeye çalışılmıştır[280].

Öte yandan, Yönetmelik m.17/3'de aramadan söz etmeyip sadece yedeklemeden söz etmekte ise de CMK m.134 gereğince arama işleminde ele geçirilmeyen aygıtlar üstünde doğrudan yedeklemenin yapılması olanaklı değildir. Çünkü, elektronik verilere erişilebilmesi öncelikle arama yapılmasına tabidir. Doğal olarak, yedekleme, aramadan sonra gerçekleştirilmesi gereken bir işlemdir. Bu açıdan, anılan Yönetmelik düzenlemesi gereğince uzak bilgisayar kütükleri, bilgisayar ağları ve USB gibi çıkarılabilir hafıza birimleri hakkında da arama, kopyalama ve elkoyma faaliyetleri tatbik edilebilecektir[281].

Öte yandan, bilgisayar ve bilgisayar kütüklerine uzaktan erişimedair kanuni bir düzenleme bulunmadığından Yönetmelik düzenlemesinde ye alan bu ifadenin; arama, kopyalama ve elkoyma önlemi neticesinde gerçekleştirilecek yedekleme işlemleriyle sınırlı tutmak ve uzaktan erişimle arama biçimde geniş şekilde yorumlamamak gerekir[282]. Bu kapsamda bir özel tüzelkişiye ait bilgisayarlarda veri araması gerçekleştirildiği sırada, gereken bilgilendirmenin yapılması ve anılan Yönetmelik maddesi gereğince tüzel kişinin ağına bağlı farklı bilgisayarlardaki veriler incelenebilir ya da kopyalanabilir. Bu durum,hukuki açından uzaktan erişim olarak kabul edilemez[283]. Ancak ağ sisteminde bilgisayar verilerinin server gibi başka sistemlerde saklanma imkanı bulunduğundan, bu düzenleme yetersiz kalmakta ve daha ayrıntılı düzenleme yapılması gerekmektedir[284].

Yönetmelik m.17/5 ile CMK m.134/5'de yer alan düzenlemeden daha geniş bir hüküm getirilmiştir[285]. Yönetmelik'teki bu hükümle kopyalanan verilerin içerik olarak ne olduğu değil,

---

[280] Başlar, s.212.

[281] Yaşar ve Dursun, s. 16.

[282] Ünal, s. 139.

[283] Değirmenci, Dijital Delil, s. 199.

[284] Kunter, Yenisey, Nuhoğlu, s. 1102-1103.

[285] CMK m.134/5'in ilk cümlesi: *"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir*

Yönetmelik m.17/5:

"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer

liste olarak isimlerinin neler olduğu yazılacaktır.Yönetmelikteki bu hükümle, uygulamada eleştirilen CMK m.134/5'deifade edilen çok fazlabelge çıktısı alma işlemine gerek kalmamıştır[286].

Bu bağlamda Yönetmeliğin 17. maddesinin, CMKm.134'deki tedbirlerin uygulama alanını kolaylaştırdığı (m. 17/5) ve genişlettiği söylenebilir (17/3). Kanaatimizce temel hak ve hürriyetleri sınırlayan ve kanunla düzenlenmiş bir koruma önleminin, Yönetmelik hükmüyle tatbik edilme sahasının genişletilmesi sorunludur. Ancak CMK'nın 134. maddesindeki tedbirin uygulama alanı içinde kalmayan bir eşya üstünde genel hükümlere yani klasik arama ve elkoyma tedbirlerine (CMK m.116 vd, m.127) başvurulacak olması sebebiyle, yasal düzenleme yapılana kadar bilgisayar ağları ve uzak bilgisayar kütükleri ile çıkarılabilir donanımları açısından uygulama alanını genişletilen Yönetmelik hükmünün uygulanması gerektiği düşüncesindeyiz[287].

2.2.5.3. Ceza Muhakemesi Kanunu'nda Bilgisayar ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri

2.2.5.3.1. Tedbirin Amacı

Bilişim sistemlerinde gerçekleştirilen aramada ele geçirilmesi hedeflenen bilgi, belli bir formatta ve bir sistem tarafından okunabilir duruma gelmiş bilgidir. Belli bir formatta olan bilgi, elektronik veri şeklinde adlandırılmaktadır. Bu elektronik veri, soruşturma veya

---

tarafından imza altına alınır" düzenlemesi yerine *"Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir"*

[286] Başlar, s.213.

[287] Başlar, s.213; Resmi Gazete, Tarih: 01.06.2005, Sayı: 25382; Son olarak, Suç Eşyası Yönetmeliği'nin "*Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler*" başlıklı m.9/2'de ele geçirilen dijital verilen saklanmasına ilişkin hüküm getirilmiştir.Bu fıkra şu şekildedir: "*Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir.*" Bu maddenin beşinci fıkrasında da şu şekilde bir düzenleme getirilmiştir: "*Yapısı gereği sabit diskler ve diğer elektronik materyaller ısıya, neme ve sarsıntıya karşı hassastırlar. Bu madde ile elkonulan bilgisayar, bilgisayar kütükleri, bu sisteme ilişkin verilerin asıl ya da kopyalarının ve depolama aygıtları gibi eşyaların bozulmalarını engellemek için uygun ortamlarda muhafaza edileceği düzenlenmiştir. Emanet dairesi / deposunda saklanması mümkün olmayan eşyaların sulh hâkiminden, soruşturma sonu bekletilmeksizin satılmasına veyahut uygun görülen farklı bir mercie teslim edilmesine karar verilmesi talep edilir ve neticede verilen karar uygulanır.*" Bu fıkradaki "satılma" hükmü kesinleşmiş müsadere kararının bulunmadığı hallerde mülkiyet hakkını ihlal edebilecektir; Kaynakçıoğlu, s.120

kovuşturma esnasında maddi olayın ispatı için kullanılabilmesi halinde delil özelliği kazanacak ve elektronik delil meydana çıkmış olacaktır[288].

CMK m. 116'da genel arama ve CMK m.123 ve 127'deki el koyma işlemlerinin amacı, failin yakalanması veya suç delillerinin ele geçirilmesi ile suç delili eşyanın iade veya müsadere edilmesine kadar korunmasıdır.

Bilgisayarlarda ve bağlantılı eşyada arama, kopyalama ve elkoyma bilhassa bilişim suçlarına dair dijital delillerin ele geçirilmesinde önemli yere sahiptir.CMK m. 134'deyer alan bu tedbirlerde ise failin yakalanması ikincil bir amaç olmakta ve bu tedbirin asıl amacı, delillerin ele geçirilmesi ve korunmasıdır. Bu açıdan bu maddedeki tedbirin ilk amacının dijital delil ele geçirmek ve bu delilin aslı veya usulüne uygunalınmış kopyasının korunması olduğu ifade edilebilir[289]. Elde edilen bu delillerle hâkim, yargılamada vicdani kanaat oluşturabilmektedir.

2.2.5.3.2. Tedbirin Kapsamı

CMK m. 134/1'de tedbirin kapsamı; maddede soruşturma aşamasında ibaresi kullanıldığından şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleridir. Bu maddede geçen kavramlardan *bilgisayar,* çok sayıda aritmetik ya da mantıki işlemlerden meydana gelen bir işi, evvelden oluşturulmuş bir programa göre yapıp neticelendiren elektronik araç ya da elektronik beyin şeklinde tanımlanmaktadır[290].

Bilgisayar programları[291], bilgisayar kullanıcılarının işlem yapabilmelerine yaramaktadır. Bu işlemlerin yaptırılabilmesi girilen komutlar ve diziler, belirli kurallara göre oluşturulmuştur. Bu kurallara "programlama dili" adı verilmektedir[292]. Bilgisayar programlarında arama gerçekleştirilmesi halinde bu tedbirin uygulaması veri saklama alanlarına da sirayet edecektir.

---

[288]Değirmenci, Dijital Delil, s. 59-60.

[289]Başlar, s.170.

[290]https://sozluk.gov.tr/, Erişim tarihi: 22.03.2022.

[291] *Bilgisayar programı ise* 5846 sayılı FSEK m. 1/B'de "*Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları*" biçiminde ifade edilmiştir; Başlar, s.171

[292] Aysan Şentürk, (Ed.). Bilgisayar Kullanımı ve İnternet. Ankara: Ekin Yayınevi, 2007, s.40.

Bilgisayar kütükleri kavramından ise*;* sabit diskin kastedildiği, İngilizce olan "log" teriminin karşılığı olarak "kütükler" kavramının çoğunlukla internet servis sağlayıcılarının kullanıcılara sağladıkları IP numaraları ve erişim bilgilerinin depolandığı veri tabanları anlamına geldiği belirtilmektedir[293]. Bunun haricinde, büyük çaptaki verileri depolayan veri tabanları ya da arşiv için kullanılan büyük kapasitedeki veri saklama birimleri de bilgisayar kütüğü şeklinde tanımlanmaktadır[294].

CMK m. 134/1'de şüphelinin kullandığı ve bilişim sistemi içeren cep telefonu, cep bilgisayarı, dijital fotoğraf makinesi veya kamera gibi taşınabilir aygıtlara ilişkin bir hüküm yoktur. Ancak adli bilişimin esas konusu dijital delil olduğundan bu delil kaynağını yalnızca bilgisayar ile kısıtlamak sorunlu bir yaklaşım olup, günümüzde neredeyse herkesin kullandığı bu cihazlarda elde edilebilecek önemli delillerin bulunabileceği açıktır. Kaldı ki bu aletlerin pek çoğu bilgisayarlar gibi işletim sistemleri, işlemciler ve depolama alanlarına sahiptir. Fakat uygulamada bu tür aygıtlarda bulunması olası delilleri elde etmek için CMK m.116 ve 123'da yer alan arama ve elkoymaya dair genel düzenlemeler kullanılmaktadır[295].Ancak, kanaatimizce bu önemli konu yasal düzenleme yapılması gerekmekte olup, koruma tedbirlerinde pozitif bir düzenleme yoksa kıyas yapılması mümkün olmasa da[296], düzenleme yapılıncaya kadar daha fazla hukuki güvenlik sağlayan CMK m.134 hükmü kullanılması daha isabetli olacaktır.

Son olarak elektronik postalara ilişkin ele geçirilmesi olası dijital delillerin CMK m.134 kapsamında olup olmadığı tartışmalıdır. Doktrinde bir görüş, elektronik posta üstünden dijital delil toplanması gündeme geldiğinde CMK m. 134 değil, m. 135'te ye alan iletişimin denetlenmesi tedbirinin uygulanması gerektiğini ileri sürmektedir[297].

---

[293] Değirmenci, Dijital Delil, s. 52-53.

[294] Başlar, s.172.

[295] Başlar, s.173.

[296]Unver/ Hakeri, C.1, s.79.

[297] Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme", Bilişim Hukuku Konferansı-YARGITAY, Ankara, 09-10 Ekim 2008, s. 124; Elektronik postanın adli soruşturmalar bakımından CMK m. 135 uyarınca teknik takibinin mümkün olmasının yanı sıra idari (önleyici) maksatla Polis Vazife ve Selahiyet Kanunu (PVSK) ek m. 7 ve Jandarma Teşkilatı Kanunu ek m. 5 uyarınca ve istihbarat amaçlı olarak Milli İstihbarat Teşkilatı Kanunu m. 6 uyarınca da teknik takibe konu olabilir, bkz. Ersan Şen, "E-Posta Takibi", Terazi Hukuk Dergisi, Cilt. 9, Sayı. 97, Eylül 2014, s. 88.

Katıldığımız diğer bir görüşe göre ise, elektronik postanın internet üzerinde posta hizmeti şeklinde verildiği, kişiye tahsis edilen alanda kendi elektronik postalarının depolandığı, normalde göndericinin sunucusundan, alıcısının sunucusuna elektronik postanın gitmesi halinde, elektronik postanın akış durumunun sonlandığı, elektronik postanın akışı esnasında CMK m.135'in uygulanabileceği, fakat elektronik posta diğer tarafa ulaştıktan sonra, elektronik posta hizmetini veren urumun bilişim sistemlerinde yer alıp okunmamış bile dahi CMK m. 134 gereğince işlem yapılması gerekir[298].

2.2.5.3.3. Tedbirin Uygulanma Şartları

CMK m.134'deki tedbirinin tatbik edileceği suç türleri açısından yasada sınırlayıcı bir düzenleme yoktur. Bu tedbirin özelliği gereği, bilişim suçlarında uygulanması gerektiği yönünde bir izlenim olsa da, sınırlama olmadığı için diğer suçlar açısından da uygulanabilmesi mümkündür[299]. Fakat bu tedbire başvurulması için yasada belli şartlar bulunmaktadır.

2.2.5.3.3.1. Bir Suç Soruşturmasının Bulunması

Bu madde kapsamındaki tedbire başvurulabilmesi için ilk olarak bir suç nedeniyle açılmış bir soruşturmanın bulunması gerekir. CMK m. 134/1'de suçun niteliği, adı veya ağırlık seviyesi açısından bir kısıtlama getirilmemiş olup bu maddenin yürürlüğe girdiği ilk halinde şüphenin niteliğinden de söz edilmemiş olup, 21.02.2014 tarih ve 6526 sayılı Kanunla (m.11) gerçekleştirilen değişiklikten evvel bir suçun işlendiğine ilişkin makul şüphenin bulunması halinde bu tedbir uygulanabilmekteydi. Bu durum doktrinde; temel hak ve hürriyetlerin korunması açısından bu tedbirin tatbik edilmesinin sadece "*kuvvetli suç şüphesi*"nin bulunması[300]ve belirli ağırlıktaki suçlar açısından tatbik edilmesi gerektiği[301] yönünde eleştirilmekteydi[302].

---

[298]Değirmenci, Dijital Delil, s. 332-333

[299] Veli Özer Özbek, Ceza Muhakemesi Hukuku. Ankara: Seçkin Yayıncılık, 2006, s. 364

[300] Muharrem Özen ve İhsan Baştürk, Bilişim-İnternet ve Ceza Hukuku, Ankara: Adalet Yayınevi, 2011, s. 147.

[301]Centel ve Zafer, s. 391.

[302] Bu konuda ceza süresi şartı aranmaksızın her fiil için bu tedbir başvurulmasının orantılılık ilkesinin ihlali olduğu belirtilmektedir. Bkz. Özen ve Baştürk, s. 148; Yaşar ve Dursun, s. 10.

Anılan Kanunla değiştirilen CMK'nın 134/1 maddesi ile bu tedbirin uygulanması "s*omut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*" koşuluna tabi kılınmıştır. Bahse konu değişiklik, söz konusu tedbirin ihlal edebileceği temel hak ve özgürlüklerin korunması açısından olumlu bir gelişme olmuştur[303].

Kuvvetli şüphenin iki unsura ilişkin olarak bulunmalıdır. İlk olarak, şüphelinin, soruşturma konusu suçu işlediğine dair kuvvetli şüphe bulunmalıdır. İkincisi ise, bu kuvvetli şüphe, şüphelinin kullandığı bilişim sistemlerinde suç soruşturmasına ilişkin bir delil elde edilebileceğine dair olmalıdır. Şüpheli aleyhinde suçu işlediğine ilişkin kuvvetli şüphe mevcut olsa bile, şüpheli tarafından kullanılan bilgisayar sisteminden, suça dair bir delil elde edileceğine ilişkin kuvvetli şüphenin dayanağı oluşturan somut delillerin bulunması gerekmektedir[304].

Öte yandan, yasa maddesinde son çare ilkesi de denilen bu tedbire diğer türlü delil ele geçirme olanağının var olmaması dur umunda başvurulabileceği hususu getirilmiştir. Ancak bu kriter ile kanun metnine daha sonra eklenen "*somut delillere dayalı kuvvetli şüphe*" nedenlerinin varlığı koşulu da maddenin teoride uygulama alanını önemli şekilde sınırlanmış olup, kanaatimizce bu durum aynı zamanda bir çelişki de oluşturmaktadır. Bu nedenle, doktrinde yasa metnine bu tedbirin uygulanabilmesi için "*belli ağırlıktaki suçlar bakımından uygulanma*" koşulunun getirilmesinin tedbiri uygulanamaz hale getirmesi olası olduğundan gerek bulunmadığı belirtilmiştir[305].

Hâkim kararında ya das gecikmesinde sakınca olan durumlarda savcının kararında tedbirin uygulamasının, soruşturma konusu bir suça ilişkin elektronik veri ya da delili ele geçirmek için yapıldığının ifade edilmesi gerekmektedir. Ancak bu kararda, delilin tedbirin uygulanacağı bilişim sisteminin belli bir yerinde olması şeklinde bir belirliliğe gerek bulunmamaktadır. Ayrıca bu tedbire işlenen herhangi bir suça ilişkin başvurulabilmesi mümkün olup, kabahat ya da disiplin fiilleri sebebiyle yapılan idari soruşturmalarda bu tedbir uygulanamaz.

---

[303] Yusuf Başlar, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, Uyuşmazlık Mahkemesi Dergisi, Cilt. 1, Sayı. 3, Haziran 2014, s. 87-88.

[304] Değirmenci, Dijital Delil, s. 352-353.

[305] Başlar, s.177.

Madde metninde bu tedbirin soruşturma safhasında uygulanabileceği belirtilmektedir. Bu neden bu tedbire kovuşturma safhasında başvurulamayacağı ileri sürülse de[306], kanun koyucunun madde metninde "sadece", "yalnızca" ve "ancak" gibi bir kelime kullanmaması ve kovuşturmada delil serbestisi ilkesi bulunduğundan bu tedbire kovuşturmada başvurulamaması hukuk mantığı ile bağdaşmayacağı ve bu tedbire başvurulabileceği kanaatindeyiz[307].

Bu tedbire başvurmanın nedeni, başka surette ele geçirilemeyen delili elde etmektir. İddianamenin kabulü ile kovuşturmanın başlaması ise kamu davası açılması amacıyla yeterli şüpheye yol açacak delilin ele geçirildiğini göstermektedir. Bu halde ise bahse konu önleme başvurmaya gerek bulunmamaktadır[308]. Ancak, kovuşturma aşamasında özellikle internet erişim ve servis sağlayıcılarının sabit disklerindeki (server) delillerin ele geçirilmesi ya da dava açıldıktan sonra sanığa ait olduğu anlaşılan bir taşınabilir bellek veya bilgisayarda delil elde etmek için bu tedbire başvurulabileceğini düşünüyoruz.

2.2.5.3.3.2. Hâkim Kararı veya Cumhuriyet Savcısı Kararı

Bu tedbire, hâkim veya 25/7/2018 tarihli ve 7145 sayılı Kanunun 16 maddesi ile CMK m.134/1'de gerçekleştirilen değişiklik ile gecikmesinde sakınca olan durumlarda Cumhuriyet savcısı karar verir. Yine aynı kanunla yapılan değişiklikle Cumhuriyet savcısı CMK 134 kapsamında verdiği kararlar, yirmi dört saat içinde sulh ceza hâkimi onayına gönderilir. Hâkim kararını en geç yirmi dört saat içinde verecektir. Hâkimin onayına sunma süresinin dolması ya da hâkim tarafından kararın onaylanmaması durumunda elde edilen kopyalar ve çözümü gerçekleştirilen dökümler hemen yok edilir.Bu değişiklikten önce bu tedbire sadece hâkim karar verebilmekteydi ve Cumhuriyet savcısı tarafından el konulan delillerin hâkim onayına sunulması gibi bir usul de bulunmamaktaydı[309].

---

[306] Kunter, Yenisey ve Nuhoğlu, s. 1098.

[307] Şahin, Ceza Muhakemesi Hukuku I, s. 268; Değirmenci, Dijital Delil, s. 318; Parlar ve Hatipoğlu, s. 532; Yaşar ve Dursun, s. 9, Tanrıkulu, s. 400.

[308] Haluk Çolak ve Mustafa Taşkın, Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku, 2. Basım, Ankara: Seçkin Yayıncılık, 2007, s. 607.

[309] Taşkın, s. 168.

Önleme aramalarında (örneğin PVSK m.9) bilişim sistemlerinde arama yapılması mümkün değildir ve bu tür bir arama, özel hayatın gizliliği ve mülkiyet haklarını birlikte ihlali anlamına gelir[310].

2.2.5.3.3.3. Tedbirin Şüphelinin Kullandığı Bilişim Sistemlerinde Uygulanması

Bu tedbir, başlatılan soruşturmada sadece şüphelinin kullandığı bilişim sistemleri üstünde tatbik edilebilecektir[311]. Üçüncü kişilerin bilgisayar ve bilişim sistemleri üstünde ise bu tedbir uygulanamayacaktır. Sanık vasfını kazananlara yönelik bu tedbirin uygulanmayacağı ileri sürülse de, sanıklar hakkında da bu tedbirin uygulanabileceği kanısındayız. Bu tedbirin uygulama alanını, şüphelinin haricindeki üçüncü kişiler aleyhinde genişletmek, bu kişilerin temel hak ve özgürlüklerinin ihlali olabilecektir.

Öte yandan bu hükümde maddede şüphelinin "sahip olduğu" yerine şüphelinin "kullandığı" ifadesi yer almıştır. Şüphelilerin işledikleri suçlarda kendi isimlerine kayıtlı olan ya da kendilerinin sahip olduğu belirlenecek haldeki bilgisayar, bilgisayar programları ve kütüklerini kullanmazlarsa,bu düzenlemenin isabetli olduğu görünmektedir. Şayet maddede yalnızca "sahip olduğu" ifadesi konulmuş olsaydı bu tedbirin uygulanması çok sınırlı olacaktı[312]. Yargıtay da internet kafede şüphelinin kullandığı bilişim sistemlerinde arama yapılabileceğine karar vermiştir[313].

