

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA MUHAKEMESİNDE DİJİTAL VERİLERİN
DELİL DEĞERİ**

YÜKSEK LİSANS TEZİ

ELİF GÖKŞEN

Tez Danışmanı: Doç. Dr. Ümit Kocasakal

Mayıs 2014

ÖNSÖZ

Bu çalışmada günümüzdeki hukuki gelişmeler kapsamında sıkça tartışılmakta olan dijital verilerin delil değeri incelenmektedir. Bu çalışma kapsamında dijital verilerin günümüz hukuk sistemlerindeki yadsınamaz etkisi belirtilmekle birlikte bu tür verilerin ceza muhakemesi kapsamında delil olarak değerlendirilmesi esnasında oldukça dikkatli davranılması gerekliliğinin, son derece kolay deforme edilebilmeleri ve aidiyetlerinin saptanamaması ihtimallerine dayanarak bu tür delilleri içeren hukuki kararların titizlikle incelenmesinin önemi belirtilmektedir.

Bu nevi tartışmalı ve gündemde olan bir konuyu detaylı olarak inceleyebilmek için öncelikle bilişim hukuku çerçevesinde genel bilgiler incelenecek olup ardından bu kapsamda veri kavramı tartışılacaktır. Çalışmanın ilerleyen kısmında dijital verinin elde edildiği dijital cihazlar incelenecek ve bu verilere ilişkin teknik ölçüm ve depolama bilgilerine değinilecektir.

Ardından, bu çalışma kapsamında ceza muhakemesinde deliller konusu incelenecek olup bu bağlamda ispat sorunu, delillerin özellikleri, delil türleri, dijital deliller ve hukuku aykırı deliller konuları incelenecektir. Böylece çalışmanın bir önceki bölümünde incelenen dijital cihazlardan elde edilen dijital verilerin ceza muhakemesinin delil sistemi içerisinde nerede yer alması gerektiği sorusuna yanıt bulunmaya çalışılmaktadır.

Çalışmanın son bölümlerinde dijital delillerin hazırlanarak sunulması konuları incelenmekte olup ayrıca dijital verilerin delil olarak nasıl değerlendirilecekleri sorusu ele alınmaktadır. Böylece gerek ulusal düzeyde gerekse yabancı hukuk sistemlerinde de güncel bir soru olan dijital verilerin delil değeri ulusal ve uluslararası standartlar kapsamında incelenmektedir.

Bu çalışmayı yürütürken bana her zaman destek olan değerli hocam Doç. Dr. Ümit Kocasakal'a ve görüşleriyle her zaman beni aydınlatan değerli hocam Prof. Dr. Köksal Bayraktar'a; benden desteğini ve zamanını esirgemeyen değerli hocam Yrd. Doç. Dr. Hakan Kızılarıslan'a; bana üreterek insanlığa faydalı olmayı öğreten sevgili annem Cumhuriyet Savcısı Sema Sonay Gökşen ve babam Özcan Gökşen'e ve mesafelere rağmen her zaman yanımda olduğunu bildiğim Seçkin Köstem'e teşekkür ederim.

***Elif Gökşen**
Nisan, 2014*

İÇİNDEKİLER

ÖNSÖZ.....	i
İÇİNDEKİLER.....	ii
ŞEKİL LİSTESİ.....	iv
KISALTMALAR.....	v
RÉSUMÉ.....	vi
ABSTRACT.....	xii
ÖZET.....	xviii
GİRİŞ.....	1
I-Bilişim hukukuna ilişkin genel bilgiler.....	2
A- Kavram ve Tanımlar.....	2
1- Bilişim Hukuku kapsamında yer alan temel terimler.....	2
2- Bilişim suçları açısından kavram ve terim tartışması.....	5
B- Bilişim yoluyla elde edilen veriler.....	8
1- Veri Kavramı.....	8
2- Dijital Veri Kavramı ve Bu Terime Seçenek Olarak Kullanılan Diğer Terimler.....	9
3- Dijital Veri ve Dijital Belge Kavramları.....	11
C- Dijital Verilere Erişebilmek Açısından Bilişim Sisteminde Kullanılan Cihazlar.....	17
1- Bilgisayar Sistemleri.....	18
2- Bilgisayarı oluşturan unsurlar.....	19
a- CPU (merkezi işlem birimi- central processing unit-mikro işlemci).....	20
b- Dahili bellek.....	21
i. RAM (random access memory- rastgele erişimli bellek).....	21
ii. ROM (read only memory- salt okunur bellek).....	22
c- Çevre Giriş (Input) – Çıkış (Output) Birimleri.....	23
3- El Bilgisayarları.....	23
4- Dijital Verilerin (Bilgilerin) Depolandığı Cihazlar.....	24
a- Hafıza Kartı.....	24
b- Cd/ Dvd ve Blu-Ray.....	25
c- Taşınabilir Bellek.....	26
d- Veri depolama cihazlarının hash değeri incelemesi.....	26
5- Dijital Kameralar, Dijital Fotoğraf Makinesi ve Mp3 Çalarlar.....	27
6- Yazıcı, Faks ve Fotokopi Makineleri.....	28
7- Cep Telefonları.....	29
8- İnternet Sistemleri.....	29
a- İnternet tarihi gelişimi.....	29
b- İnternetin teknik yapısı.....	31
II- Türk Ceza Muhakemesi Açısından Deliller.....	33
A- Genel Olarak.....	33
B- Türk Ceza Muhakemesinde İspat Sorunu ve Deliller.....	35
1- Temel İlkeler.....	37
2- Delillerin Özellikleri.....	38