Uzaktan erişim ya da çok kullanıcılı erişim biçimindeki "kullanma" hallerinde tedbirin tatbik edilip edilmeyeceği konusu da sorunlu alanlardan biridir. İlk olarak, şüphelinin bir bilişim sistemini kullanmak suretiyle uzaktan erişimle farklı bir bilişim sistemine müdahale etmesi ve kötü niyetli yazılımlarla yönlendirmesi halinde de bu tedbirin tatbik edilip edilmeyeceğinin tespiti gerekir. Uzaktan erişilen bilişim sistemlerinde şüphelinin işlediği ileri sürülen suçun delillerinin bulunulabilmesi mümkündür. Fakat şüphelinin kullandığı

---

[310] Başlar, s.182-183.

[311] Yargıtay 17. CD. T: 15.02.2017 E: 2015/27517 K: 2017/1716, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, erişim tarihi: 05.04.2022.

[312] Çolak ve Taşkın, s. 608.

[313] Yargıtay 1. CD. 14.11.2005. E. 2005/3891, K. 2005/3230, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, erişim tarihi: 05.04.2022.

bilgisayarın internete bağlı olması, onun bağlantı kurduğu sunuculara da bu tedbirin uygulanabileceği sonucu, başkalarının temel hak ve özgürlüklere zarar verecektir[314].

Bunun yanında, şüpheli, çok kullanıcının olduğu işletim sistemlerinde kendisinin hesabına girerek kullanmış olabilir. Burada, fiziki anlamda tek bilgisayar kullanılmasına rağmen, bilgisayar sanal şekilde pekçok parçaya bölünmüştür. Burada sadece şüpheli tarafından kullanılan hesaba ait aygıt ve veriler üstünde inceleme yapılabilmelidir. Bunun haricinde, sanal anlamda bölünmüş bir sistemin tümü üstünde tedbirin tatbik edilmesi isabetli olmayacaktır[315].

CMK m.134'de tedbirin şüpheliye uygulanacağı belirtilmişken, mağdur veya şikayetçinin bilişim sistemlerinde uygulanmasına ilişkin bir düzenleme yer almamıştır. Doktrinde katıldığımız görüş uyarınca[316]bilgisayar veya bilişim sisteminin mağdur ya da şikâyetçinin olması şartıyla, bu şahısların açık rıza beyanı ile gereken arama, kopyalama ve muhafaza işlemleri CMK m. 134'te yer alan şartlara bakılmaksızın yapılabilir. Çünkü bu işlemler CMK m.134 kapsamında değil, CMK m. 160/2 çerçevesinde emrindeki kolluk aracılığıyla savcılığın maddi gerçeğin araştırma ve delilleri toplama ve muhafaza altına alma yükümlülüğü içinde görülmelidir.

Kamu görevlilerinin görev yaptıkları kurumca tahsis edilen bilişim sistemleri üstünde kurum amiri ya da teftişle görevlendirilen kişinin tarafından arama işlemini yapması amacıyla CMK m. 134'daki usulün uygulanıp uygulanmayacağı tartışmalıdır. Bir görüş, kamu kurumunca verilen bilişim sisteminin kurum faaliyetlerinde kullanılmak için verildiği ve mülkiyetinin kuruma ait olması nedeniyle, kurum amiri veya müfettiş tarafından inceleme yapılabileceği ileri sürülmektedir[317]. Katıldığımız diğer görüş uyarınca, kurum tarafından kamu görevlilerine tahsis edilen bilişim sistemleri üzerinde bu görevlilerin mahremiyet hakları vardır. Ancak bu hak, ilgili kurumun ilan ettiği ve periyodik şekilde

[314] Değirmenci, Dijital Delil, s. 321.

[315]Değirmenci, Dijital Delil, s. 322.

[316] Başlar, s.185.

[317] Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt. 12, Özel Sayı, 2010, s. 1410.

yapılan bilişim sistemleri üzerindeki denetimleri engellemeyecektir[318]. Fakat bir suç ihbarı alındıktan sonra kurum amirleri tarafından yapılan arama ve delil toplama işlemleri hukuka aykırı kabul edilir. Bu durumda ilgili kolluk birimlerince CMK m.134'de usule uyularak işlem yapılmalıdır.

2.2.5.3.3.4. Tedbirin Uygulanması

CMK m. 134/1 düzenlemesinde yer alan koşulların bulunması durumunda ilk olarak şüphelinin bilgisayar ve bilişim sistemlerinde arama yapılır, suça ilişkin dijital delilin bulunup bulunmadığı araştırılır, dijital delilin bulunması halinde kopyalama yapılır ve ele geçirilen veya kopyalanan delil çözümlenerek metin haline getirilir.

Anılan fıkra çerçevesinde bilişim sistemlerinde gerçekleştirilecek arama, adli bilişim normlarına uygu şekilde yapılmalı ve dijital delillerin zarar uğraması önlenmelidir. Delil niteliğine sahip dijital kayıtların belirlenmesi halinde, bu kayıtların imajı (kopyası) çıkartılmalı ve bu kayıtlar çözümlenerek metne dökülmelidir. Bu düzenleme gereğince metne dökülen bilgisayar kayıtları,dijital delil vasfında olduğu kabul edilen ve kopyası alınan kayıtlardan oluşmaktadır. Ayrıca bu düzenleme kapsamında yapılan birebir kopyalama işlemi sonrasında sistemin hash (veri bütünlük) değerinin alınması gerekir. Ceza yargılamasının süjelerinin dijital delillere yönelik önyargılı tutumları, yasa koyucuyu Dijital delilleri, fiziksel delil vasfına büründürme çabasına iten neden olmuştur[319]. Ancak tüm verilerin kağıda dökülmesi halinde milyonlarca sayfa tutabilecek metinler çıkabilecek ve adli makamlar bunları inceleyemeyecektir[320]. Bu açıdan CMK m.134'de bir düzenleme yapılması gerektiği öne sürülse de[321], adli bilişim alanında tarafsız bilirkişileri raporlarının bu sorunu çözebileceği kanısındayız.

Bu maddenin 2. fıkrasında ise bilişim sistemlerine şifrenin çözülememesinden ötürü girilememesi ya da gizlenmiş verilere erişilememesi veyahut işlemin uzun sürmesi hallerinde çözümlemenin gerçekleştirilebilmesi ve gereken kopyaların temini için, bunlaraelkonulabilir. Şifrenin çözümlenmesi ve gereken kopyaların elde edilmesi

---

[318]Değirmenci, Dijital Delil, s. 340.

[319]Değirmenci, Dijital Delil, s. 378.

[320] Kunter, Yenisey ve Nuhoğlu, s. 1100.

[321] Başlar, s.195.

durumunda ise, elkonulan aygıtlar gecikmeksizin iade edilecektir. Bu fıkradaki kopyalama faaliyeti de birebir kopyalamadır ve bu faaliyetin sonrasında da sistemin hash değeri alınmalıdır[322]. Kanun koyucu burada orantılılık ilkesinin bir sonucu olarak, bilişim sistemlerine elkoymak için şifrenin çözülememesi nedeniyle sisteme erişilememesi veya gizlenmiş bilgilere erişilememesi koşulunun mevcudiyetini aramıştır[323].

Öte yandan bazı bilişim sistemlerinin, kullanıcı şifresi ile sistem açılmadığı müddetçe, sabit diske ulaşmaya engel koyabilmektedir. Bu açıdan, kullanıcı adı ve şifresi bulunmadan sisteme ulaşılamaması, kopyalamanın yapılamaması ve kullanıcının şifreyi aramayı gerçekleştiren görevlilere verilmemesi halinde elkoyma işlemi yapılabilir[324]. Ayrıca bilgisayar programları kullanılarak gizlenmiş veya silinmiş bilgilere de olay yerinde erişilememesi halinde elkoyma işlemi yapılabilecektir.

Elkoyma işleminden sonra şifrenin çözülmesi ve kopyalamanın yapılmasından sonra gecikmeksizin el konulan cihazların iadesi gerekmektedir. Avrupa İnsan Hakları Mahkemesi Smirnov /Rusya kararında, başvuranın bilgisayarına altı günden fazla alıkonulmasının bir sebebinin bulunmadığı, bilgisayarın başvuranın mesleğini yerine getirmesi için bir araç olduğu ve elkoymanın başvuranın mesleki faaliyetlerine zarar verdiği,bu yüzden yargı organlarının toplumun genel menfaati ve avukatın hakları arasındaki adil dengeye müdahalede başarısız olduğu ve gerçekleştirilen işlemin hukuka aykırı olduğuna karar vermiştir.Uygulamada şüphelinin ev ve işyerinde yapılan aramada üçüncü kişilere ait bilişim sistemlerine el konulduğu ve kopyalama işlemlerinin de işlem sayısının fazlalılığın ötürü bir yıldan fazla sürdüğü, bilgisayar, cep telefonu veya diğer aygıtlara ihtiyaç duyan kişiler açısından bu durumun mağduriyete yol açtığı görülmektedir.

Doktrinde bazı görüşler, bilişim sistemlerine el konulması halinde bir suçun işlenmesinde araç olarak kullanılmaları sebebiyle, kovuşturma sonunda müsadere edilebilecek eşya

---

[322]Ünver ve Hakeri, 1. Cilt, s. 579

[323] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 365; Yavuz Erdoğan, Türk Hukuk Sisteminde Bilgisayar Araması ve Bulunan Delillere Elkonulması, Bilgi Sistemleri ve Bilişim Yönetimi (Edt. Fahrettin Özdemirci/Zeynep Akdoğan), Ankara 2017, s. 178.

[324]Değirmenci, Dijital Delil, s. 367-368.

vasfına sahip olduklarından CMK m. 127 gereğince elkonulabilmesi gerektiğini[325], başka bir görüş uyarınca de, burada müsadereye konu olabilecek mal varlığı değeri bulunduğundan CMK m. 123 gereğince elkoyma işleminin gerçekleştirilmesi gerektiği belirtilmektedir[326].Kanaatimizce suçta kullanılan veya içinde suç unsur bulunan cihazın kendisine yargılamanın sonuna kadar el konulması yönünde bir yasal değişiklik yapılması isabetli gözükmektedir. Ancak, bu durumda adil yargılanma hakkının bir parçası olan silahların eşitliği ilkesi uyarınca, bu elektronik aygıtın dijital bir kopyası mutlaka şüpheliye verilmelidir.

Bu konuda Avrupa Konseyi Siber Suç Sözleşme m.19/3-d'de suç unsuru ya da suç aracı olan verilerin erişilemez ve kullanılamaz hale getirilmesi ve kopyaları alındıktan sonra silinmesi hükmünün uygulanabileceği ileri sürülmüşse de[327], kanaatimizce yargılama aşamasında dijital delillere yönelik itirazlar ve tarafsız bir bilirkişi raporu alınması gerekebileceğinden Sözleşmenin bu maddesinin uygulanması sorunlu gözükmektedir.

Bilgisayar ya da bilgisayar sistemlerine elkoyma işlemi esnasında, sistemdeki tüm verilerin yedeklemesi yapılmak zorundadır (CMK m. 134/3). Çünkü, bunu yapılmaması durumunda bazı bilgilerin kaybolması ve zarar gelmesinin önlenmesi ile bu nedenle şüphelinin de, örneğin bilgisayarına ikinci kez el konularak mağdur edilmemesi için yedekleme yapılması zorunludur. Yasada da yedeklemenin yapılması zorunlu tutulmuştur. Bu tedbirin bir diğer önemli amacı da delil üretmenin engellenmeye çalışılmasıdır. Bu hüküm bilgisayar ve diğer delillerin dıştan müdahale edilmesinin engellenmesine yönelik bir hükümdür[328]. Son olarak bu fıkradaki "el koyma işlemi sırasında" ibaresinin inceleme yapılmaya başlamadan önce şeklinde anlaşılması gerekmektedir. Ayrıca bu fıkrada, bilgisayar programlarından bahsedilmemişse de bu programlar genelde bilgisayarın sabit diskinde olduklarından

---

[325] Özcan Özbey, Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK'nın 134. Maddesi), Yargıtay Dergisi, Cilt. 36, Sayı. 3, (Temmuz 2010), s. 121.

[326]Değirmenci, Dijital Delil, s. 377.

[327] Başlar, s.190.

[328] Avni Güçlü Sevimli, "Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar", İstanbul Barosu Dergisi, Cilt. 81, Sayı. 3, (Mayıs-Haziran 2007), s. 997; Çolak ve Taşkın, s. 609

yedekleme kavramının bilgisayar programını da kapsadığı anlaşılmaktadır[329].Bilgisayar dışındaki veri saklama birimlerine ilişkin aşağıda ayrıntılı açıklama yapılacaktır.

Yapılan yedekleme işleminden sonra bir kopya daha çıkarılarak şüpheli ya da vekiline verilmeli ve bu durum tutanağa yazılarak imzalanmalıdır (CMK m. 134/4).Bu uygulamanın nedeni, dijital delile dair hukuka aykırılık iddialarının önüne geçmektir. Bu nedenle, Kanunda bu uygulama, işlemi yapan kolluk görevlilerinin isteğine bırakılmamıştır. Ancak, uygulamada bu kopyanın bir yıldan fazla sürede verilmesi bu şüphelerin artmasına neden olmaktadır.

İçinde suç unsuru olan elektronik aygıt veya bilgisayarın bir kopyasının da şüpheliye verilip verilmeyeceğinin Kanunda belirtilmediği ve bu konuda düzenleme yapılması gerektiği ileri sürülmüşse de[330], CMK m.153/2 uyarınca gizlilik kararı alınan soruşturmalar hariç, herhalde kopyanın bir örneğinin şüpheliye verilmesi gerektiği kanısındayız.

Bilgisayar ya da bilgisayar sistemlerine elkonulmadan, sistemdeki verilerin tümünün ya da bir bölümünün kopyasının elde edilmesi olanaklıdır (CMK m.134/5). Bu maddede düzenlenen kopyalama işleminden anlaşılması gereken birebir kopyalamadır ve düzenlenecek tutanağın ilgililer tarafında imzalanması gerekir (CMK m.134/5).

2.2.5.3.4. Arama ve Elkoymaya İlişkin Genel Hükümlerin Geçerlilik Durumu

Bilgisayarlar ve bilgisayar sistemlerinde arama, kopyalama ve elkoyma tedbirinin uygulanması sırasında öncelikle CMK m.134 hükmü uygulanacak olup, bu tedbir aykırı olamayan CMK'daki arama ve koymaya ilişkin genel hükümlerin geçerliliği devam edecektir. Bu kapsamda, arama kararında olması gereken bilgi ve unsurlar, arama ve elkoymanın tutanağının düzenlenme şekli, aramayı gerçekleştiren kolluk görevlilerinin ve varsa Cumhuriyet savcısının isimlerinin tutanağa yazılması, CMK m.119/4, 120 veya 130 gereğince arama esnasında hazır olması gerekli olan şahıslar, arama neticesinde verilecek

[329] Ünal, s.119.

[330] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt. 4, Sayı. 2, 2013, s. 152; Başlar, s.193.

belge, elkonulmayacak belgelere dair düzenlemeler bu tedbire aykırı olmadığı müddetçe geçerli olacaktır[331].

Arama sırasında, bilişim sisteminin sahibi ya da zilyedi olan şahıs aramaya katılabilir (CMK m.120/1). Şüphelinin avukatının aramaya katılmasına da engel olunamaz (CMK m. 120/3). Arama sonunda elkonulan eşya ve kopya alınması işlemine ilişkin tutanak düzenlenecektir. Hakkında CMK m.134'deki tedbir uygulanan kişiye CMK m. 121/1'de yer alan genel düzenlemeler gereğince bu durumu ve aramanın konusunu oluşturan eylemin niteliğini gösteren bir belge düzenlenerek ilgili kişiye verilir. Ancak burada CMK m.134 kapsamında ilgili kişi veya vekilinin talebi olmaksızın kolluk güçlerince hazırlanan tutanağın bir örneği verilecektir[332].

Yine CMK m.122/1 gereğince arama işlemi uygulamasına maruz kalan kişinin belge ya da kâğıtlarını inceleme yetkisi, Cumhuriyet savcısına ve hâkimindir. Bu açıdan, bu genel düzenleme gereğince CMK m. 134 kapsamında icra edilen tedbiri tatbik eden kolluk, bilişim sistemlerinde yer alan belge ve verileri kâğıda yazdırmışlarsa, bu belgeler üstünde inceleme yapmaksızın bunları Cumhuriyet savcısına teslim etmelidirler.

Kamu kurumlarına bilgisayar veya bilgisayar kütüklerinde yapılan aramalar esnasında, devlet sırrı vasfında bilgi ve belgelere rastlanması halinde, söz konusu belgeler üstündeki inceleme CMK m. 125/2 gereğince hâkim ya da mahkeme başkanınca yapılmalıdır. Bu madde uyarınca devlet sırrı vasfında bilgi içeren belgelerde Cumhuriyet savcısınca bile incelenemeyeceğinden ötürü, bu belgelerin delil şeklinde kabul edilmesi de Cumhuriyet savcısınca gerçekleştirilemeyecektir[333].

Öte yandan devlet sırrı özelliğine sahip belgelerin yalnızca incelenmesinden söz edilmesi sebebiyle bu özellikteki belgeler alınamayacak, örneği çıkarılamayacak, fotokopisi ve filmi çekilemeyecektir. Bu belgelerde bulunan ve yalnızca şüpheli veya sanığa atılı suçu açığa kavuşturacak olan bilgiler hâkim ya da mahkeme başkanınca tutanağa kaydedilebilir. Bu çerçevede, dijital delilin de belge delili olduğu göz önüne alındığında devlet sırrı içeren bir bilişim sistemi üstünde yapılacak inceleme esnasında CMKm.125'deki düzenlemelerin göz

[331]Başlar, s.196; Çolak ve Taşkın, s. 609.

[332]Başlar, s.197.

[333]Değirmenci, Dijital Delil, s. 398.

önüne alınması, incelemenin hâkimce gerçekleştirilmesi ve bu sistemler üstünde kopyalama işleminin yapılamaması gerekmektedir. Ancak buradaki başka bir sorun devlet sırrının Türk mevzuatında tanımlanmamış olmasıdır[334].

CMK m. 126 gereğince şüpheli ve sanık ile tanıklıktan çekinme hakkı bulunan kişiler arasında gönderilmiş mektuplara ve belgelere, bu kişilerin uhdesinde olduğu müddetçe elkonulamaz. Bu çerçevede, şüphelinin kullandığı, ancak soruşturma çerçevesinde tanıklıktan çekinme hakkı bulunan bir kişiye ait bilişim sisteminde arama gerçekleştirilmesi halinde, bilişim sisteminde olan şüpheli ve tanıklıktan çekinme hakkı bulunan kişi arasındaki mektup ve belge vasfındaki verilere elkonulamaz. Bu tedbir çerçevesinde gerçekleştirilen kopyalama işlemi de, bir tür elkoyma vasfına sahip olduğundan bu özellikteki verilere ilişkin hakkında kopyalama yapılamayacaktır[335].

Bununla birlikte, CMK m.134 kapsamındaki tedbirlerin uygulanması aleyhine başvurulacak kanun yoluna ilişkin maddede bir düzenleme bulunmamaktadır. Bu durumda sorun da genel hükümler kapsamında çözüme kavuşturulmalıdır. İtiraz kanun yolunun düzenlendiği CMK m. 267 gereğince, CMK m.134 kapsamında hâkimin tedbir veya onaylama kararı üzerine şüpheli ya da müdafii bu karara itiraz edebileceklerdir. Öte yandan CMK m. 35/2 gereğince bu tedbirin uygulanması esnasında hazır olmayan ilgili kişilere karar tebliğ olunmayacağından şüpheli ve müdafii, bu tedbir kararını öğrenme tarihten başlayarak itiraz edebilirler[336].

Şüphelinin CMK m.134 kapsamındaki bilişim sistemlerinde gerçekleştirilen aramanın ölçüsüz şekilde icra edilmesi halinde istenebilecek tazminat talepleri de genel hükümler uyarınca tespit edilecektir. Bu tedbirin kişilerin özel hayatına saygı hakkına doğrudan

---

[334] 2012 yılında gündeme gelen mevzuat çalışmalarında Devlet Sırrı Kanun Tasarısı hazırlanmış olup, bu tasarı yasalaşmamıştır. Bu Tasarının 3. Maddesine göre "devlet sırrı; açıklanması veya öğrenilmesi, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek ve bu nedenlerle niteliği itibarıyla gizli kalması gereken bilgi ve belgelerdir". Yine Tasarının 6. maddesine göre hangi belge ve bilgilerin devlet sırrı olduğuna, oluşturulacak Devlet Sırrı Kurulu karar verecektir.www.memurlar.net/common/news/documents/108331/101-1218.doc+&cd=4&hl=tr&ct=clnk&gl=tr, erişim tarihi: 23.3.2022; Yine 2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu'nda (m.6/2, Ek Madde 2) devlet sırrı tanımlanmamıştır, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf, erişim tarihi: 23.3.2022

[335]Özbek Veli Özer / KanburMehmet Nihat / Doğan Koray / Bacaksız Pınar / Tepe İlker, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, 7. Baskı, Ankara, Ekim 2015, s.430.

[336] Özbek/Kanbur/Doğan/Bacaksız/Tepe, s.438 .

müdahale etme özelliği dikkate alındığında, önlemin ölçüsüz şekilde tatbik edilmesi halinde şüpheli ya da müdafii CMK m. 141/1-i gereğince tazminat isteminde bulunabilir[337].

Bilişim sistemlerine gerçekleştirilecek arama sonucunda ele geçirilen verilerin genel hükümler gereğince müsadere edilip edilmeyeceği de bir sorundur. Bir eşyanın müsaderesi için, bu eşyanın maddi bir varlığa sahip olması gerekir. Bu sistemlerden ele geçirilecek veriler ise maddi olmayan mal niteliğine sahiptir. İyiniyetli üçüncü şahıslara ait olmaması şartıyla, kasıtlı bir suç işlenirken kullanılan veya suçun işlenmesine tahsis edilen eşyanın müsadere edilebileceği TCK m. 54'te düzenlenmiştir bu çerçevede TCK m.54'te yer aslan şartların bulunması durumunda elektronik aygıtlarda bulunan veriler, içinde bulundukları aygıtla beraber müsadere edilebilecektir[338].

CMK m. 134 gereğince bilişim sistemlerinde gerçekleştirilecek tedbir işlemlerinde uygulamaya ilişkin olarak kişi açısından istisnai bir hüküm getirilmemiştir. Bu sebeple CMK m. 134 hükmünün, avukatların bürolarında arama ve el koymaya dair CMK m. 130 hükmü ile birlikte uygulanabilmesi olanaklıdır[339]. Ancak, CMK m.130 hükmü gereğince avukat bürolarında bilişim sistemlerine arama ve elkoyma tedbiri sadece hâkim kararı ile Cumhuriyet savcısının kontrolünde ve baro başkanı ya da onu temsilen bir avukat huzurunda yapılabilir.

AİHM Kırdök ve Diğerleri/ Türkiye[340] kararında avukatların elektronik verilerine ve taşınabilir belleklerine el konulmasına ilişkin önemli bir karar vermiştir. Başvurular avukat olup, aynı büroda çalıştıkları başka bir avukat aleyhine yapılan soruşturma sırasında adli makamlarca elektronik verilerine elkoyulmasını şikayet etmişlerdir. Mahkeme, başvurucuların bilhassa, avukat ve müvekkil gizliliği kapsamında korunan elektronik verilerine elkonulması ve bunların geri verilmesi veya yok edilmesi taleplerinin reddedilmesinin sosyal bir ihtiyaç baskısına karşılık gelmediğine ve demokratik bir

---

[337] Yaşar/Dursun, s.30; Tanrıkulu, s.412.

[338] Başlar, s.198.

[339] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 364

[340]Kırdök ve Diğerleri v. Türkiye, Başvuru No. 14704/12, Karar tarihi: 03.12.2019, karar metni için bkz. https://anayasagundemi.com/2019/12/05/ihamin-kirdok-ve-digerleri-v-turkiye-kararinin-ozet-cevirisi-ofis-baskininda-avukatlarin-mesleki-gizlilik-uyarinca-korunan-elektronik-verilerine-usuli-guvenceler-olmadan-el-konulmasi-ozel-hayata/, erişim tarihi: 23.3.2022.

toplumda gerekli bulunmadığına kara vermiştir. AİHM, yargı organların yorumladığı ve tatbik ettiği haliyle yeterli usuli teminatların bulunmadığını belirleyerek özel ve aile yaşamını, konut dokunulmazlığı ve haberleşmenin gizliliğine saygı hakkına ilişkin AİHS m.8'in ihlal edildiğine karar vermiştir[341].

2.2.5.3.5. Tesadüfen Elde Edilen Deliller

Bilişim sistemlerinde arama yapılması esnasında, yürütülen soruşturma ya da kovuşturma ile ilgisi bulunmayan, fakat başka bir suçun işlendiği şüphesini uyandıran bir delilin ele geçirilmesi durumunda CMK m. 138/1 gereğince, bu delil muhafaza altına alınır ve bu durum hemen savcıya bildirilir.

Öte yandan, soruşturmaya konu suç bahanesi ile tesadüfen elde edilen delillere ilişkin delil araştırmasına başlamak, bu maddede yer alan "bir suç soruşturmasının varlığı" koşuluna aykırı olabilecektir. Bu açıdan, tesadüfen elde delile ilişkin olarak aramayı genişletmeden hemen Cumhuriyet savcısına bilgi verilmelidir. Bu sınırın uygulanamaması durumunda, tedbirin, var olan suç soruşturmasının dışına çıkması ve hukuka aykırılıklara yol açması olasıdır[342]. Örneğin bir bilişim suçuna ilişkin yapılan arama esnasında çocuk pornografisine dair fotoğraf veya videoların ele geçirilmesi halinde, aramada müstehcenlik suçunun (TCK m. 226/3) delillerine yönelik bir araştırma yapılmaması, tesadüfi olarak ele geçirilen bu delilin muhafaza altına alınarak hemen savcıya bildirilmesi ve başlatılacak yeni soruşturmaya istinaden yeni aranma kararı bu suç delilinin elde edilmesi daha doğru olacaktır.

2.2.5.3.6. CMK m.134'deki Tedbirin Temel Hak ve Özgürlüklere Etkisi

Koruma tedbirleri uygulandığı takdirde genelde temel hak ve hürriyetlere müdahale edilmektedir. CMK m. 134 gereğince bilişim sistemlerinde tedbirler uygulanırken de birtakım temel hak ve özgürlüklere müdahale yapılacağı açıktır. Bu koruma tedbiri, özel hayat saygı, haberleşmenin gizliliğinin korunması ve düşünceyi açıklama hürriyetinin korunması açılarından ayrı ayrı değerlendirilmelidir.

---

[341] Benzer karar için bkz. Wieser ve BiocosBeteligungenGmBH/Avusturya, 16.10.2007, Serkan Cengiz (çev.), İnsan Hakları Avrupa Mahkemesi Kararları, Türkiye Barolar Birliği Dergisi, Sayı. 82, (Mayıs 2009), s. 461-462.

[342] Başlar, s.200.

2.2.5.3.6.1. Özel Hayatın Gizliliğinin Korunması

Özel hayatın gizliliği ve korunması, bir kimsenin, maddi ve manevi kişiliğini geliştirmek, sahip olduğu değerleri teminat altına almak için başkalarınca bilinmemesini istediği özelliklerin meydana getirdiği ve korunması hukuken gerekli görülen alan üstündeki hakkı olarak tanımlanabilir[343]. Bireyin yaşamının gizli alanı, yalnızca bireyi ilgilendiren ve onun haricinde başka kimsenin bilemeyeceği bölümü olarak tarif edilebilir ve bu bölüm mutlak anlamda korunmaktadır.

Özel hayatın gizliliği hakkı AİHS m.8'dekorunmakta olup, bu maddeye göre, bu hak, AİHS'de yer alan durumlarda ve oranlılık ilkesine uyularak sadece kanunla sınırlandırılabilir. Özel hayatın gizliliği hakkı, Türk Anayasası m.20,21 ve 22'de kişinin aile hayatı, konut dokunulmazlığı ve haberleşme özgürlüğü ile beraber korunmaktadır. 2010 Anayasa değişikliği ile kişisel verilerin korunması hakkı da özel hayatın gizliliği çerçevesinde korumaya alınmıştır.

Özel hayatın gizliliğine nasıl müdahale yapılabileceği ve bu müdahalenin hukuka uygun biçimde hangi şartlarda yapılabileceği Anayasa'nın 20/2 maddesinde[344] yer almıştır. Bu çerçevede bireylerin özel kişisel bilgi ve belgelerinin yer aldığı bilişim sistemlerine hukuka uygun şekilde erişebilmek ve delil elde edebilmek için maddedeki istisnalara bağlı olarak hâkim ve savcı kararı, Anayasa m.20/2'deki hükme ve yürürlükteki düzenlemelere uygun mevcut düzenlemelere uygun hareket etmekle olacaktır[345].

Bilişim sistemlerindeki bilgiler, kişisel veri ya da ticari sır veyahut meslek sırrı özelliğini taşıyan bilgiler de olabilir. Hem temel hak ve hürriyetlerin korunması, hem de kamusal yarar olan maddi gerçeğin ortaya çıkarılması dikkate bilişim sistemlerinde arama,

---

[343] Ersan Şen ve Yasemin Yurttaş, "Bilgisayar Programları Karşısında Özel Hayatın Korunması", Terazi Hukuk Dergisi, Cilt. 5, Sayı. 42, Şubat 2010, s. 29.

[344] Anayasa m.20/2: "*Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar*".

[345] Şen ve Yurttaş, s. 30.

kopyalama ve elkoyma CMK'da özel hükümle öngörülmüştür[346]. CMK m.134 gerekçesinde de yasa koyucu bu hükmün temel hak ve özgürlüklere etki etmesi nedeniyle kanunla düzenlendiğini belirtmektedir[347].

Bireyler, çevrimiçi veya elektronik ortama katılmalarıyla beraber birtakım kişisel verilerini de farklı yerlerde kaydedilmekte ve kullanıma açılmaktadır. Modern dünyada veri toplama kapasitesine sahip elektronikler sistem, kullanıcıya dair bilgileri kaydedebilmektedir. Kişinin rızası olmaksızın, kişinin kimliği, sosyal, etnik, dini, siyasi, psikolojik, ekonomik ve diğer niteliklerinin belirlenmesi için kaydedilmesi, işlenmesi ve aktarımı halinde kişisel verilerin korunması hakkı ihlal edilmiş olacaktır. Elektronik ortamda kişisel verilerin güvenlik gerekçesiyle kaydedildiği açıklansa da uygulamada genellikle gereksinim duyulandan fazla kişisel veriye erişim ve kaydetme yönelimi bulunmaktadır[348].

Elektronik aygıtlarla kişisel verilerin toplanması, kaydedilmesi, aktarılması kolaylaştığından bu verilerin korunması, bireylerin özel hayatlarının gizliliğinin korunması açısından önem arz eder hale gelmiştir. Ayrıca bilgisayarlar, bireylerin hem iş hem de özel hayatlarına ilişkin pek çok kişisel veriyi tutmaları sebebiyle CMK m.134'deki tedbirin uygulanması neticesinde pekçok kişisel veriye ulaşılmakta ve kişilerin mahremiyet arz eden kişisel verileri de açığa çıkmaktadır[349].

Özel hayatın gizliliğinin korunması açısından, tedbirin uygulanmasının CMK m.134'de somut delillere dayalı kuvvetli şüphe nedenlerinin bulunması koşuluna bağlanması önemlidir. Bunun yanında, bu tedbirinde iletişimin denetlenmesi tedbirinde olduğu gibi kişilik hakları ihlal etmesi olası olduğundan göz önüne alındığında, kesinleşmiş kovuşturmaya yer olmadığına dair kararlarında ele geçirilen verilerin soruşturma dosyasından çıkartılarak yok edilmesi hususunda herhangi bir hükmün (CMK m.137)

---

[346] Şahin, Ceza Muhakemesi Hukuku I, s. 267.

[347]Değirmenci, Dijital Delil, s. 315.

[348] Habip Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, Cilt. 1, Sayı. 3, Haziran 2014, s. 4-5; Değirmenci, Dijital Delil, s. 107.

[349] Güray Dağ, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", Yayınlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2011, s s.235,238.

bulunmaması bir eksikliktir. CMK m.137'ye, CMK m.134 açısından bu hükmün uygulanacağı düzenlemesi getirilmesi yerinde olacaktır.

CMK m.134 hükmünün farklı surette delil ele geçirme olanağının olmaması durumunda uygulanması yani istisnai hallerde uygulanması veya bu tedbirin herkesin değil sadece şüphelinin kullandığı bilgisayarlarda uygulanması yani ölçülülük ilkesiyle uyumlu şekilde uygulanması, bu tedbirin AİHS m.8 ve Anayasa m.20/2'ye uygun şekilde uygulandığını göstermektedir[350].

2.2.5.3.6.2. Haberleşmenin Gizliliğinin Korunması

Haberleşmenin gizliliği hakkı, bireylerin kişilerin diğer bireylerle hangi vasıta veya yolla yapılırsa yapılsın özel niteliğe sahiphaberleşmelerinden kişiler ya da devlet makamlarının haberdar olması endişesi olmaksızın gerçekleştirme hakkı anlamına gelmektedir. Bu kapsamda üçüncü kişiler ya da devletin organlarının, bireylerin mektup, elektronik posta, faks veya telefonlagerçekleştirdiği iletişimi; okumaması, dinlememesi ve içeriğine erişememesi gerekir[351].

AİHS m. 8'de haberleşmenin gizliliğinin korunması hakkı,teminat altına alınmıştır. Bu madde uyarınca, haberleşmenin gizliliği hakkı da AİHS'de öngörülen durumlarda, ölçülülük ilkesine uygun olmak şartıyla sadece yasayla sınırlandırılabilir.AİHM de, AİHS m.8'de yer alan "corresponce" kelimesinin; bireyler arasında, her türlü araç ve yolla yapılan özel nitelikteki haberleşme anlamına geldiğini ifade etmektedir[352].

Herkesin haberleşme özgürlüğünün olduğu ve haberleşmenin gizliliğinin kural olduğu Anayasa'nın 22. maddesinde düzenlenmiştir. Bu maddenin ikinci fıkrasında ise haberleşmenin gizliliğine nasıl, hangi zaman ve hangi şekilde müdahale edilebileceği ve bu müdahalenin koşulları Anayasa'nın 22/2 maddesinde yer almıştır.

Kişilerin haberleşmeleri bazen durağan şekilde elektronik aygıtlarda bulunabileceği gibi, elektronik posta gibi yollarla yapılan haberleşmelerde akış halindeki veriler de delil

---

[350] Başlar, s.206.

[351] Ömer Anayurt, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, Ankara: Seçkin Yayıncılık, 2004, s. 116-117.

[352]Klass ve öte./ Almanya, 6.9.1978, A 28, para. 10 ve 11, ayrıca bkz. A. Şeref Gözübüyük ve Feyyaz Gölcüklü. Avrupa İnsan Hakları Sözleşmesi ve Uygulaması Avrupa İnsan Hakları Mahkemesi İnceleme ve Yargılama Yöntemi. 9. Basım. Ankara: Turhan Kitabevi, 2011, s. 341.

olabilmektedirler[353]. Elektronik postalardaki gibi transfer halindeki verilerin ele geçirilmesi de, bireylerin haberleşme özgürlüğüne ve dolayısıyla haberleşmenin gizliliğine müdahale oluşturur[354].

Haberleşmenin gizliliği hakkına Anayasanın 22/2. maddesindeki meşru nedenlere bağlı olarak, kanuni bir temele istinaden, kişilere teminatlar getirmek ve ölçülülük ilkesine bağlı kalmak şartıyla haberleşmenin gizliliğine devletçe müdahale yapılması mümkündür[355]. Bu çerçevede CMK m.134'de yer alan tedbire ilişkin düzenleme incelendiğinde, AİHS m.8 ve Anayasa m.22/2'de belirtildiği üzere bu tedbir istisnai olarak ve ölçülülük ilkesine uygun şekilde düzenlenmiştir[356].

2.2.5.3.6.3. Düşünceyi Açıklama ve Yayma Özgürlüğünün Korunması

AİHS'in 10. maddesine göre düşünceyi açıklama ve yayma özgürlüğü, Sözleşmede yer alan durumlarda sadece kanunla bazı usuller, şartlar, sınırlamalar ya da müeyyidelere bağlanabilir. AİHM de bu özgürlüğün demokratik toplumun köşe taşlarından biri olduğunu vurgulamakta, toplumların ilerlemesi ve bireylerin gelişmesi için bu hakkın olmazsa olmaz olduğunu belirtmektedir[357]. AİHM, demokrasinin, düşünceyi açıklama özgürlüğü ile beslendiği, çoğulculuğun bulunmadığı yerde de demokrasiden bahsedilemeyeceğini ifade etmektedir. Mahkeme, bu özgürlüğün yalnızca zararsız veya önemsiz haber ve görüşler için değil, şok edici, rahatsız edici ve aykırı görüşler bakımından da geçerli olduğunu belirtmektedir[358].

Anayasa m.26/1'de[359] düşünceyi açıklama ve yayma özgürlüğü düzenlenmiştir (m.26/1). Bu özgürlüğüne nasıl ve ne zaman müdahale yapılabileceği de m.26/2'de yer almıştır[360].

---

[353]Değirmenci, Dijital Delil, s. 99.

[354] Zafer Gören, "Düşünceyi Açıklama Özgürlüğü", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Sayı. 24, (Güz 2013/2), s. 49; Değirmenci, Dijital Delil, s. 99.

[355] Anayurt, s. 117.

[356] Başlar, s.208.

[357] Gözübüyük ve Gölcüklü, s. 358.

[358] Gözübüyük ve Gölcüklü, s. 358; Anayurt, s. 121-122.

[359] Anaysa m.26/1: " *Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar*".

Bilgisayar ve benzeri elektronik aygıtlarla insanlar internet üstünden düşüncelerini açıklayabilir, yayabilir ve başka kişilerin de düşünce ve görüşlerine ulaşabilir. CMK m. 134'de yer alan tedbirin tatbik edilmesi, bilişim sistemleri vasıtasıyla düşünce açıklama ve yayma hakkıyla doğrudan ilişkilidir. Öte yandan, bireylerin düşünce açıklama ve yaymaları, iletişim vasıtalarıyla hayata geçecek haklardandır. Akış halindeki verilerin de elde edilmesi bireylerin açıklama ve yayma haklarına müdahale oluşturacaktır[361]. Bu çerçevede, CMK m.134'de düzenlenen tedbire ilişkin düzenleme incelendiğinde, AİHS m.10/2 ve Anayasa m.26/2'da yer aldığı üzere bu tedbir, istisnai olarak ve ölçülülük ilkesine uygun şekilde düzenlendiği söylenebilir[362].

2.2.5.4. Türk Hukukunda Düzenlenmeyen Dijital Delil Elde Etme Halleri

2.2.5.4.1. Uzaktan Erişimle Arama

Teknolojideki hızlı ilerlemeler sonucunda, internet erişimi bulunan bilişim sistemlerinin dışarıdan müdahale veya saldırıya maruz kalmaları gündeme gelmektedir. İnternet bağlantısı olan bir bilişim sistemine, kullanıcı kişilerin bilgisi dışında erişim sağlanmakta ve bu bilişim sistemindeki verilere ulaşmak mümkün olmaktadır. Öte yandan bilişim sistemlerine uzaktan erişim sağlanma yoluyla arama işlemi gerçekleştirilip gerçekleştirilmeyeceği konusu karşılaştırmalı hukukta ve iç hukukumuzda tartışma konusu olmuştur.

Ülkemizin de taraf olduğu Avrupa Konseyi Sanal Ortamda İşlenen Suçlar (Siber Suç) Sözleşmesi'nin[363] 32. maddesine göre sözleşmenin bir tarafı, diğer tarafın ülkesinde, bilgisayarda tutulan verilere, bahse konu bilgisayar sistemi üstünden erişim yetkisine sahip olan şahsın hukuki olarak izin verdiği hallerde ya da bu verilerin herhangi bir kimsenin erişebileceği biçimde açık olduğu hallerde sınır ötesinden erişim sağlayabileceği ve bunları temin edebileceği ifade edilmiştir[364].

---

[360] Gören, s. 38.

[361] Değirmenci, Dijital Delil, s.102.

[362] Başlar, s.208.

[363] 22.4.2014 tarih ve 6533 sayılı Kanun, 09.08.2014 tarih ve 29083 sayılı Resmi Gazetede yayımlanmıştır, https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm, erişim tarihi: 26.03.2022.

[364] Bu hüküm doktrinde eleştirilmekte olup, bireyin rızasıyla, devletlerin egemenliği ilkesine aykırı olarak, başka bir devletin ülkesinde yargı yetkisi kullanılmakta olduğu belirtilmektedir. Bkz. Önok, Murat, Avrupa

Türkiye bu Sözleşmenin tarafı olduğundan, Türk yargı organları taraf başka bir ülkedeki halka açık verilere ya da bilgisayar sistemine erişim yetkisine sahip kişinin izni ile uzaktan erişimle arama yapılabilecektir. Yine doktrinde CMKm.134'de yer alan "arama" kavramının "elektronik veri takibi"ni de içerdiği, elektronik veri takibinin ise bilişim sisteminin kolluk güçlerinin hâkimiyet alanına alınması yoluyla açık şekilde gerçekleştirilebileceği gibi bilgisayar sistemine uzaktan erişilerek, yazılım üstünden ve gizli şekilde de yapılabileceği öne sürülmüştür[365].

Karşıt görüşe göre; CMK m. 134 gereğince bilişim sistemine bu sistemde gözükmeyecek şekilde bir (kötü niyetli) yazılım yükleyerek arama yapılması, sistemdeki verilerin bir yere nakli ve sistemdeki hareketlerin gözlenmesine olanak yoktur[366]. Çünkü CMK m. 134 depolanmış bilişim sistemlerindeki verilerde arama yapmayı düzenleyen, arama sırasında ilgili şahsın haberinin olması gereken, yasada öngörülen yöntem ve esaslar çerçevesinde arama yapılmasını gerektiren bir koruma tedbiridir. Bilişim sistemi kullanıcısının haberi olmaksızın, uzaktan arama yapmak için kullanılan kötü niyetli yazılımlarla bilişim sisteminde arama gerçekleştirilmesi olanaklı değildir. Zira kötü niyetli yazılımlar kullanarak veri veya delil elde etme bir arama işlemi şeklinde de tanımlanamaz.

Kanaatimizce de, yukarıdaki gerekçelerle bilişim sistemi kullanıcısının haberi olmaksızın, uzaktan arama yapılması için ilgili yüklenen kötü niyetli yazılımlarla arama yapılması olanaklı değildir. Kaldı ki, Türkiye içinde soruşturmanın başka bir ildeki bilişim sistemleri ile ilişkisinin olması halinde, arama ve elkoyma işleminin yapılması, o yer Cumhuriyet savcılığına veya mahkemesine talimat yazılması ile mümkündür.

Türkiye sınırları dışındaki bilişim sistemlerinden uzaktan erişim ile arama yapılmasının mümkün olup olmadığı sorunu karşımıza çıkmaktadır. Türkiye, Avrupa Konseyi Sanal Ortamda İşlenen Suçlar (Siber Suç) Sözleşmesi'ne taraftır ve Sözleşmenin 32. maddesine hiçbir devlet tarafından çekince konulamayacaktır (m.42). Ayrıca, Türk Anayasası m.90 uyarınca. usulüne uygun biçimde yürürlüğe konulan sözleşmeler ve anlaşmalar kanun

---

Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof. Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt.19, Sayı:2, 2013, s.1258.

[365]Vahit Bıçak,Suç Muhakemesi Hukuku, 2. Basım. Ankara: Seçkin Yayıncılık, 2013, s.671-673.

[366] Değirmenci, Dijital Delil, s.364-365.

hükmünde olduğuna göre, uygulayıcıların önünde, uzaktan erişime izin veren kanuni bir düzenleme bulunmaktadır. Ancak, anılan Sözleşmeye ilişkin bir uygulama kanunu bulunmadığından,ülke sınırları dışında uzaktan arama yapmak amacıyla yasal bir düzenleme bulunmamaktadır. Kanaatimizce ülke sınırları dışında uzaktan erişim ile bilişim sistemindeki bilgilerin bu sistemin kullanıcısının rızası ile alınması ve bu işlem yapılırken daha güvenceli bir delil toplama sistemi getiren CMK m.134'ün uygulanması gerekir. İlgili şahıs izin vermediği takdirde Sözleşmenin 23. maddesi uyarınca taraf ülkeden adli yardım talebi ile bu bilgiler istenebilecek ve bu durumda talep edilen ülke hukuku uygulanacaktır.

Burada oluşabilecek sorun, sistemdeki bilgiler alındığında bunun kopyasınınilgili kişiye ne şekilde verileceğidir. Günümüzde bulut teknolojisi veya internet üzerinden gigabaytlar tutan verilerin transferi mümkün olduğundan[367], bu kopya bu yolla ilgili kişiye gönderilebilir. Ayrıca gerek Sözleşmenin 32. maddesi gerekse Sözleşmenin Açıklayıcı Raporunda[368] bu durumda hangi ülke hukukunun uygulanacağı belirtilmemiştir. Kanaatimizce bu talep, ülkeler arasında geleneksel bir adli yardım talebi olmadığından, soruşturma veya kovuşturmayı yürüten ülkenin hukuku uygulanmalıdır. Türkiye'nin Sözleşme'nin 32. maddesi kapsamında talebi olması halinde Türk hukuku uygulanacaktır.

Tüm bu açıklamalarla birlikte, uzaktan erişim yoluyla veri elde etme debireylerin temel hak ve hürriyetlere ağır müdahale teşkil ettiğinden, bu özelliği taşıyan bir arama usulü açısından yeni bir kanuni düzenleme yürürlüğe konulması zorunludur[369]. Zira, uzaktan arama yoluyla ele geçirilebilecek verilerin, otomatik sistemler kullanılarak, suçla ilgisi olmayanlarının ve özel hayatın gizliliğine girenlerin ayırt edilmesi ve bu verilerin açığa çıkmasının engellenmesi gerekmektedir[370].

---

[367]Wetransfer, Dropbox, Google Drive, Share it gibi siteler çok büyük miktarda veri transferine izin vermektedir, https://www.webtekno.com/wetransfer-dosya-transfer-android-ios-indir-h83301.html, erişim tarihi: 26.03.2022

[368]Avrupa Konseyi Sanal Ortamda İşlenen Suçlar (Siber Suç) Sözleşmesi Açıklayıcı Raporu için bkz. https://rm.coe.int/16800cce5b, https://www.webtekno.com/wetransfer-dosya-transfer-android-ios-indir-h83301.html, erişim tarihi: 26.03.2022.

[369] Ünal, s.111.

[370]Değirmenci, Dijital Delil, s.366.

2.2.5.4.2. Bulut Bilişimde Arama

Bulut bilişim kavramına ilişkin olarak uzlaşıya varılmış bir tanım bulunmamaktadır. Doktrinde bir tanım göre bulut bilişim, bilişim sistemlerinin aralarında bilgi transferine olanak veren hizmetlerin genel adıdır[371]. Başka bir tanıma göre bulut bilişim, veri merkezlerinde birden çok sunucunun birlikte kullanıldığı, sanal hale getirilmiş bir platform üstünde yazılım ve donanım hizmetlerinin kullandırılmasıdır[372].

Verilerin saklanması ve depolanmasında bulut bilişimin kullanılması,devam eden bir soruşturmada delil niteliğinesahip dijital verilerin elde edilmesi açısından önemlidir. Öte yandan, bulut hizmetleri; farklı şekillerde sunulduğundan[373], bu hizmetleri sunan şirketlerin, yani üçüncü kişilerin denetiminde ve sorumluluğunda olan verilerin ne şekilde ele geçirileceği ve bunların delil değerinin ne olacağı yürürlükteki hukuki düzenlemeler karşısında tartışma konusudur[374].

Bulut ortamında delil araştırması yapılırken soruşturma makamları bazı engellerle karşılaşabilmektedir. Bulut hizmetleri, yasa dışı bilgi ve belgeleri, depolamak, korsan saldırıları yapmak için kullanılabilmektedir. Veri sunucusu ülke içinde bir kuruluş olsa bile, verilerin denizaşırı ülkelerde yani soruşturma makamının yargı yetkisi dışında bir yerde depolanması da sıklıklakarşılaşılan bir durumdur. Verilerin bulunduğu yer, soruşturması esnasında uygulanacak hukuku ve yargı yetkisinin tespiti bakımından son derece önemlidir. En önemli zorluklardan biri ise, bulut sistemlerinin hizmetinden faydalanan çok sayıda kullanıcının verilerinin tek bir yerde tutulması ve arama yapılırken soruşturmasıyla ilişkisi olmayan kişilerin verilerine ulaşılarak onların özel hayatlarının gizliliğini doğrudan

---

[371]Özge Dereboylular, Bulut Bilişim Bakımından Arama Ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği, CHD - Nisan 2019, S.: 39, ss. 161-202, s.164; Topaloğlu, Murat/Özkişi, Harun/Tekkanat, Egemen, Bulut Bilişim, Seçkin Yayınevi, Ankara 2017, s. 19. Öğretide farklı tanımlar için bkz. Martin Kratz, "PrivacyandCloud Computing", LawNow, Volume 37, (2013), 35-40; Metin Turan, Bilişim Hukuku, Seçkin Yayıncılık Ankara 2017, s. 226; M. MürselBaşgül /OumoutChoeseinoglou, "Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukuki Sorunlar", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Ankara, 2013, 210-215; Selvi, Onur/Küçüksille, Ecir Uğur, "Bulut Ortamında Adli Bilişim", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Eylül, (2013) Ankara, 268-273.

[372] Selvi/Küçüksille, s. 268; Dereboylular, s.164.

[373]Dereboylular, s.168.

[374]Serhat Turan, "Bulut Bilişim Teknolojisi ve Hukuki Problemler, https://www.keyofchange.com/tr/611/Bulut%20Bili%C5%9Fimi%20Teknolojisi%20ve%20Hukuki%20Problemler/, erişim tarihi: 26.03.2022.

müdahale edilmesidir. Ayrıca bulut sistemlerinde arama yapılırken bu sorunu önleyecek etkili bir sistemin ortaya konulduğu da söylenemez[375].

Verilerin bir başka ülkede depolanması, soruşturmayı yürüten ülke açısından elkoymayı fiili olarak olanaksız hale getirmektedir. Bulut hizmet sağlayan kuruluşun yurt dışında olması durumunda sistem üstündeki verilere hızlı bir biçimde erişilmesi oldukça zordur. Bu haldedesüreç uzayacaktır ve hatta delillerin imha edilmesi ya da kasıtlı şekilde değiştirilmesi tehlikesi oluşacaktır[376].

CMK, egemenlik (mülkilik) ilkesi gereğince ülke sınırları içinde uygulanabileceğinden sınır ötesi ağ aramalarına izin veren bir iç hukuk kuralı bulunmadığından, kolluk güçlerinin yabancı bulut sistemi sağlayıcılarından veri ele geçirmesi, verinin bulunduğu ülke ile karşılıklı adli yardım talep edilmesine bağlıdır de etmesi için karşılıklı yardıma dayanması gerekir.Siber suç soruşturmalarında, sınır ötesinde veriye ulaşma erişim sorunları yanında bulut teknolojisi ile ortaya çıkan "yer kaybı" (loss of location) daha da fazlalaşmaktadır[377].

Bulut bilişim hizmetinin, özel ve çerçevesinin dar olduğu bir ağda verilmesi yani tek bir istemcinin kullanımı için oluşturulmuş olması durumunda[378], şüphelinin kullandığı sistemdeki bilgilerinin CMK m. 134 gereğince arama kararı ile ele geçirilmesinin olanaklı olduğu ve bu halde kullanıcının hesap bilgilerine ilişkin verilerin ele geçirilmesi ve kopyalanmasınınolanaklı olduğu ileri sürülmüştür[379].

Bulut bilişim sistemleri bakımından, CMK m. 134'ün madde metni lafzı bazı sorunlara yol açabilecek gibi görünmektedir. Madde metni ve gerekçesinde, bulut bilişime dair herhangi bir atıf veya açıklık yoktur. Yürürlükteki hükmün bulut altyapısı üstünde meydana gelen ya da bulut altyapısını hedef alan suçlara ilişkin muhakeme faaliyetini yürütmek için uyarlanması gerekmektedir. Bulut bilişime CMK m.134'de ye alan tedbirin

---

[375]Dereboylular, s.169-170.

[376]Dereboylular, s.172

[377]Matthew A. Verga, "Cloudburst: WhatDoes Computing MeantoLawyers?", Journal of Legal Technology Risk Management 5/1, 2010, s. 46.

[378]SinemBirsin/Çelebi CemBeril, "A Study on Cloud Computing and Data Protection in theLight of EU andTurkishLaws", Turkish Commercial LawReview, Volume 2, Issue 2, (2016), ss.269-280, s.270; Dereboylular, s.168.

[379]Değirmenci, Dijital Delil, s.242.

uyarlanmasındaki en önemli sorun, hizmet sağlayan işletmenin yurtdışındaki olması ya da işletme yerli bile olsa verilerin yabancı bir ülkede saklanmasıdır. Türkiye'de bulut hizmetlerinden yararlananların çoğunluğunun yurtdışından hizmet aldığıdikkat alındığında, bu kişilerin verilerinin de yurtdışında saklandığı ifade edilebilir. Bununla birlikte, Türkiye'de bulut hizmeti veren bazı Türk şirketlerin veri merkezleri Türkiye'de olduğundan, kullanıcı kişilerin verileri de Türkiye'de saklanmaktadır. Hizmet sağlayıcısının yabancı bir şirket olması halinde CMKm.134'e başvurularak soruşturma için gereken verilerin Türkiye'ye teslimini sağlanabilmesi için adli yardımlaşma yoluna gidilecektir[380].

Öte yandan, bulut bilişim sistemlerinde kişi ve kurumlar, sanal bir kullanım yapmaktadırlar. Arama işlemi sırasında sadeceilgili kişi veya kurumun hesabına tabi veriler üstünde arama yapılmalıdır. Aksi halde,bulut bilişim hizmeti sunan şirketin, sunucu bilgisayarları ve ağının tümünde arama yapılabileceği kastedilmiş olur ki, bu durum gerek CMK m. 134 kapsamında yasa koyucunun beklemediği bir neticenin meydana gelmesine gerekse soruşturmaylailişkisi bulunmayan üçüncü kişilerin, kişisel verilerinin gizliliği ve mahremiyet haklarınazarar verilmesi neticesini ortaya çıkaracaktır[381]. Diğer bir deyişle, CMK m.134'teki tedbirin bulut sistemine uyarlanmasındaki sorunlardan biri de, failin kullanmadığı bir bilgisayarda arama işleminin yapılamayacak olmasıdır. Maddede yalnızca şüphelinin kullandığı bilgisayarda arama yapılması hükmü getirilmiştir.

Sanal Ortamda İşlenen Suçlar Avrupa Konseyi Sözleşmesi'nin 32. maddesi uyarınca bulut hizmet sağlayıcılarındaki verilere erişilip erişilmeyeceği hususunda, bu sağlayıcılarının kendisinden hizmet alanları koruma eğilimi gösterdiği ve bir suç soruşturmasında gizliliğe ve veri korumasına daha fazla önem verebildiği belirtilmektedir[382]. Bu durumda dabulut hizmet sağlayıcısın soruşturma organlarına yardımcı olmaması durumunda soruşturma organları karşılıklı adli yardım sözleşmelerini kapsamında sağlayıcının ve/veya verinin bulunduğu ülkeye adli yardım talebi iletecektir.

[380]Dereboylular, s.183.

[381]Değirmenci, Dijital Delil, s.322.

[382]Dereboylular, s.194.

Diğer taraftan, kamusal bilişim sistemlerinde, bulut hizmetinin verildiği yerin ülke sınırları içerisinde ya da dışarısında olup olmadığına bakılarak sorunun çözülmesi gerekmektedir. Kamuya bulut bilişim hizmetini veren kuruluşun ülke hudutları içerisinde olup olmamasına göre, kamu kurumu tarafındanbulut bilişime sunulan ve kullanıcısı kamu kurumu olan veri, program veya altyapı bilgilerinin ele geçirilmesinde farklı bir yöntem takip etmek gerekmektedir[383]. Burada kamu kurumu olan kullanıcıya ait veriler tutulmaktadır ve bu verilerin bilişim sistemlerinde tutulması ile bulut bilişimde tutulması arasında herhangi bir fark yoktur. Bu yüzden CMK m. 134 kapsamındaverilecek bir arama kararı ile bulut bilişim hizmetini sunan kuruluşta arama yapma olanağı vardır. Ancak bulut bilişim hizmeti veren ülke sınırları haricinde olması halinde ise bulut bilişimde arama yapılması ve verilere elkonulmasıilgili ülke ile varsa adli yardımlaşma sözleşmesi hükümleri veya ilgili ülke tarafsa Sanal Ortamda İşlenen Suçlar Sözleşmesi (m.23 vd) kapsamında adli yardımlaşma çerçevesinde yapılabilecektir[384].

Sonuç olarak, bulut sistemlerindeki delillerin belirlenmesi ve elde edilmesinin güç olduğu görülmektedir. Yukarıdaki açıklamalarda görüldüğü üzere CMK m.134'teki düzenlemenin dar kapsamlı ve yetersiz olduğu, bulut sistemlerini kapsamadığı kanaatindeyiz. Uzaktan erişim ve bulut sistemlerinde aramada bu maddenin uygulanması dahi pek çok soruna yol açabilecektir. Bu açıdan hüküm yeniden düzenlenmeli ve yeni teknolojilere uyumlulaştırılmalıdır. Bulut bilişimin karmaşık niteliği ve delile ulaşmanın zorluklarına ilişkin farkındalığın düşük olması, bulut sistemlerde etkin bir soruşturmayı engelleyecektir. Bununla birlikte,bulut sisteminde araştırma yapacak olan kolluk görevlilerinin donanımlı olmaları zorunludur. Kolluk görevlileri yasada yer alan arama, elkoyma ve inceleme usullerini aynen icra etmeli ve yasadaki yetkilerinin dışına çıkmamalıdırlar. Aksi durumda, teknolojik gelişmelerleuyumlu ve en çağdaş hukuki düzenlemeler yapılsa bile, uygulamanın kötü olması yasaları anlamsız kılacaktır[385].

---

[383]Şeriban Ebem, Kamu Bilişim Sistemleri Açısından Bulut Bilişimin Teknik, Yönetim ve Hukuki Boyutlarıyla İncelenmesi: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler, BTK Teknik Uzmanlık Tezi, Ankara, 2013, s.15 vd.

[384]Değirmenci, Dijital Delil, s.242-243.

[385]Dereboylular, s.184.

2.2.6. Dijital Delilin Toplanması ve Muhafazası

2.2.6.1. Genel Olarak

Uzun yıllardır adli tıp gibi adli uzmanlık bilimleri suç soruşturma ve kovuşturmalarını yapan organlara yardımcı olmakta ve adli olayların bilimsel usullerle çözülmesine yardımcı olmuşlardır. İlgili alanda uzman kişiler, olay yerindeki fiziki ve biyolojik izleri baz alarak olay hakkında detaylı bilgiye ulaşmışlardır. Öte yandan günümüzde suç ve suçlular dijital ortamda faaliyet gösterdikleri için suçu aydınlatma ile görevli uzmanlar bilişim sistemlerindeki sayısal veri ve kodları bulmaya çalışmaktadırlar[386].Fiziki ortam ve delillerde olduğu gibi bilişim sistemleri üstünde dijital iz bırakmaksızın işlem yapmak neredeyse olanaksızdır[387]. Bu izlerin doğru bir biçimde saptanması ve alanındaki teknik ve ilkelerle doğru sonuca ulaşılması amacıyla adli bilişim bilimi ortaya çıkmıştır[388].Bu kavram İngilizce'deki "computerforensic" veya "digitalforensic" kelimesinin karşılığı olarak kullanılmaktadır[389].

Adli bilişim, ceza muhakemesinde etkin şekilde kullanılmasına rağmen özel hukuktaki uyuşmazlıkların da çözümünde yargılamada delilleri ortaya çıkarabilecek bir bilim dalıdır[390]. Adli bilişim incelemeleri de olay yeri inceleme kavramına benzemekte, adli bilişim sürecinde görünmeyen dijital delil, görünür ve ceza yargılaması açısından anlaşılır duruma gelmektedir. Ayrıca bu incelmede delilin tahrifata uğrayıp uğramadığı veya değişip değişmediği belirlenebilmektedir[391].

Adli bilişim, suçun açığa çıkarılabilmesi amacıyla bilimsel metotlar kullanılarak, farklı elektronik (elektromanyetik, elektro optik) aygıtlar içinde bulunan, suçla ilgili ses, görüntü, veri gibi dijital delillerin değişmeden ve tahrif edilmeden anlaşılabilir bir biçimde adli makamlar sunulacak hale getiren ve bilimsel teknik ilkelerin uygulandığı bir delil inceleme

---

[386]Dokurer, s.246.

[387] Yusuf Uzunayve Kemal Bıçakçı. "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu. İstanbul, 9-11 Haziran 2005, http://www.emo.org.tr /ekler/ 4843973f9b66701ek.Pdf, erişim tarihi: 26.3.2022.

[388] Çakır, Sert, s.146.

[389] Başlar, s.221.

[390] Özbey, s.65.

[391]Ünal,s.21.

sürecinin bütünüdür[392]. Bilişim sistemlerindeki dijital delile ilk ulaşıldığı andan başlayarak yargı organlarının sunulması anına kadar geçen aşamaların bir bütün olarak ele alınması, adli bilişimin adli bilimler içinde kabul edilecek bir disiplin konumuna koymaktadır. Öte yandan,adli bilişim işlemleri yalnızca delil toplama ve adli makamlara sunma süreci şeklinde düşünülmemeli ve bilgisayar depolama birimleri üstünden gerçekleştirilen sistematik bir inceleme aşaması şeklinde de kabul etmek gerekmektedir[393].

Adli bilişim aşamalarında belirleyici unsurlar; adli bilişim uzmanı ile incelemenin gerçekleştirileceği laboratuvar ve incelemede yararlanılacak yazılım ve donanımlardır[394]. Bu süreç, genelde olay mahallinde kolluk güçleri ve sonrasında da çoğunlukla zaman laboratuvar ortamında çalışan bilirkişiler tarafından yerine getirilmektedir[395].

2.2.6.2. Dijital Delilin Toplanması ve Muhafazası

Bir suçun işlenildiğinden şüphelenilmesiyle suça ya da olaya ilişkin muhtemel delillerin toplanması gerekir. Delil toplama sürecin hukuka uygun bir biçimde işlemesi, düzenlemelerde yer alan uygun usulün uygulanması ve hukuki koşulların icrasına bağlıdır. Dijital delil toplama işlemi, hukuk kurallarına uygun bir sahada başlatılmalıdır. Bu çerçevede, bir adli soruşturma bağlamında dijital delil toplanıyorsa, arama ve elkoyma kararı öncesinde gerek hukuki sürecin işletilmesi, başka bir deyişle bu konuda mahkeme kararı veya yazılı bir savcılık emrinin bulunması gereklidir[396].

Adli makamlarca bu kararın alınmasından sonra, adli kolluk görevli arama işlemlerinde yasa ve diğer hukuki düzenlemelerde yer alan kurallara göre bir plana göre hareket etmeleri gerekir. Öte yandan soruşturma aşamasında yapılması gereken arama planı, arama kararının çerçevesini de oluşturur. Doktrinde arama kararı isteminin ciddi bir plana dayalı yapılması

---

[392] Ahmet Hasan Koltuksuz, "Adli Bilişimde Olay Yeri İnceleme Esasları", Bilişim Hukuku Konferansı-YARGITAY, Ankara, 09-10 Ekim 2008, s. 12.

[393] Hüseyin Çakır ve Mehmet Serkan Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", Polis Bilimleri Dergisi, Cilt. 15, Sayı. 3, (2013), s. 24.

[394] Keser Berber, s.7.

[395]Henkoğlu,, s.22.

[396]Jasmin CosicandZoranCosic, "Chain of Custodyand Life Cycle of DigitalEvidence", ComputerTechnologyand Application, Vol. 3, No. 2, (February 2012), s. 127.

gerektiği belirtilmektedir[397]. Bunun yapılmaması halinde ise alınacak arama kararına istinaden gerçekleştirilen arama işlemleri esnasında, çoğunlukla arama kararının içeriği yetersiz kalmakta ve bu durumda yeni bir arama kararının alınmasına nende olmaktadır. Yetkilendirilmeksizin arama işlemi gerçekleştirilmesi ve arama işleminin sonlandırılması ve soruşturmanın çıkmaz girmesi gibi problemlere yol açabilecektir[398]. Kanaatimizce 2018 yılında CMK m.134'de yapılan değişiklikten sonra Cumhuriyet savcısının emriyle de bilişim sistemlerine el konulabileceğinden bu sorunun çıkması artık zor görünmektedir.

Kosova hukukunda dijital delillerin elde edilmesine ilişkin düzenlemelere bakıldığında Kosova Ceza Muhakemesi Kanunu'nun (KCMK) "Bilgisayar Analizleri" başlıklı 147. maddesinde bir mahkeme emri veya onay üzerine hukuka uygun bir şekilde alınan bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da benzer teçhizatların içinde bulunan bilgi ya da verilerin ele geçirilmesi ve incelenmesi için resmi bilirkişi olarak polis görevlisi veya bilirkişinin atanacağını öngörmüştür. KCMK m.147/2'da bu alet ve teçhizatların incelenmesi için mahkeme kararı aranmaktadır.

Yine, KCMK m.105/8'de bilgisayar, kamera, cep telefonu, seyyar elektronik cihazlar ya da korunmaya yarayan seyyar elektronik aygıtların esaslı nedenlerin olması halinde muhafaza altına alınmasına (kontrol) karar verilebileceği, kontrol emri ya da geçici el koyabileceği ve bunlardaki dijital verilerin kopyalanabileceği hükmü yer almaktadır.

Mahkeme kararı olmaksızın arama ve el koyma KCMK m.110'da düzenlenmiş olsa bile, bu hükümde, gecikmesinden sakınca olan hallerde, Devlet savcısı veya kolluk amirine bilgisayarlar başta olmak üzere, dijital delillere el koyma yetkisini verilmediği görülmektedir. Dijital delil içeren alet ve teçhizatın mahkemece verilmiş arama kararında yer alması mümkün olamayacağından, gecikmesinden sakınca olan hallerde, Devlet savcısı veya kolluk amirine de el koyma yetki yasa ile tanınmalıdır. El konulma işlemi gerçekleştikten sonra hakim onayı sunma koşulu da getirilebilir.

Öte yandan, dijital delille ilk temasta bulunacak kişi konusu da önemlidir. ABD gibi bazı ülkelerde bu tür delillerle ne şekilde temas edileceğine ilişkin eğitim almış özel müdahale

[397]Karagülmez, s. 98.

[398]Karagülmez, s. 98.

birimleri bulunmaktadır. Türkiye'de fiziki delillerin toplanması ilişkin her ilde örgütlenmiş olay yeri inceleme birimleri bulunsa da,yurt çapında adli bilişime ilişkin delillerin toplanmasını yürütecek birimler[399] henüz kurulmamıştır.

Bilişim sistemleri suç işleme vasıtası olarak kullanılabilir, bu sistemler suça dair deliller içerebilir ve bu sistemler suçun hedefi olabilirler. Bu açıdan olaya ilk temas eden kolluk personelinindijital delilin tanınması, bulunması, korunması ve taşınmasına ilişkin temel bilgi ve eğitimlere sahip olması, hassas bir yapısı olandijital delil için önemlidir[400].

Dijital delil, görsel veya işitsel yapıda olsa da bu delilin ele geçirilmesi kolay olmamaktadır. Çoğu kez, elde edilen bilişim aygıtları farklı bir bilişim cihazı kullanılarak delile ulaşılmaya çalışılmaktadır. Bu sebeple,delil elde etmede kullanılacak ürün, yazılım ve cihazların kapsamı ve yapabilecekleri nispetinde delil ele geçirilebilmektedir. Delil elde edilebilmesi açısından bilişim aygıtlarında suça ilişkin iz ve belirtilerin olabileceği mahallerin iyi tahmin bilinmesi ve bütün olasılıkların titiz şekilde gözden geçirilmesi gerekir. Bilişim aygıtlarındaki dijital delilin belirlenebilmesi için, bu aygıtların iyi bilinmesi ve delil oluşturabilecek verilerin iyi tanınması gerekmektedir[401].

Dijital delillerde, bilgi, belge ve görüntüler manyetik ortamda kaydedilerek saklanır. Bu açıdan suçun özelliğive hedef alanın özelliğine bakılarak dijital delil ele geçirme usulü, cihazı ve yazılımı da farklı olabilir. Bu belirsiz durum, deliller toplanırken yapılacak yanlış bir temasta işlemi başarısız kılabilir ve delil yok olabilir veya hukuka aykırı hale gelebilir[402]. Örneğin hardisk veya hafıza kartı gibi manyetik medyaları anti-statik paketlerle paketlenmezse bozulabilir ve bir daha açılmayabilir[403].

Dijital delil elde edildiğinde adli makamlarca muhafazaya alınmalı ve muhafaza safhasında koruma zinciri meydana getirilmesi gerekmektedir. Koruma zincirinin zarar görmesi, dijital

---

[399] Yusuf Başlar, Adli Bilişim Sürecinde Karşılaşılan Sorunlar Ve Çözüm Önerileri, TBB Dergisi 2020, S.148, s.55 (Adli Bilişim); Cosic and Cosic, s. 127.

[400] Ali Osman Özdilek, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul: Vedat Kitapçılık, 2006, s. 202.

[401] Başlar, s.227.

[402]Karagülmez, s.31.

[403] Hakan Ekizer, Bilişim Suçları, Adli Bilişim, İnceleme Araçları ve Örnek Olay Analizi, 2013, https://www.ekizer. net/wp-content/uploads/2013/12/A.Hakan_Ekizer_Adli_Bilisim-Bilisim_Suclari_Sunum.pdf, erişim tarihi: 27.3.2022.

delilin geçerliliği hususunda şüpheye yol açacaktır. Öte yandan, muhafaza safhasında dijital delilin, kasıtlı şekilde zarar vermek isteyen kötü niyetli şahıslardan ya da deneyimsiz personelden güvenli bir şekilde korunması gerekmektedir. Dijital delilin ele geçirilmesi ve muhafazası safhasında; delillerin bütünlüğünün temin edilmesi ve kontrolü gerçekleştirilmektedir. Esasında bu safhadan önce ya da bu safhayla beraber sürdürülen bir diğer safha da dijital delilin tespiti aşamasıdır. Bu aşamadan, nelerin dijital delil olduğu tespit edilerek, bu doğrultuda delil toplama ve muhafaza işlemi yapılmaktadır[404].

Dijital delilin belirlenmesi ve muhafaza altına alınması kendine özgü niteliklere sahip olsa da dijital delilin araştırma usulleri ve fiziki delillerin araştırılma usulleri pekçok yönden benzerdir. Suçluların bilişim sistemlerini suçun işlenmesinde araç olarak kullanmaları ya da kendi aralarındaki iletişimi veyahut işlemleri kolay hale getirmek ve bilgileri kaydetmek için amacıyla kullanması halinde adli bilişim devreye girecektir. Dolandırıcılık suçu bilişim sistemleri vasıtasıyla yapıldığında bu sistem suçta kullanılmış olacaktır[405].

Bilişim sistemleriyle ilişkili suçların araştırılması esnasında suç mahalli veya arama yapılan yerde çalışan adli bilişim görevlilerinin en fazla süre ayırdığı safha, delillerin toplanması ve belgelere kaydedilmesi safhasıdır. Bu safhanın titiz şekilde gerçekleştirilmesi, dijital delilin nerelerden ele geçirilebileceği hususunda önemli ipuçları vermektedir[406].

2.2.6.3. Dijital Delil Ele Geçirilirken Uyulacak Temel İlkeler

Dijital delilin ele geçirilmesi ve korunması safhası, adli bilişimin başlangıç safhasıdır. Bu safha, delil bütünlüğünün temin edilmesi açısından da oldukça önemli bir safhadır. Çünkü bu safhada dijital delilin zarar görmesi ya da yok olması olasıdır. Bazen bilgisayarın çok ufak bir şekilde hareket ettirilmesi veya depolama aygıtlarının anti-statik poşete konulmaması dahi, dosya, veri, zaman damgası gibi delilin dijital özelliklerinin

---

[404] Başlar, s.228; Osman Nihat Şen, "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, s. 36.

[405]ServetYetim, "Dijital Kanıt Araştırma Yöntemleri". İstanbul Barosu Dergisi. Cilt. 82, Sayı. 3, Mayıs-Haziran 2008, s.1209.

[406]Henkoğlu, s.5.

değişmesine yol açabilmektedir. Bu durumda elektronik delilin ele geçirilmesi safhasında bazı ilkelere uyma mecburiyetini beraberinde getirmektedir[407].

Türkiye'de dijital delilin nasıl ele geçirileceğine dair ayrıntılı bir yasal düzenleme yoktur. CMK m.134 ve Adli ve Önleme Aramaları Yönetmeliği m.17'de ayrıntılı kanuni hükümler olarak görülemez. ABD gibi bazı ülkelerde soruşturma aşamasında dijital delilin ele geçirilmesine dair işlemleri yapan ekibin nasıl davranacağını düzenleyen, bağlayıcı olan, delil toplamada yanlış gerçekleştirilen işlemlerin ihlal şeklinde kabul edilerek ceza soruşturmasına konu olacağını düzenleyen yasal hükümler bulunmaktadır. Türkiye'de dijital delilin ele geçirilmesine dair hukuki boşluğun nedeni olarak alt yapısı olmaksızın bilişim teknolojilerinin Türkiye'ye ithal edilmesi, bilişim suçlarının boyutlarına dair farkındalığın olmaması ve mağdurlarca dahi konunun bilinmemesi olduğu ifade edilmiştir[408].

Bilişim suçları ve başkaca suçlarda adli bilişim; soruşturma ve kovuşturmanın ayrılmaz bir parçası olmuştur. Adli bilişim sürecinin başlamasına ihtiyaç duyulan yerlerde, olay yeri ile ilk temas edecek kolluk görevlilerinin elkonulacak bilişim sistemlerine müdahale usulüne dair kurallar konulması, toplanacak delillerin hukuka aykırılığı iddialarını önemli ölçüde engelleyecektir[409].Olay mahallindeki işlemlerde gerçekleştirilen hatalar, delillerin güvenilirliği ve gerçekliğine zarar verebilir ve soruşturma veya kovuşturmayı zora sokabilir[410].

Olay yerine ilk temas eden adli bilişim ekibi ilk olarak delil elde etmede kullanılacak aygıtları hazır hale getirmeli, olay yerinin güvenliğini ve bozulmamasını temin etmeli, olay yerinde dijital vasfa sahip olan ya da olmayan bütün delillerin sağlamlığı ve bütünlüğünü muhafaza altına almalıdır[411].

---

[407] Yusuf Başlar, Elektronik Delilin Toplanması Ve Muhafazası, Hacettepe HFD, 10(1) 2020, ss.77-107, s.82 (Elektronik Delilin Toplanması Ve Muhafazası).

[408] Başlar, Elektronik Delilin Toplanması Ve Muhafazası, s.82; Karagülmez, s.403.

[409] Keser Berber, s. 7.

[410]Henkoğlu, s. 17.

[411] Yetim, s.1209.

Adli işlemlere başlamadan evvel denetim listeleri, donanım birimleri ve kullanılacak yazılımlar hazır tutulmalıdır. Özellikle denetim listeleri, olay mahallindeki tüm sorunlara karşın, safhaları atlamadan, eksiksiz bir delil toplama işlemi yapılmasın sağlayacaktır[412].

Dijital delil ele geçirme işlemleri olabildiğince adli bilişim uzmanlarınca gerçekleştirilmelidir. Çünküsadece bir adli bilişim uzmanı, delil kaybına ve delil güvenilirliğinin ihlaline sebep olmaksızın dijital delil toplayabilir[413].

Olay yerinde soruşturma işlemine başlamadan evvel ve gerçekleştirilen işlemler esnasında olay yeri ile bilişim sistemi ve donanımlarının fazla sayıda fotoğrafı çekilmelidir. Bununla birlikte, sistemin tüm bağlantıları ve seri numaraları ayrıntılı ve incelenebilecek şekilde görüntüye alınmalıdır. Bu fotoğraflar ve görüntü kayıtları, daha sonra ileri sürülebilecek şüpheleri gidermek için kullanılabilir[414]. İnceleme esnasında olay mahallindeki bilişim sisteminin işletim şemasının oluşturulması da yararlı olabilecektir. Dijital delilleri tahrip edebilecek nesne ve durumlara dikkat edilmeli, olay mahallinde hesap adı ya da şifre olması muhtemel yazı ve notlara da bakılmalıdır[415].

Olay mahallinde yer alan ve delil olabilecek nesnelerin üzerine yeterli açıklayıcı bilgi yazılan delil etiketleri konulması da önem arz etmektedir. Öte yandan, bir liste meydana getirilerek elkonulan tüm nesne ve materyaller seri numaralarıyla beraber buraya yazılmalıdır. Tüm nesneler için farklı listeleri oluşturulması ileri sürülmüşse de[416], bunun uygulamada kolluk güçlerine sorun oluşturabileceği ve karışıklığa sebep olacağı kanısındayız. Hatta elkonulan bilişim sistemlerinin sonradan kolayca birleştirilebilmesi için bütün kablolar renk kodu ile kodlanmalıdır[417].

Dijital delil elde edilirken yapılan bütün işlemler tutanağa bağlanmalıdır.Dijital delilin ele geçirilmesine dair araştırma ve incelemeler, fiziki ortama dayanmadığındanarama işlemi bitene kadar gerçekleştirilen işlemler tek tek tutanağa bağlanmalıdır. Çünkü bu tutanaklar,

---

[412]Henkoğlu, s. 17.

[413]Çakır ve Sert, s. 156; Karagülmez, s.401.

[414]Henkoğlu, s. 19.

[415]Cem Günal, "Adli Bilişim ve Delillerin Toplanması", Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu. İstanbul, 18 Şubat-11 Mart 2012, s.41.

[416]Henkoğlu, s. 19.

[417]Değirmenci, Dijital Delil, s.214; Henkoğlu, s. 19.

dijital delilin, delil niteliğini güçlendirmektedir. Ayrıca bu tutanaklar, kovuşturma safhasında bu delile yöneltilecek itirazlar önlenebilecek ve uzman bilirkişi raporu alınırken, bu delilin arama yapılan bilişim sisteminden ele geçirilip geçirilmediği de daha kolay denetlenebilecektir[418].

Olay yerindeki bilişim sistemlerinden kapalı konumda bulunanların açılmaması gerekir. Çünkü bilişim sistemlerinde dijital delillervarsa sistemin açılması halinde bu delillerin zarar görebileceği haller olabilir. Örneğin bilgisayarın işletim sistemi açılırken birçok konfigürasyon dosyası açılmakta ve delil olabilecek verilerin zarara uğramasınaneden olabilir[419]. Ayrıca, arama yapılan yerdeki bilişim sistemleriaçık ise bunlarada dokunulmamalı, ekranda görünen pencere veya gerçekleştirilen bir işlem buluyorsa bu durum tutanağa geçirilmeli, sonra bilişim cihazının türüne bakılarak ve güç kesilerek e kapatılmalıdır. Hatta, bilişim sistemlerine müdahale edilirken bu sisteme uzaktan erişim sağlanarak delilsilinmesi olasılığına karşı gerekli koruma sağlayacak donanım ve yazılımlar da olay yerine getirilmelidir[420].

Arama yapılan yerde dijital delilharicinde fiziki deliller de yer alabileceğinden bilişim sistemleri ve donanımlar üstünde bırakılmış olabilecek parmak izi, şüpheliye ait giysi ve kullandığı eşyada delil vasfında bulunabilir. Bu fiziki deliller toplanırken hassas yapısı olan dijital delile de zarar verilmemelidir[421].

2.2.6.4. Canlı Analiz İşlemi

Dijital delil toplamak için arama yapılan yere ekipler, ilk olarak incelemenin yapılacağı bilgisayarların doğru bir şekilde kapatılması ve bunların korunmasından sorumludurlar. Bundan sonra bilişim sistemleri üzerinde ve başka depolama birimlerinde imaj alma işlemlerine başlanabilir. Bunun yanında, inceleme yapılacak bilişim sisteminin örneğin bilgisayarın kapatılması ya da yeniden başlatılması, sistem üstündeki uçucu verilerin

---

[418]Karagülmez, s.401.

[419] Hakan Ekizer, Adli Bilişim, http://www.ekizer.net/adli-bilisim-computer-forensics, erişim tarihi: 27.3.2022.

[420] Çakır ve Sert, s. 157.

[421] Başlar, s.233.

kaybolmasına yol açabilmektedir[422]. Yakın zamana kadar çalışır haldeyken elkonulan bilgisayarlar,olağan kapatma ile değil doğrudan kablo çekilerek birden elektriğin kesilmesiylekapatılmakta ve bu şekilde elkoyma işlemi yapılmaktaydı. Bu şekilde elektrik kesilmesiyle kapanan bilgisayardaki bilgilerin farklı bölümlere kaydedilmesi amaçlanmaktaydı[423].

Günümüzde ise açık şekilde elkonulan bilgisayarlardaki uçucu verilerin soruşturmanın aydınlatılmasında önemi anlaşıldığından bilgisayar kapatma yerine açık tutulması için başka araçlar ortaya çıkmış ve canlı analiz usulü de tatbik edilmeye başlanmıştır. Çalışır durumdaki bilgisayar sistemlerinde, uçucu verilerin elde edilmesi için canlı analiz yapma niteliğini barındıran pekçok yazılım vardır. Bu yazılımlar, sisteme kurulum yapılmadan çalışabilmektedir. Bu yolla incelenen bilgisayar diski üstünde bir ekleme gerçekleştirilmeksizin ve dijital delilin de orijinalliği bozulmadan gereken inceleme ve işlemler gerçekleştirilebilmektedir[424].

Canlı analiz işlemi, olağandijital delil ele geçirme işlemindendaha fazla teknik uzmanlığa ihtiyaç duyulan bir işlemdir. Bazı durumlarda suç işlenen bilişim sistemleri içinde, dijital delilleri silecek ya da bir virüsü etkinleştirecek tuzaklar bulunmaktadır. Bilhassa siber saldırılar, kredi kartları veya internet üstünden işlenen dolandırıcılık suçları ve zararlı kod dağıtımı gibi suçlar işlenirken kullanılan bilişim sistemlerinde gerçekleştirilecek incelemelerde,sistem kapatılmadan uçucu verilerin ele geçirilmesi ve kayda alınması gerekir. Bu yöntem, bir siber saldırının olması durumunda sistem yöneticilerinin verileri kurtarmak için kullandığı bir yöntemdir. Ayrıca, olay mahallinde açık halde ele geçirilen bilgisayarın üstünde halen şüpheli programların çalışıyorsa ve ekranda delil niteliği vasfına sahip dosyalar bulunuyorsa, canlı analiz işleminin yapılması gerekmektedir[425].

Soruşturmada ağ trafiği bilgilerinin ele geçirilmesi gerekiyorsabuna yönelik işlemler de canlı analiz işlemi ile yapılmalıdır. Sistem açık durumda olduğunda ağ trafiği bilgileri

---

[422]Henkoğlu, s. 26.

[423] Bilal Şen, "Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller", Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt. 3, Ankara, 11 Ocak-15 Ocak 2010, s. 69.

[424]Henkoğlu, s. 29

[425] Başlar, s.234; Henkoğlu, s. 27

toplanabileceğinden, sistemin anlık resmi çekilerek o esnada sistemde bulunan veriler ele geçirilir ve analize tabi tutulur[426].

2.2.6.5. İmaj Alma

Genel hukuk kurallarına göre belgeler üstünde gerçekleştirilecek olan (sahtecilik) inceleme, sadece gerçek metin üstünden yapılabilecek olup, örneğin fotokopi üstünden sahtecilik incelemesi yapılamayacaktır.Bu bağlamda kopyası ele geçirilen bir dijital verinin geçerli bir dijital delil şeklinde kabul edilmesi,ispata ilişkin kuşkulara yol açabilecektir. Bunun yanında, adli bilişim aşamalarında dijital veri kopyasının usulüne uygun alındığı hallerde dijital verilerden hangisinin asıl olduğunun bir önemi bulunmayacağı kuralının, imajı alınan dijital delil açısında geçerli olmadığı ileri sürülmektedir[427].

Bilişim sistemlerinde kopyalama işlemi; dosya düzeyi, bölüm düzeyi ve disk düzeyi olarak üç aşamada yapılır. Dosya düzeyinde ve bölüm düzeyinde gerçekleştirilen kopyalamalarda, bir dosya sıradan bir kullanıcı şeklide kopyalanmaktadır. Bu halde, diskiçin yer alan silinmiş ya da kısmen silinmiş dosyalar kurtarılamaz. Fakat disk düzeyinde yapılan kopyalamada orijinal diskin aynen kopyası alınabilmektedir. Disk düzeyinde yapılan birebir kopyalama, adli bilişim işlemlerinde kullanılan kopyalama yöntemidir. Bu kopyalama çeşidinde orijinal ve kopya disk tamamıyla ve her yönden birbirine eşit gelmektedir[428].

Adli bilişim sürecinde gerçekleştirilen birebir kopyalama işlemine, imaj alma adı verilir. İmaj almada alınan kopya;var olanve silinmiş verileri, gizli dosyaları, verinin depolandığı aygıttaki başka verileri de içermektedir[429]. Fakat birebir kopyalama (imaj alma) işlemi esnasında bazı uygun önlemlerle orijinal veride gerçekleşebilecek tahrifatların önü alınmalıdır. Bu durum,dijital delil toplama safhasının en mühim safhalarından biridir.İmaj alma işleminin amacı, bilişim sistemlerindeki verilerin bütünlüğü ve güvenliğini temin etmektir. Şüphelinin kullandığı bilişim sistemi içindeelkonulan verilerin sonradan değiştirilmediği, verilere ekleme ya daçıkarma yapılmadığıteminat altına alınmaktadır. Bu

---

[426]Değirmenci, Dijital Delil, s.223.

[427]Değirmenci, Dijital Delil, s.140.

[428] Say, Bilişim Suçlarında, s.71.

[429] Ahmet Serhat Şirikçi ve Nergis Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi", Bilişim Teknolojileri Dergisi, Cilt. 5, Sayı. 3, Eylül 2012, s. 30.

şekilde savunmanınöne süreceği delillerin değiştirildiği veya eklendiği iddialarıönlenebilecektir. Ayrıca imaj alma, verilerin elde edilmesi safhasında verilerin zarar görmesini önleyecektir[430]. İmaj alma olağan kopyalamadan farklı olup, sistem dosyaları ve gizli dosyaların kopyalanmasını da içermektedir.

Diskin imajının alınması, dijital delilin, adli anlamda analiz aşamasının başlangıcıdır. İmajın doğru bir biçimde alınması, tüm soruşturma ve kovuşturmaya etki edebilecek önemli bir aşamadır. İmajın doğruluğu, dijital delilin adli analizinin gerçekleştirilmesi ve mahkeme süreci sırasında sorgulanması bunu göstermektedir. Dijital delilin incelenmesinin orijinal delil üstünde doğrudan yapılması, suç şüphesinin bulunduğu veri depolama aygıtının zarar görmesi ya da analizi yapan şahıs tarafından verilerin değişmesine yol açabilmektedir[431]. Ufak bir hata dahi delil niteliği kazanabilecek bir verinin yok olmasına sebep olabilir.Hatta imaj üstünde yapılan incelemede bir yanlışlık varsa orijinal veriler yeni bir imaj alınması için kullanılabilir[432].

İmaj alma, özel yazılımlar kullanılarak ve alt düzey bit değeri olarak diğer bir ortamda bir örnek meydana getirilmesi yoluyla gerçekleştirilir. Bunun yapılmasının sebebi; silinen, değiştirilen, deforme edilen verilere de ulaşma imkanını vermesidir[433]. Örneğin olağan kopyalama ile bir bilişim siteminde yeni dosya yapısında (NTFS)tutulan bilgilere ulaşılabilirken eski dosya yapısı olan FAT ile tutulan verilerin kopyalanmadığı görülmektedir[434]. YineNorton Ghost vePartitionImager gibi sistem yedeği alan programların da sistem üzerinde var olan, ancak dosyaların bulunmadığı alanları kopyalamadığı görülmektedir. Bu durumda dosyaların bulunmadığı alanlarda silinmiş veriler olabileceğinden, bu boş alanlar da delil kaybına yol açabilecektir[435]. İmaj alma,

[430]Değirmenci, Dijital Delil, s.76.

[431]Henkoğlu, s. 47.

[432] Say, s.86.

[433]Günal,s51.

[434] Murat Özbek, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu, Elazığ, 20-21 Mayıs 2013, s. 2.

[435]Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (erişim tarihi:3.4.2022).

donanım araçlarıyla imaj alma[436] ve bilgisayar ortamında imaj alma yazılımlarıyla yapılmaktadır[437].

2.2.6.6. Hash (Veri Bütünlük) Değeri

Gelişen teknolojiler adli bilişim yoluyla elde edilen verilerin onaylanmasını sağlayacak hizmet ve yolların ortaya çıkmasını gerekli kılmıştır. Diğer bir deyişle veriye bağlanacak hüküm ve sonuçların doğrulamasının yapılması ve ispat edilebilirliğinin de temin edilmesi de zorunludur. Aksi halde adli bilişimde dijital verilerden yararlanmak olanaklı olmayacaktır[438].Bu bağlamda, dijital delillerin bütünlüğü, aramada ele geçirilen, incelenen ve hakkında görüş bildirilen dijital verinin değişikliğe uğrayıp uğramadığını göstermektedir.Arama yapılan yerden ele geçirilen bir verinin orijinal hali ile incelmesi yapılan veri birebir aynı olmalıdır[439].

Elde edilen verinin orijinal haliyle kullanıldığına dair teknik inceleme gerçekleştirilebilmesi ve ispatlanabilmesi için, dijital delilin muhafazası ve denetimin yapılması için zaman damgası ve kopyalama işlemi esnasında hash değerinin belirlenmesi gerekir[440].

Hash değeri, bir veri ya da veri depolama aygıtının ilk kısmından (sektör) son kısma kadar tamamının belli bir algoritmik fonksiyondan geçmesi neticesinde meydana gelmektedir. Bu değer, dijital verinin orijinal olup olmadığı konusunda tek ölçüt olmasa da en önemli ölçütlerden biridir.Bu değer hakkında "*bir dijital belgenin DNA'sıdır*" denilmektedir[441].Bu değer benzersiz özellikte olduğundan veri depolama ünitesi üstündeki bir karakterin değişimi bu değerin de değişikli göstermesine yol açar. Bu açıdan dijital delil ya da bu delilden temin edilen imaj üstünde bir değişiklik meydana gelip gelemdiğini denetlemek içinhash değeri hesaplatılır ve üstünde işlem yapılan verilerin orijinal veri ile aynı olup

---

[436] Şen, s.37.

[437] Aydoğan, s. 36.

[438]Seyithan Deliduman, "Elektronik Verilerin Delil Değeri", Bilişim Hukuku, Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s. 47.

[439]Henkoğlu, s. 80.

[440]Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tespit edilmemiş bulunması..," Yargıtay 8. CD. 24.10.2013, E. 2012/21817, K. 2013/25428 (UYAP).

[441]Dülger, s.823; Tanrıkulu, s.324.

olmadığı denetlenir[442].Sıklıkla kullanılan hash algoritmaları, MD5 ve SHA'dır[443]. Bu algoritmaların kullanımı neticesinde meydana çıkan değerler, imajla beraber aynı dosya içinde saklanabilir ya da ayrı bir dosyada toplanabilir[444].Hash hesaplaması neticesinde bulunan hash değeri ile veri ilke el konulduğunda hesaplanan hash değerinin birbiri ile aynı ise dijital delilin ya da dijital delilden elde edilen kopyada bir değişiklik olmadığı neticesine ulaşılır[445]. Her iki değerin aynı olmaması durumunda, elde edilen veri veya bulguların geçerli bir delil olarak kabul edilmesi olanaklı olmayacaktır[446].

Öte yandan, çalışan sistemler, RAM' veya cep telefonlarından alınan imajlarda sistem çalışmaya devam ettiğinden,sistem içi zararsız küçük değişiklikler yapıldığı bilindiğinden bu tür bir inceleme yapılmamaktadır[447].Sabit diskler gibi manyetik veri depolama aygıtları, CD-DVD gibi optik veri depolama aygıtları ve SSD disklerde de hash sorunlarının ortaya çıkmaktadır[448]. Bununla birlikte, hash değeri, yalnızca verinin değiştirilmesi ile değil, veri depolama aygıtında gerçekleşen mekanik bozulmalardan ya da bozuk birimlerden de oluşabilir[449]. Sabit disk üstünde verilerin yer aldığı alanlar; nem, manyetik etkiler, sarsıntı ve benzerinedenlerle kullanılamayacak duruma gelebilir. Bu alanlara *bozuk alan* adı verilmekte olup, belge özeti hesap edilirken bu bozuk sahalar göz önüne alınmamaktadır. Bu sebeple bozuk alan sayısı da önemli görülmektedir[450].

---

[442] Özbek, s.2.

[443]Leyla Keser Berber, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma Paneli,9 Temmuz, 2008, s.478; http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/h/Hm12.pdf, erişim tarihi: 04.04.2022.

[444] Say, s.78.

[445] Özbek, s.2.

[446]Henkoğlu, s. 54-55.

[447] Özbek, s.6.

[448]Özbek, s.2.

[449]MuratKızılyar, "Ceza Yargılamasında Dijital Verilerin Delil Değeri". Adalet Dergisi. Sayı. 50, Eylül 2014, ss. 72-89.s, 86.

[450]Mehmet SerkanKılıç, Elektronik Delillerin Hukuken Geçerliliği Açısından İlk Müdahalenin Önemine İlişkin Bir İnceleme, Terazi Aylık Hukuk Dergisi, Yıl:10, Sayı:102, Şubat 2015, s.40; MesutOrta, Bilişim Suçlarında Adli Analiz, Yetkin Yayınevi, Ankara, 2015, s.270-271; Dülger, s.824.

2.2.6.7. Zaman Damgası (Time Stamping)

Dijital delilin bütünlüğünün korunmasındahash değerinin alınması yanındayargılama sürecinde dijital delile ne zaman ulaşıldığı, görevli kolluk personelinin delille temasta bulunduğu süre, dijital delilin bütünlüğünün ne kadar süreyle temin edilebileceği gibi soruların cevaplanması gerekir. Çünkü,dijital delilin bütünlüğünün kanıtlanması ve dijital delile erişilme zamanının kesin şekilde bilinmesi önemli olup, bu, zaman damgası ile temin edilebilmektedir[451].

Dijital alemde zaman damgası dijital formatta belirli bir anı tanımlamaktadır. Zaman damgası, bir dijital verinin üretilme, değiştirilme, gönderilme, alınma, kaydedilme zamanın belirlenmesini sağlayan dijital bir veridir[452]. Zaman damgasının bu özelliği nedeniyle ele geçirilen dijital delili üretme, erişme ya da değiştirme zamanları üstünde oynama yapılması ya da değiştirilmesi önlenmiş ve delillerin doğruluğu kanıtlanmış olmaktadır[453].

5651 sayılı Kanun kapsamında çıkarılan Yönetmelik[454]7/1-c maddesinde yer sağlayıcının yükümlülükleri yer almış olup, yer sağlayıcılar trafik bilgilerini altı ay süreyle saklamak, bu bilgilerin doğruluğu, verilerin dosya bütünlük değerlerini zaman damgasıyla beraber saklamak ve gizliliğini sağlamakla yükümlü oldukları hükme bağlamıştır. Aynı Yönetmelik m.8/1-b'de erişim sağlayıcının yükümlülüklerini düzenlenmiş ve onlara da bu yükümlülükler bir yıl süre ile yüklenmiştir.

Dijital delilin zamanla çok ilişkili olmasından dolayı zamanın kaynağı da güvenilir olmalıdır. Örneğinbaşkasına ait ve saat ayarı da hatalı olan bir bilişim sistemi kullanılırsa yanlış bir zaman damgası oluşturulabilir. Bu halde zamanın tamamıyla güvenilir olduğundan söz edilemez ve bu şekilde oluşturulan zaman damgası, bu dijital delilin soruşturmada tartışmalı hale gelmesine yol açar[455].

---

[451]JasminCosicandMiroslov Baca, "(Im)ProvingChain of CustodyandDigitalEvidenceIntegritywith Time Stamp, http://czb.foi.hr/upload/datoteke/10_400.pdf (erişim tarihi: 04.04.2022).

[452] Başlar, 2020, s.95.

[453]Aydoğan, s.37.

[454] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik; RG Tarih: 30.11.2007, Sayı: 26719

[455] Tamer Soysal, "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu", Türkiye Barolar Birliği Dergisi, Sayı. 61, Kasım-Aralık 2005, s. 309.

Zaman damgasına ilişkin en yaygın hatayı, sistem saatindeki kaymalar oluşturmaktadır. Dijital delilin toplandığı sistem saatindeki hatalar ve ya sunucuların ağ üzerindeki uzak sistemlerden alınan günlük kayıtlarda oluşturulan zaman damgalarında sunucudaki saat kayması hataya yol açabilmektedir[456].Ağ günlüklerinde genellikle görülen zamansal hata kaynağı, saat dilimi farklılıklarıdır.Örneğin bir internet sunucusundan bilgi talep edildiğinde, saat dilimi uyumsuzluğu bu sağlayıcının yanlış abone bilgilerin sunmasına ve hatta suçla ilgilisiz bir kişinin yargılanmasına yol açabilir.

2.2.6.8. Koruma Zinciri

Koruma zinciri, bir delilin fiziksel ya da dijitalşekilde toplanması, korunması, farklı bir yere nakli ve incelenmesini belgeleyen kronolojik belgelendirme sürecidir. Bu zincirle birlikte delillerin de doğrulanması temin edilmektedir. Bu açıdan dijital verilerin soruşturma ve kovuşturmada kullanılabilecek özellikte geçerli bir delilşeklinde kabulü, bu verilerin elde edildiğiandan başlayarak koruma zinciri kriterlerine uygun şekilde, el değmeksizin korunmakta ve incelemeyi gerçekleştirecek uzmana tevdi edilmesine bağlıdır[457]. Koruma zinciri, gerek elektronik aygıtı gerekse bu aygıtta bulunan dijital veriyi kapsar.

Delillerin koruma zinciri ile toplanması ve belgelendirilmesi, hash değerinin belirlenmesi gibi delil toplama sürecinin en önemli öğelerinden birisidir. Uygun bir koruma sürecinde dijital delilin nerede, ne zaman, nasıl ele geçirildiği ve analize tutulduğu, ilk olarak temas zamanı ve kişisinin de bilinmesi gerekmektedir. Bunun en sağlam yolu delilin kayda alınmasıdır. Bu kayıt belgesi korunarak dijital delinin ele geçirildiği andan itibaren değişikliğe uğramadığı kanıtlanmış olacaktır[458]. Bu soruların cevapsız kalması durumunda koruma zinciri de bozulmuş kabul edilir. Sağlıklı bir koruma zincirinin bulunmaması, dijital delilin kirlenmesine ve geçerliliğini kaybetmesine yol açabilir[459]. Dijital delile ilişkin

---

[456]Casey, Eoghan, "Error, Uncertainty, andLoss in DigitalEvidence", International Journal of DigitalEvidence, Yıl: 2002, Cilt: 1, Sayı: 2,https://www.academia.edu/2983793/Error_Uncertainty_and_Loss_in_Digital_Evidence, (erişim tarihi: 04.04.2022).

[457]Kunter, Yenisey ve Nuhoğlu, C. I, s. 1320.

[458] Başlar, s.249.

[459]Casey, DigitalEvidenceandComputerCrime, s. 22.

koruma zincirine dair akreditasyon standartları, laboratuvar politikaları, prosedürler ve başka kurallarına bilinmesi ve uygulanmasında da sapma olmaması gerekir.

Soruşturma safhasında dijital delili ele geçiren her kimse, bu delilin ilk ele geçirildiği hali ile kovuşturma aşamasında öne sürüldüğü halinin aynı olup olmadığı noktasında ifadesine başvurulabilir. Delillere ilk temas eden kişinin mahkemede hazır bulunması gerekli olmasa dahi, bu halin asgari seviyede tutularak dijital delilin ilk elde edildiği andan başlayarak mahkemeye gönderildiği süreye kadar değiştirilmediğinin açık olması isabetli olacaktır[460].

2.2.6.9. Dijital Delilin Paketlenmesi, Taşınması ve Muhafazası

Dijital delillere ilişkin önemli sorunlardan birisi de bu delillerin güvenilirliğinin korunmasıdır. Dijital deliller, hassas yapılarından ötürü, hatalı koşullarda paketleme veya taşıma ya da yanlış şekilde korunma neticesinde kolaylıkla bozulabilir, değişime uğrayabilir veya yok olabilir. Bu sebeple, dijital delili paketleme, taşıma ve koruma için özel tedbirler alınması gerekir. Aksi durumda, dijital delil kullanılamaz ya da muhakeme açısından faydasız bir hale gelebilir[461].

Uygulamada veri depolama biriminin anti-statik poşetle veri depolama aygıtını paketlememesi, elektronik medya ve aygıtlara aşırı basınç uygulamak suretiyle yazı yazılması, zımba ile CD gibi dijital medya üstünde delik açılması, sıcak yapışkan kullanılması neticesinde medyalar üstünde kâğıt ve yapışkan madde artıklarının kalması gibi yanlışlıklar sebebiyle elektronik aygıtlar veya veri depolama birimlerine zarar verildiği görülmektedir[462].

Dolayısıyla ilk olarak elde edile dijital delilin paketlenmesine başlamadan evvel delillerin düzgün bir şekilde listelenmesi ve etiketlenmesi gerekir. Dijital verinin depolandığı araçlar, anti statik poşetlere konulmalı, statik elektrik üreten olağan plastik torbalar gibi malzemeler kullanılmamalıdır. Yine CD-ROM, floppy disk ya da bantlar gibi elektronik medyanın

---

[460] Başlar, s.249.

[461]ChetHosmer, "ProvidingtheIntegrity of DigitalEvidencewith Time", International Journal of DigitalEvidence, Vol. 1, No. 1, Spring 2002, s.1.

[462]LeventBayram, Adli Bilimlerde Ses ve Konuşma İncelemeleri, Ankara: Seçkin Yayıncılık, 2008, s. 155.

bükülmemesi, çizilmemesi ve katlanmaması gerekir. Delilleri taşımak için kullanılan paketlere doğru şekilde etiketleme yapılması gerekir[463].

Veri depolama birimlerinden imaj alınırken hash değerleri yazılmalı ve bu değerler tutanaklarda belirtilerek sonradan ileri sürülebilecek itirazlar engellenmelidir[464]. İmaj alma,olanaklar elverdiğince olay yerinde bağımsız fiziki kopyalama aygıtları ile yapılmalı ve bu imajlar korunarak orijinal materyaller ile adli emanete teslim edilmelidir[465].

Yine dijital delil taşınırken manyetik alanlardan uzak tutulmalı, radyo verici ve ısı kaynaklarına yakın konulmamalıdır. Ayrıca dijital delili, aşırı sıcak, aşırı soğuk, nem ya da aşırı titreşime maruz kalmamalıdır[466].

Bir başka dijital veri kaynağı cep telefonları da bozulma ve değişikliklere yönelik korunması gerekmektedir. Delil elde edilecek cep telefonlarının başka cep telefonlarıylaya da hücresel ağlarla bağlantı kurmasına izin verilmemelidir, çünkü bu bağlantı kurulduğunda, bu veri depolama birimlerindeki dijital verilerin zarar görebilir. Bu nedenle radyo sinyallerini ya da başka telefonlarla bağlantıyı önleme özelliği olan "faraday poşetleri" kullanılabilir[467]. Yine batarya ile çalışan ve dijital delil bulunduran aygırlara el konulduktan sonra bir miktar şarj edilmesi yararlı olacaktır. Çünkü bazı dijital aygıtların bataryasının tümüyle boşalması durumunda bu cihazlar, program ve tarih/zaman bilgilerini unutmak suretiyle fabrika ayarlarına dönebilmektedirler. Görüldüğü üzere bu elektronik aygıtların korunmasına özen gösterilmediği takdirde, elektronik aygıtlar veya veri depolama birimleri bozulabilmektedir. Bu açıdan adli emanete teslim edilecek olan orijinal aygıt veya veri depolama birimi, mühürlü torbada korunmalıdır[468].

---

[463] Keser Berber, Adli Bilişim, s. 72.

[464]Henkoğlu, s. 25.

[465] Çakır ve Sert, s. 159

[466] Keser Berber, Adli Bilişim, s. 72.

[467] Başlar, s.252.

[468] Çakır ve Sert, s. 160; Henkoğlu, s. 25

3. SONUÇ

Maddi gerçeğin açığa çıkarılması, ceza yargılamasının amacı olup, bu amaç gerçekleşen fiil ile fail arasındaki bağın kanıtlanmasıyla sağlanmaktadır. Muhakeme aşamalarında edilen deliller hâkimin vicdani kanaatinin oluşmasına yardımcı olmaktadır. Öte yandan olayı ispatlayacak delillerin ortak özellikleri;gerçekçi olmaları, akla ve mantığa uygun olmaları, gerçekleşen olayı temsil etmeleri, taraflarınca bilinir, erişilebilir ve tartışılabilir olmaları ile hukuka uygun şekilde elde edilmeleridir.

Ayrıca deliller; beyan delili, belge delili ve ispata konu olan olayı dolaylı olarak ispatı eden her türlü iz ve eser anlamına gelen belirti delili şeklindeayrımlara tabi tutulmaktadır. Dijital delil, bilişim sistemlerinden ve elektronik aygıtlardan elde edilse de,bilirkişi raporu ile hayat bulduğundan, belge niteliğindeki delillerindendir. Gerek Türk gerekse Kosova hukukunda dijital delillere ilişkin bilirkişi raporu hazırlanacağı belirtildiğinden her iki hukuk açısından dijital delillerin belge delili olduğu söylenebilir.

Türk hukukunda Anayasa'nın 38/6. maddesine uygun şekildeyüklenen suçun sadece hukuka uygun biçimde toplanmış delille ispat edilebileceği (CMK m.217/2) ve kanuna aykırı şekilde toplanan delillerin duruşmada ortaya konamayacağı (CMK m.206/2-a) hükme bağlanmıştır. Kosova hukukunda da mahkemelerin karar alırken adli inceleme kapsamında değerlendirilen ve doğrulanan delillere dayanarak karar vereceği (KCMK m.8/2) belirtilmiştir. Ayrıca, bazı maddelerde de örneğin kontrol (muhafaza altına alma) sırasında delillerin hukuka uygun elde edilmiş olması gerektiği vurgulanmıştır (m.111/1).

Dijital delil yerine elektronik delil kavramının da kullanıldığı görülmekte olup, elektronik delil kavramını kullananlar, bu kavramın, gerek elektronik aygıtı gerekse bu aygıt içindeki dijital verileri kapsadığından, dijital delil kavramına oranla daha üst bir mana içerdiği ifade edilmiştir. Kanaatimizceelektronik yapısı olan her aygıtın dijital verisinin olduğundan bahsedilemez. Dijital delillerin; elektronik yapıda olduğu gerçek olsa da, sadece dijital durumda bulundukları hallerde dijital delil anlamında değerleri olacaktır ve bu çeşit deliller de elektronik delil değil, dijital delil şeklinde tanımlanmaları daha isabetli olacaktır.

Modern dünyada bilişim sistemleri her alanda kullanılmakta olup, bilişim suçları gibi önceden bilinmeyen yeni suç türlerinin meydana çıkmasına yol açmış ve pek çok klasik suç türü bilişim sistemleriyle işlenir hale gelmiştir. Bu açıdan dijital delil;gerek bilişim suçları

gerekse bilişim sistemleri vasıtasıyla işlenen hırsızlık, dolandırıcılık, hakaret gibi suçların soruşturulması ve şüpheli ve sanıkların belirlenmesi açısından önemlidir. Bazıhallerde kasten öldürme suçunun kamera görüntülerine ilişkin delillerin bilişim sistemlerinde gizlenmesi halinde olduğu gibi tümüyle fiziksel dünyada gerçekleşen bir olayın çözülmesinde dijital delillere ihtiyaç duyulabilir.

Dijital delilin kendine özgü özelliklerinden biri, DNA gibi gizli yapıya sahip olmasıdır. Dijital delilin elde edilebilmesi ve incelenebilmesi için bazı teknik cihazlarla gözlem yapılması gerekir. Ayrıca bu delil, hassas bir yapıya sahiptir ve kolayca değişikliğe uğrayabilmektedir. Dijital delilin soyut verilerden oluşması, bu verilerden bazen net bir sonuca varılmasını da zorlaştırabilmektedir. Dijital delilin korunmasının zor olması ve bütünlüğünün sağlanması açısından sorunlara rastlanabilmektedir. Dijital delilin kasten ya da kazayla değiştirilebilir olması, bu delilin güvenilir bir delil olması noktasında itirazlara yol açabilmektedir. Dijital delillerin yapılarından doğan hassaslık sebebiyle çoğunlukla savunma tarafı, bu delillerin hukuki ve teknolojik geçerliliğine ilişkin itirazda bulunmaktadır.

Öte yandan, dijital delilin, birebir kopyasının(imaj) alınarak bunun üstünde inceleme gerçekleştirilmesi, orijinal delilin bozulma ihtimalini önleyebilir. Dijital delilin tümüyle ortadan kalkması zor veya bazenolanaksızdır. Çünkü, dijital deliller silindiğinde geri getirilebilir, bu delilin değiştirilmesi ve bozulması halinde de orijinal delilden yeniden birebir kopya alınarakdurum tespit edilebilir.

Dijital delillerde de gerçeklik, rasyonellik, erişebilirlik, temsil edicilik, müştereklik ile hukuka uygunluk gibi fiziki delillerde olması gereken özellikler yanında;dijital delilin bütünlüğü, doğrulanması, hususundaki geçerlilik ilkelerine uygun olmalıdır.

Bilişim sistemlerindeki yani dijital delillere ilişkin koruma tedbirleri,temel hak ve hürriyetlerden olan özel hayata saygı, haberleşmenin gizliliği ile düşünceyi açıklama ve yayma özgürlüğünün korunması hakları açısındna AİHS m.8/2 ve 10/2'u ihlal edebilmektedir. Bu temel hak ve özgürlükler, Türk Anayasası'nın 20/2, 22/2 ve 26/2. maddelerinde ve Kosova Anayasasının 36/1, 36/3 ve 40/1. maddelerinde korunmakta olup, bu özgürlüklere yönelik müdahaleler belirtilen istisna hallerinde ve ölçülülük (orantılılık)

ilkelerine uygun şekilde bu özgürlüklere müdahale edilebilir. Bu müdahaleler kanunla öngörülmelidir.

Kosova hukukunda dijital delillerin elde edilmesine ilişkin düzenlemelere bakıldığında Kosova Ceza Muhakemesi Kanunu'nun (KCMK) "Bilgisayar Analizleri" başlıklı 147. maddesinde bir mahkeme emri veya onay üzerine hukuka uygun bir şekilde alınan bilgisayar teçhizatları, elektronik muhafaza teçhizatları ya da benzer teçhizatların içinde bulunan bilgi ya da verilerin ele geçirilmesi ve incelenmesi için resmi bilirkişi olarak polis görevlisi veya bilirkişinin atanacağını öngörmüştür. Ayrıca, KCMK m.105/8'de bilgisayar, kamera, cep telefonu, seyyar elektronik cihazlar ya da korunmaya yarayan seyyar elektronik aygıtların esaslı nedenlerin olması halinde muhafaza altına alınmasına (kontrol) karar verilebileceği, kontrol emri ya da geçici el koyabileceği ve bunlardaki dijital verilerin kopyalanabileceği hükmü yer almaktadır. Yine Kosova hukukunda Sibernetik Suçlarla Mücadele Kanunu gibi kanunlardaki bilgisayar sistemleri kullanılarak işlenen suçlarda dijital delil etme yöntemleri yer almaktadır. KCMK m.147, m.105/8 ve m.110 hükmü birlikte değerlendirildiğinde, gecikmesinden sakınca olan hallerde, mahkeme kararı olmaksızın Devlet savcısı veya kolluk amirine bilgisayarlar başta olmak üzere, dijital delillere el koyma yetkisini verilmediği görülmektedir. Elde edilmesi umulan tüm dijital delil içeren aletlerin mahkemece verilmiş arama kararında yer alması mümkün olamayacağından, gecikmesinden sakınca olan hallerde, Devlet savcısı veya kolluk amirine de bu yetki yasa ile tanınmalıdır.

Türk hukukunda ise CMK m.134'de bilgisayar ve bilgisayar sistemlerinde arama, kopyalama ve elkoyma koruma tedbiri düzenlenmiş olup, bu maddeye göre bu bilişim sistemlerindeki dijital delillerin mahkeme kararı ve gecikmesinde sakınca olması durumunda Cumhuriyet savcısı kararıyla el konulabileceği hükmü yer almaktadır. Türk hukukunda da 5651 sayılı Kanun'da erişim sağlayıcı, yer sağlayıcı gibi sağlayıcıların kayıt altına aldıkları verileri adli makamlarla paylaşmaları gerektiğine dair hükümler bulunmaktadır.

Bilgisayarın bütün özelliklerini taşıması sebebiyle bilgisayar tanımı içinde kabulü gereken, ancak bilgisayar şeklnde görülmeyen cep telefonu, cep bilgisayarı ve elektronik veri içeren pekçok cihaz ve diğer bilişim sistemlerinde CMK m. 134 yerine m. 116 ve 123

düzenlemelerine göre arama ve elkoyma işlemleri yapılması temel hak ve özgürlük ihlallerine yol açacaktır. Uygulamada da bu aygıtlara ilişkin yapılan el koyma ve arama kararlarında CMK m.134'ün uygulanması isabetlidir.

CMK'nın 134. maddesinde düzenlenmeyen veya eksik olarak düzenlenen bazı konuların Adli ve Önleme Arama Yönetmeliği m.17'de düzenlemeye çalışılmışsa da, bu eksikliklerin tamamıyla giderildiğini söylemek olanaklı değildir. Nitekim, temel hak ve özgürlükleri doğrudan etkileyen ve bilişim sistemlerinin kullanıldığı suçlardaki eksikliklerin kanun yerine yönetmelik hükümleriyle kapatılamaya çalışması da yerinde değildir.

Yine CMK m.134'de yer alan koruma tedbirinin, uzaktan erişimle arama için tatbik edilemeyeceği söylenebilir. CMK'da kıyas mümkün olsa da, koruma tedbirleri temel hak ve özgürlükleri doğrudan etkilediğinden, bu hükümlerde kıyasın kullanılmaması ile bu konuda açık ve öngörülebilir bir yasal düzenleme yapılması gerektiği kanaatindeyiz. Bu tedbirin bulut bilişim üzerinde uygulanıp uygulanamayacağı konusunda ise üç olasılık bulunmaktadır. İlk olarak, özel bulut bilişim ile servis sağlayıcısı yurt içinde bulunan kamusal bulut bilişim hakkında söz konusu koruma tedbiri uygulanabilecektir. İkinci olarak servis sağlayıcısı yurt dışında bulunan kamusal bulut bilişim hakkında ise adli yardımlaşma talebi ile bu veriler istenebilecektir. Üçüncü yol olan ve CMK m.134 ve KCMK m.147'de düzenlenen bilgisayar ve bilgisayar kütüklerine el koymaya ilişkin koruma tedbirine ilişkin hüküm, Siber Suç Sözleşmes m.19'da yer almaktadır. Bu madde gereğince taraflar, yetkili makamlarını kendi ulusal sınırları içinde, bir bilgisayar sisteminde veya sistemin bir parçasında ya da veri saklama cihazlarında arama yapma veya benzer şekilde erişim yapma konusunda yetkilendirmeleri gerekmektedir. Yine Sözleşme'nin 32. maddesine göre sözleşmenin bir tarafı, diğer tarafın ülkesinde, bilgisayarda tutulan verilere, bahse konu bilgisayar sistemi üstünden erişim yetkisine sahip olan şahsın rızasının olduğu hallerde veya bu verilerin herhangi bir kimsenin erişebileceği biçimde açık olduğu hallerde sınır ötesinden erişim sağlayabileceği ve bunları temin edebileceği ifade edilmiştir.

Dijital delilin delil olarak kabul edilebilmesi, onun hukuki anlamda geçerliliğinin kontrol edilmesine bağlıdır. Elektronik aygıtlar üstünde olan suça dairdijital delilin bozulmadan veya zarar görmeden anlaşılabilir bir biçimde soruşturma ve kovuşturma makamlarınaverilmesini sağlayan ve bilimsel ilkelerin tatbik edildiği bir delil inceleme

sürecinin tümü olan adli bilişim, aslında dijital delilin teknolojik anlamda geçerliliğini sağlamaya dair bir süreçtir. Adli bilişim sürecinin göze çarpan iki unsuru, adli bilişim uzmanı ve laboratuvardır.

Adli bilişimin aşamaları; dijital delilin elde edilmesi ve korunması, incelenmesi, analizi ve raporlanması aşamalarıdır. Dijital delilin elde edilmesi ve korunması safhası, adli bilişimde ilk aşama olup delil bütünlüğünün temini açısından çok önemli bir aşamadır. Bu açıdan dijital delille ilk temas edecek kişinin uzmanlığı, yeterliliği, tecrübesi, bu delil toplanırken izlenmesi gerekli kurallara bağlılık, delillerin paketlenmesi ve korunmasındaki hassasiyet seviyesi, dijital delilin bir bütün olarak incelenmesi ve raporlanarak yargı organlarına sunulmasında belirleyici rol oynamaktadır.

Dijital delil üstünde uygulanan bazı teknik işlemlerden biri; imaj alma işlemidir. İmaj işlemi, elektronik aygıtta olan bütün verilerin, silinmiş ve gizlenmiş verilerin ve boş alanların kopyalanması işlemi anlamına gelmektedir. Birebir kopyalanmış veri ile asıl veri arasında fark bulunmamakta, inceleme işlemleri bu kopya üstünde yapılmakta ve bu şekilde orijinal verinin bozulmaması temin edilmektedir. Bir başka işlem ise orijinal ya da imajı alınmış verinin hash değerinin yani veri bütünlük değerinin hesaplanmasıdır. Hash değeri, dijital veri üstünde gerçekleştirilen matematiksel algoritma ile meydana getirilen tek taraflı bir değerdir. Dijital veri elde edilirken bulunan hash değeri ile mahkemeye sunulan bilirkişi raporunda hash değerinin aynı olması gerekmektedir. Aksi halde bu verinin delil olarak kullanılması olanaklı olmayabilecektir. Ayrıca, dijital verinin üretilme, değiştirilme, gönderilme, alınma ve kaydedilme tarih ve saatinin belirlenmesi için verinin zaman damgasıtespiti yapılmaktır. Bu şekilde dijital verinin üretildiği, erişildiği ya da değiştirildiğitarihler üstünde değişiklik yapma olanağı önlenmiş olacaktır.

Dijital delilin toplanması ve muhafazasındadikkate alınması gereken bir başka nokta da koruma zincirinin sağlanmasıdır. Koruma zinciri, dijital delilin doğrulanması ve geçerliliğinin sağlanması açısından çok önemli olsa da, dijital ya da fiziki delilin, toplanması, korunması, nakli veya incelenmesini gösteren kronolojik belgelendirme sürecidir. Dijital verinin inceleme işlemi, genelde anahtar kelimeyle arama işlemi aracılığıyla yapılır. İnceleme aşamasında, silinen verilerin geri getirilmesi, internet gezinti geçmişinin incelenmesi, gizli verilerin açığa çıkartılması işlemleri yapılır.Dijital delilin

analizi aşamasında da delil olabilecek verilerden hangilerinin ve ne orandaisnat edilen suçlailgili olduğu hususu açığa çıkarılması ve adli makamlara rapor halinde sunulması sağlanır. Analiz aşaması, teknik anlamda açığa çıkarılan dijital delilin kanıt değerini meydana çıkaran hukuki değer verme işlemidir.

Son aşama olan raporlama aşamasında dijital delil, taraflarca anlaşılır şekilde ortaya konulmaktadır. Diğer adli bilişim aşamaları, usul ve esaslarına uygun şekilde yapılmış olsa da iyi bir raporlama işlemiyle mahkemeye sunulmazsa adli bilişim süreci verimli şekilde işlemeyecektir. Bu sebeple raporlama safhasında adli bilişim süreçlerinden geçen dijital delilin bütünlüğünü sağlayanbütün hususlar tarafların anlayabileceği şekilde rapor haline getirilmelidir.

Tüm bu açıklamalardan görüldüğü üzere, bilgisayarlar ve cep telefonları gibi bilişim sistemlerinde bile dijital verinin elde edilmesine ilişkin CMK m.134 ve KCMK m.147'nin yetersiz kaldığı ve bu delillerin elde edilme süreçlerine ilişkin daha ayrıntılı yasal düzenlemeler yapılması gerektiği açıktır. Bununla birlikte, her iki ülkenin mevzuatında uzaktan erişim ile arama ve bulut bilişim sistemlerinde yapılacak aramalar için yasal düzenleme yapılması gerekmektedir. Türk hukukunda 5651 sayılı Kanun ve Kosova hukukunda Sibernetik Suçlarla Mücadele ve Önlenmesi Yasası hükümleri bu iki yeni dijital verinin aranacağı yerlere ilişkin hüküm getirmekte yetersiz kalmaktadır. Elbette, verilerin tutulduğu sunucuların yurt dışında olması halinde AK Siber Suçlarla Mücadele Sözleşmesinin 32. maddesi gündeme gelecektir. Ancak verilerin tutulduğu sunucuların sahibi olan şirketlerin uzaktan erişime izin vermeyecekleri dikkate alındığında, sunucuların bulunduğu ülkeden verileri adli yardımlaşma yoluyla temin edilmeye çalışılacaktır.

Dijital delilin elde edilme sürecinde değişime uğraması ihtimali taşıması sebebiyle bu aşamada görev alan bütünkolluk görevlilerinindijital delile dair bütün işlemlere dair hukuki düzenlemeler ve prosedürlere karşı bilgilendirilmeleri gerekmektedir. Ancak, adli bilişim alanına ilişkin önemli sorunların da adli bilişim alanındakiprensip ve standartlarının tespit edilmemesi, uygulanacak yasal usule çerçevesindeki işlemlerin öneminin kolluk güçlerince bilinmemesi, adli bilişimdeki görevlilerin yeterince eğitilmemiş olması olduğu görülmektedir.

KAYNAKLAR

ACPO GoodPractice Guide forComputerBasedEvidence, https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf, Erişim tarihi: 08.03.2022

Ademaj, X., *Kriminoloji Uzmanlığı*, Priştine, 2010.

Akarslan, H., Bilişim Suçları, Ankara: Seçkin Yayıncılık, 2012.

Akbulut, B., Delil Değerlendirme Yasakları, Fasikül, Y: 2, S: 13, 6-25, Aralık 2010.

Akıncı, H., Alıç, E., Er, C., "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk, Yeşim Atamer (der.), İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

Akyürek, G., Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu, Türkiye Barolar Birliği Dergisi, Sayı: 101, Temmuz 2012, 61-82. 2012.

Aksoy İpekçioğlu, P., Gözaltında Alınan İfadenin Önemi Ve Delil Değeri, AÜHFD , C.57 Sa.3, 51-82, 2008

Anayurt, Ö, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, Ankara: Seçkin Yayıncılık, 2004.

Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk, Ankara: Ankara Barosu Yayınları, 2009.

Arifi, B., Olay Yerinin Gözlemlenmesi, 2012.

Arnavutluk Cumhuriyeti Başsavcılığı, Maddi Kanıta El Koyma Rehberi, Tiran 2003.

Ashcroft J., "Electronic CrimeSceneInvestigation: A Guide for First Responders", Washington: PhotoDisc, Inc, 2001, s.6, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (erişim tarihi 25.03.2022).

Avşar, Z., Öngören, G., Bilişim Hukuku, İstanbul: Pasifik Ofset, 2010.

Aydın, D., Ceza Muhakemesinde Deliller, Yetkin Yayınevi, Ankara 2014.

Aydoğan, H., Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Yayınlanmamış Yüksek Lisans Tezi. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara 2009.

Ayers, R., Brothers, S., Jansen, W.,. Guidelines on Mobile Device Forensics, NIST Special Publication Revision 1, (800-101), 2014, ss.1-85.

Badem, S., Ceza Muhakemesi Hukukunda Tanık, TAAD, Yıl: 12, Sayı: 45, 289-326, Ocak 2021.

Başlar, Y., Adli Bilişim Sürecinde Karşılaşılan Sorunlar Ve Çözüm Önerileri, TBB Dergisi S.148, 77-107, 2020

Başlar,Y., Ceza Yargılamasında Elektronik Delil, Yetkin Yayınları, Ankara 2016.

Başlar, Y., Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, Uyuşmazlık Mahkemesi Dergisi, Cilt. 1, Sayı. 3, 47-75, 2014.

Başlar, Y., Elektronik Delilin Toplanması Ve Muhafazası, Hacettepe HFD, 10(1), 77-107, 2020 (Elektronik Delilin Toplanması Ve Muhafazası).

Başgül, M. M./Choeseinoglou, O., "Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukuki Sorunlar", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Ankara, 210-215, 2013.

Beebe, N., Digital Forensic Research: The Good, The Bad And The Unaddressed. IFIP Int. Conf. Digital Forensics, 2009, ss.17-36.

Begeja, S. Kriminoloji, Cilt I, Tiran Yayınları 2001.

Batalli, F., *Adli Tıp*, Priştine 1987.

Bayraktar, B., "Muhakemelerde Delillerin Önemi", Kırgızistan-Türkiye Manas Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı. 25, 9-19, 2011

Bayram, L., Adli Bilimlerde Ses ve Konuşma İncelemeleri, Ankara: Seçkin Yayıncılık, 2008.

Bıçak, Vahit, Suç Muhakemesi Hukuku, 2. Basım. Ankara: Seçkin Yayıncılık, 2013.

Birsin, S., Çelebi Cem, B., A Study on Cloud Computing and Data Protection in theLight of EU andTurkishLaws, Turkish Commercial LawReview, Volume 2, Issue 2, 269-280, 2016.

Birtek, F., AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat, 2. Baskı, Adalet Yayınevi, Ankara 2017.

Bozdağ, A.- Sarıusta, K., Ceza Yargılamasında Mağdurun Beyanı Ve Delil Değeri, İnönü Üniversitesi Hukuk Fakültesi Dergisi –İnÜHFD- C:8 S:2, 573-602, 2017.

Casey, E., DigitalEvidenceandComputerCrime: ForensicScience, Computersandthe Internet, 3. Edition, Londra: AcademicPress, 2011.

Casey, Eoghan, "Error, Uncertainty, andLoss in DigitalEvidence", International Journal of DigitalEvidence, Yıl: 2002, Cilt: 1, Sayı: 2, https://www.academia.edu/2983793/Error_Uncertainty_and_Loss_in_Digital_Evidence, (erişim tarihi: 04.04.2022).

Casey, E., Kerr, S.O., "DigitalEvidenceandthe New CriminalProcedure", Columbia LawReview, 105, 279-318. 2005.

Cengiz, S., Wieser ve BiocosBeteligungenGmBH/Avusturya (çev.), İnsan Hakları Avrupa Mahkemesi Kararları, Türkiye Barolar Birliği Dergisi, Sayı. 82, Mayıs 2009, 461-462, 2009.

Centel, N- Zafer, H., Ceza Muhakemesi Hukuku, Beta Yayınları, İstanbul 2015.

Centel, N., Zafer, H., Çakmut, Ö., Türk Ceza Hukukuna Giriş, 11. Bası, İstanbul: Beta Yayınevi, 2020.

Caloyannides, M. A., Privacy Protection and Computer Forensics(Artech House Computer Security Series) [2 ed.], Artech House Publishers, 2004.

Council of Europe, Electronic Evidence Guide, 2013, s. 11, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20 Guide/2467_EEG_v18protected.pdf (Erişim tarihi: 01.04.2022).

Cosic, J. - Baca, M., (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO. 2010, ss: 1226-1230

Cosic, J., Cosic, Z., "Chain of Custodyand Life Cycle of DigitalEvidence", ComputerTechnologyand Application, Vol. 3, No. 2, February 2012, 126-129, 2012.

Cosic, J, Baca, M., (Im)ProvingChain of CustodyandDigitalEvidenceIntegritywith Time Stamp, http://czb.foi.hr/upload/datoteke/10_400.pdf (erişim tarihi: 04.04.2022).

Çakır, H., Kılıç, M.S., "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", Polis Bilimleri Dergisi, Cilt. 15, Sayı. 3, 23-44, 2013.

Çakır., H., Sert, E., Bilişim Suçları ve Delillendirme Süreci, Örgütlü Suçlar ve Yeni Trendler, Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010), Oğuzhan Ömer Demir ve Murat Sever (dr.), Ankara, 2011.

Çolak, H., Taşkın, M., Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku, 2. Basım, Ankara: Seçkin Yayıncılık, 2007.

Dağ, G., Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Yayınlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2011.

Değirmenci, O., Ceza Muhakemesinde Sayısal (Dijital) Delil. Ankara: Seçkin Yayıncılık, 2014, (Dijital Delil).

Deliduman, S., "Elektronik Verilerin Delil Değeri", Bilişim Hukuku, Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 44-56, 2006.

Demirbaş, T., Soruşturma Evresinde Şüphelinin İfadesinin Alınması, Ankara 2011.

Department of Justice of USA, SearchingandSeizingComputersandObtaining Electronic Evidence in CriminalInvestigations, https://www.justice.gov/file/442111/download, (Erişim tarihi: 08.03.2022).

Dereboylular, Ö., Bulut Bilişim Bakımından Arama Ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği, CHD - Nisan 2019, S. 39, 161-202, 2019.

Dokurer, S., Adli Bilişim", Ses Görüntü ve Data İncelemeleri, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 239-249, 2008.

Donay, S., Ceza Yargılama Hukuku, İstanbul: Beta Yayınevi, 2012.

Donay, S., İnsan Hakları Açısından Sanığın Hakları ve Türk Hukuku, İstanbul 1982.

Dülger, M.V., Bilişim Suçları ve İnternet İletişim Hukuku, 6. Baskı, Ankara: Seçkin Yayıncılık, 2015.

Dülger, M.V., Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması, TAAD, Yıl:8, Sayı:31, 141-258, 2017.

Ebem, Ş., Kamu Bilişim Sistemleri Açısından Bulut Bilişimin Teknik, Yönetim ve Hukuki Boyutlarıyla İncelenmesi: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler, BTK Teknik Uzmanlık Tezi, Ankara, 2013.

Ekizer, H., Adli Bilişim, http://www.ekizer.net/adli-bilisim-computer-forensics, erişim tarihi: 27.3.2022.

Ekizer, H., Bilişim Suçları, Adli Bilişim, İnceleme Araçları ve Örnek Olay Analizi, 2013, https://www.ekizer. net/wp-content/uploads/2013/12/A.Hakan_Ekizer_Adli_Bilisim-Bilisim_Suclari_Sunum.pdf, erişim tarihi: 27.3.2022.

Erdem, M.R., "5271 Sayılı Ceza Muhakemesi Kanunu'nda Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", www.ceza-bb.adalet.gov.tr/makale/115.doc, Erişim tarihi:08.06.2022

Erdoğan, Y., "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt. 12, Özel Sayı, 1363-1433, 2010.

Erdoğan, Y., Türk Hukuk Sisteminde Bilgisayar Araması ve Bulunan Delillere Elkonulması, Bilgi Sistemleri ve Bilişim Yönetimi (Edt. Fahrettin Özdemirci/Zeynep Akdoğan), Ankara, 173-190, 2017.

Ergün, İ., Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara: Adalet Yayınevi, 2008.

Eryılmaz, A., Ceza ve Disiplin Hukukunda Hukuka Aykırı Delil, Ankara 2013.

Feyzioğlu, M., Ceza Hukuku Muhakemesinde Tanıklık, Ankara 1996.

Feyzioğlu, M., Ceza Muhakemesinde Vicdani Kanaat, Yetkin Yayınevi, Ankara 2002

Gaxha, A., Biyolojik İzler ve Bunların Ceza Muhakemesi Kanunundaki Rolü Ve Önemi, Tiran Yayınları, 2014.

Gordon, A. (Ed.). Official (ISC)2 Guide to the CISSP CBK. 4. Baskı, CRC Press, 2015

Gökcen, A.- Çakır, K., Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi Ve Delil Yasakları, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2911-2951, 2019.

Göksu, M., Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayınevi, 2011.

Gören, Z. "Düşünceyi Açıklama Özgürlüğü". **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi.** Sayı. 24, Güz 2013/2, 31-60, 2013.

Gözübüyük, A. Ş., Gölcüklü, F., Avrupa İnsan Hakları Sözleşmesi ve Uygulaması Avrupa İnsan Hakları Mahkemesi İnceleme ve Yargılama Yöntemi. 9. Basım. Ankara: Turhan Kitabevi, 2011.

Günal, Cem. "Adli Bilişim ve Delillerin Toplanması", Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu. İstanbul, 18 Şubat-11 Mart 2012, 1-69, 2012.

Güngör, D., Ceza Muhakemesinde Tanık Beyanının Delil Değeri Üzerine Bazı Tespit Ve Değerlendirmeler, İnönü Üniversitesi Hukuk Fakültesi Dergisi, C:6, S. 2, 307-318, 2015.

Hajdari, A., Ceza Muhakemesi Hakkı, Yayın Priştine, 2010.

Hajdari, A., Kosova Ceza Muhakemesi Kanunu Yorumu, Basımı, Priştine, 2016.

Halili, R., Kriminoloji, Sekizinci Baskı, Priştine 2016.

Hekim, H. Başıbüyük, O., Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt. 4, Sayı. 2, 2013, 135-158, 2013

Henkoğlu, T., Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, 2. Baskı, İstanbul: Pusula Yayıncılık, 2014.

Hewling, M.O. Digital Forensics: An Integrated Approach For The Investigation of Cyber/Computer Related Crimes, Bedfordshire University, Phd Thesis, 2013.

Hosmer, C., "ProvidingtheIntegrity of DigitalEvidencewith Time", International Journal of DigitalEvidence, Vol. 1, No. 1, Spring 2002, 1-7, 2002.

Hueske, E., Essentials of ForensicsScience- Fire armsandfingerprints, Set Editor, SuzaneBell, 2009.

Hukuk Sınavı El Kitabı, Kosova Cumhuriyeti, Priştine, 2016.

Irons, A., Stephens, P., Ferguson, I. Digital Investigation As A Distinct Discipline: A Pedagogic Perspective. Digital Investigation, 6(1-2), 2009, ss.82-90.

Kajtazi, F., Tabancalar ve Revolverler, 2015.

Karagülmez, A., Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014

Karakehya, H. - Arabacı, M., Cumhuriyet Savcısının Hukuki Statüsü, Muhakemedeki Taraf Pozisyonu Ve İspat Yükünün Bulunması Üzerine., Ankara Üni. Hukuk Fak. Dergisi, 65 (4), 2059-2081, 2016.

Karakurt, A., Türk Ceza Muhakemesi Hukukunda İddianamenin İadesi, S.8-9, 71-114,2004.

Kaygısız,M., Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği, Ankara 2010

Kaymaz, S., İletişimin Denetlenmesi: Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan, 4. Baskı, Ankara: Seçkin Yayınevi, 2015.

Kaynakçıoğlu, U., Ceza Muhakemesinde Dijital Deliller, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2015.

Keser Berber, L., Adli Bilişim, Ankara: Yetkin Yayınları, 2004.

Keser Berber, L., Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma Paneli, 9 Temmuz, 2008, s.478; http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/h/Hm12.pdf, erişim tarihi: 04.04.2022.

Ketizmen, M., Türk Ceza Hukuku'nda Bilişim Suçları, Ankara: Adalet Yayınevi, 2008.

Kılıç, M. S., Elektronik Delillerin Hukuken Geçerliliği Açısından İlk Müdahalenin Önemine İlişkin Bir İnceleme, Terazi Aylık Hukuk Dergisi, Yıl:10, Sayı:102, Şubat 2015, 39-51, 2015.

Kızılyar, M.. Ceza Yargılamasında Dijital Verilerin Delil Değeri. Adalet Dergisi. Sayı. 50, Eylül 2014, 72-89, 2014.

Koca, M. Ceza Muhakemesi Hukukunda Deliller, Ceza Hukuku Dergisi (CHD), Sayı. 2, Aralık 2006, 207-225.

Koltuksuz, A. H., "Adli Bilişimde Olay Yeri İnceleme Esasları", Bilişim Hukuku Konferansı-YARGITAY, 09-10 Ekim 2008, Ankara, 2008.

Korajliq, N., Kriminoloji Taktikleri,Priştine, 2007.

Kosova Cumhuriyeti Siber Güvenliği Devlet Stratejisi, 2016-2020, 2016.

Kratz, M., "PrivacyandCloud Computing", LawNow, Volume 37, 35-40, 2013.

Kunter, N., Yenisey, F., Nuhoğlu, A., Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Baskı, İstanbul: Beta Yayınevi, 2010.

Latifi, V., *Kriminoloji, Suç Tespiti Ve Kanıtlanması*, Priştine, 2011.

Lee, H. C., Materijalnitragovi (Maddi izler), Zagreb, 1998.

Memushi, L., İnsani Biyoloji. Tiran 2006.

Marcella, A. J. –Menendez, D., Cyber Forensics: A Field Manual for Collecting,Examining,and Preserving Evidence of Computer Crimes, Auerbach Publications, 2007

Marcus, P., Waye, V., Australiaandthe United States: TwoCommonCriminalJusticeSystemsUncommonly at Odds, College of William & Mary Law School FacultyPublications,2004,s. 32,

http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1245&context=facpubs. (Erişim tarihi: 08.03.2022);

Mason, S., "Introduction", Stephen Mason (ed.), International Electronic Evidence, Londra: British Institute of International andComparativeLaw, 2008.

Modly, D., Çağdaş Kriminolojik Teoriler, (Çev.) MustafReqica, Priştine 2007.

Murati, R., Protection of Human RightsunderKosovo'sCriminalCodeandCriminalProcedureCode, Chicago Kent-LawReview, 80 (1), 99-117, 2004.

Myftari, E., Olay Yerini Gözlemlemek, Tiran, 1984.

Gürkan Özocak, "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması". İzmir 2. Uluslararası Bilişim Hukuku Kurultayı, İzmir, 17-19 Kasım 2011, 110-125, 2011.

Oğuz, H., Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, Uyuşmazlık Mahkemesi Dergisi, Cilt. 1, Sayı. 3, 1-38, 2014.

Orta, Mesut,Bilişim Suçlarında Adli Analiz, Yetkin Yayınevi, Ankara, 2015.

Önok, M., Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof. Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt.19, Sayı:2, 1229- 1269, 2013.

Özbek, M., Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları, 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu, Elazığ, 20-21 Mayıs 2013, 1-7, 2013.

Özbek, V.Ö., Ceza Muhakemesi Hukuku. Ankara: Seçkin Yayıncılık, 2006.

Özbek, V. Ö., Ceza Muhakemesi Hukukunda Delil Yasakları, Alman Türk Karşılaştırmalı Ceza Hukuku, Cilt III, İstanbul 2010.

Özbek, V.Ö., Kanbur, M. N., Doğan K., Bacaksız, P., Tepe, İ., Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, 7. Baskı, Ankara, 2015.

Özbey, Ö., Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK'nın 134. Maddesi), Yargıtay Dergisi, Cilt. 36, Sayı. 3, Temmuz 2010, 61-126, 2010.

Özdilek, A. O., Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul: Vedat Kitapçılık, 2006.

Özen, M., Baştürk, İ., Bilişim-İnternet ve Ceza Hukuku, Ankara: Adalet Yayınevi, 2011.

Özkan, H., Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği", Yener Ünver (Ed.), Ceza Muhakemesi Hukukunda Delil ve İspat içinde Ankara: Seçkin Yayıncılık, 265-287, 2014.

Öztürk, B., Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Güncellenmiş 14.Baskı, Ankara 2020.

Öztürk, B., Yeni Yargıtay Kararları Işığında Delil Yasakları, AÜSBF Yayınları, Ankara 1995.

Öztürk, B., Erdem, M.R. Uygulamalı Ceza Muhakemesi Hukuku, 12.Baskı, Seçkin Yayınevi, Ankara 2008.

Öztürk, B., Erdem, M.R., Özbek, V.Ö., Uygulamalı Ceza Muhakemesi Hukuku, 7. Baskı, Ankara: Seçkin Yayıncılık, 2002.

Parlar, A., Hatipoğlu, M., Yüksel, E.G., Açıklamalı-İçtihatlı Ceza Muhakemesi Hukukunda Deliller, Çapraz Sorgu ve İspat, Ankara: Yayın Matbaacılık, 2008.

Petrovic, B., Kriminolojiye Giriş, AAB Yayını, Priştine, 2006.

Polat, H., Teori ve Uygulamada Cumhuriyet Savcısının El Kitabı, Adalet Yayınevi, Ankara 2009.

Sahiti, E., Adli Psikoloji, Priştine, 2007.

Sahiti, E., Murati, R., Ceza Muhakemesi Hakkı, Priştine, 2016.

Salihu, I., Zhitia, H., Hasani, F., *Kosova Cumhuriyeti Ceza Kanunu Hakkında Yorumlar*, I Baskı, Priştine 2014.

Sarsıkoğlu, Ş., Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı, TAAD, Sayı:22, 427-454, Temmuz 2015.

Say, K., "Data İncelemeleri", Oğuz Karakuş (ed.), Kriminalistik, Ankara: Adalet Yayınevi, 2. Baskı, 2013.

Selvi, O., Küçüksille, E. U., "Bulut Ortamında Adli Bilişim", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Eylül 2013, Ankara, 268-273, 2013.

Sevimli, A.G. Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar", İstanbul Barosu Dergisi, Cilt. 81, Sayı. 3, Mayıs-Haziran 2007, 993-1000, 2007.

Shala, A., Ceza Hukukuna Giriş, Priştine Yayınları 2019,

Shinder, D.J - Tittel, E., Scene of the Cybercrime: Computer Forensics Handbook, Syngress, 2007.

Shkembi, A., Arnavut ve Avrupa Mevzuatının Uyumlaştırılması, Yayın 1, Tiran 2015.

Sınar, H., İnternet ve Ceza Hukuku, İstanbul: Beta Yayınevi, 2001.

Sijerçiq – Çoliq, H., Haliloviq, H., Kosova Ceza Muhakemesi Usulü Özel İncelemeyle Ceza Muhakemesi Hakkı, Priştine, 2007.

Smibert, J., Principles of Evidence, ABD Adalet Bakanlığı, Priştina, 2014.

Sommer, P., DigitalEvidence, DigitalInvestigationsand E-Disclosure: A Guide toForensic Readiness forOrganisations, Security AdvisersandLawyers, 3. Edition, Information AssuranceAdvisoryCouncil, 2012, s. 30, https://cryptome.org/2014/03/digital-investigations.pdf, (Erişim tarihi: 07.03.2022).

Soyaslan, D., Ceza Muhakemesi Hukuku, Güncelleştirilmiş 8.Baskı, Yetkin Yayınları, Ankara 2020.

Soyaslan, D. Hukuka Aykırı Deliller, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi (AÜEHFD), Cilt. 7, Sayı. 3-4, 9-26, 2003.

Soysal, T., İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu, Türkiye Barolar Birliği Dergisi, Sayı. 61, Kasım-Aralık 2005, 304-339, 2005.

Şahin, C., "Telekomünikasyon Yoluyla İletişimin Denetlenmesi", Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XI, Sayı: 1-2, 1095-1112, 2007.

Şahin, C., "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme", Bilişim Hukuku Konferansı-YARGITAY, Ankara, 09-10 Ekim 2008, 123-135, 2008.

Şahin, C., Göktürk, N. Ceza Muhakemesi Hukuku Temel Hukuk Dizisi, 3. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Şahinkaya, Y., İnsan Hakları Avrupa Mahkemesi Kararlarında ve Türk Hukukunda Suçsuzluk Karinesi, Seçkin Yayınevi, Ankara 2008

Şen, B., Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller, Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt. 3, Ankara, 11 Ocak-15 Ocak 2010, 69-70, 2010.

Şen, E., "E-Posta Takibi", Terazi Hukuk Dergisi, Cilt. 9, Sayı. 97, Eylül 2014, 88-89, 2014.

Şen, E., Şüpheli veya Sanık İkrarının Delil Değeri, https://www.hukukihaber.net/supheli-veya-sanik-ikrarinin-delil-degeri-makale,6082.html, erişim tarih: 07.06.2022.

Şen, E. Türk Ceza Yargılaması Hukukunda Hukuka Aykırı Deliller Sorunu, 1. Baskı, İstanbul 1998.

Şen, O. N., "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, 35-41, 2005.

Şen, E., Yurttaş., Y., .Bilgisayar Programları Karşısında Özel Hayatın Korunması", Terazi Hukuk Dergisi, Cilt. 5, Sayı. 42, 29-44, 2010.

Şentürk, A., Bilgisayar Kullanımı ve İnternet. Ankara: Ekin Yayınevi, 2007.

Şirikçi, A.S., Cantürk, N., Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi", Bilişim Teknolojileri Dergisi, Cilt. 5, Sayı. 3, Eylül 2012, 29-34, 2012.

Tanrıkulu, C., Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma, Ankara: Adalet Yayınevi, 2014.

Topaloğlu, M., Özkişi, H., Tekkanat, E., Bulut Bilişim, Seçkin Yayınevi, Ankara 2017.

Toroslu, N., "Hukuka Aykırı Deliller Sorunu", Prof. Dr. Hamide Topçuoğlu'na Armağan, Ankara 1995

Toroslu, N., Feyzioğlu, M. Ceza Muhakemesi Hukuku, 21.Baskı, Savaş Yayınevi, Ankara 2021.

Tozman, Ö., "Suçsuzluk Karinesi: Türk Hukukundaki Sonuçları", EÜHFD, C. XI, S. 3-4, 315-353, 2007.

Trenova, G., Arnavutluk Ceza Muhakemesi Kanunu'nun Adli Yorumları, Dita Yayınları, Tiran 2009.

Turan, S. "Bulut Bilişim Teknolojisi ve Hukuki Problemler, https://www.keyofchange.com/tr/611/Bulut%20Bili%C5%9Fimi%20Teknolojisi%20ve%20Hukuki%20Problemler/, erişim tarihi: 26.03.2022.

Turan, M., Bilişim Hukuku, Seçkin Yayıncılık Ankara 2017.

Turhan, F., Ceza Muhakemesi Hukuku, Asil Yayınevi, Ankara 2006

Uğur, H., Suçların İhbarı ve İhbarcıların Korunması, TBB Dergisi, S.108, 386-406, 2013.

Uzunay, Y., Dijital Delil Araştırma Süreci, 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, 42-47, 2005.

Uzunay, Y., Bıçakçı, K., A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu. İstanbul, 9-11 Haziran 2005, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. Pdf, Erişim tarihi: 08.02.2022

Uzunay, Y., Koçak, M., Bilişim Suçları Kapsamında Dijital Deliller, AB'05 Akademik Bilişim Konferansı, Gaziantep, 31 Ocak - 4 Şubat 2005, https://9lib.net/article/teknolojik-ge%C3%A7erlili%C4%9Fin-denetlenmesi-elektronik-delilin-ge%C3%A7erlili%C4%9Finin-denetlenmesi.q7wx8xnd, Erişim tarihi: 08.02.2022.

Ünal, O.G., "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma", Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011.

Ünver, Y., Hakeri, H. Ceza Muhakemesi Hukuku Temel Bilgiler, 19.Baskı, Adalet Yayınevi, Ankara 2021.

Ünver, Y., Hakeri, H., Ceza Muhakemesi Hukuku C.3, Adalet Yayınevi, Ankara, 2019.

Vacca, J. R., Computer Forensics: Computer Crime Scene Investigation *[1st ed.]*, Charles River Media, 2002.

Veliqoti, L., Kriminoloji, Cilt I, Tiran 2015.

Verga, M. A., "Cloudburst: WhatDoes Computing MeantoLawyers?", Journal of Legal Technology Risk Management 5/1, , ss.41-49, 2010.

Westveer, A.E. *BehavioralScienceUnit, FBI,* ManagingDeathInvestigation, U.S. Department of Justice, Federal Bureau of Investigation, 1997.

Yarman-Vural, F.T., Erten, Y.M., Bilgisayar Sistemleri, 5. Baskı, Ankara: Akademi Yayıncılık, 2000.

Yapar, M.E. Amerika Birleşik Devletleri Federal Ceza Hukukunda PleaBargaining (İddia Pazarlığı) Kavramı Ve Uygulaması, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Konya 2012.

Yaşar, O., Yeni İçtihatlarla Uygulamalı e Yorumlu Ceza Muhakemesi Kanunu I. Cilt, 7. Baskı, Seçkin Yayıncılık, Ankara, Nisan 2017.

Yaşar, Y., Dursun, İ., Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri, MÜHF-HAD, C. 19, S. 3, s. 3-34, 2013.

Yavuz, M., Ceza Muhakemesinde İspat Sorunu, TAAD, S:9, 151-176, 2012.

Yayla, Y., İdare Hukuku, 2. Basım, İstanbul: Beta Yayınevi, 2010.

Yazıcıoğlu, Y. Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul: Alfa Yayınevi, 1997.

Yenidünya, C., Değirmenci, O., Mukayeseli Hukukta ve Türk Hukukunda Bilişm Suçları, İstanbul: Legal Yayıncılık, 2003

Yenisey, F., Nuhoğlu, A., Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Güncellenmiş 9.Baskı, Ankara 2021.

Yetim, S., "Dijital Kanıt Araştırma Yöntemleri". İstanbul Barosu Dergisi. Cilt. 82, Sayı. 3, Mayıs-Haziran 2008, 1201-1222, 2008.

Yıldız, A.K. “Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu”, Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, 253-264, 2006.

Ylli, G., Adli Tıp Uzmanının Ateşli Silah Yaralanmalarına Katkısı, "Justinian I" Bilimsel Dergisi, Sayı 1, Aralık 2009.

Yurtcan, E., Ceza Yargılaması Hukuku, 8. Baskı, Melisa Matbaacılık, İstanbul 2002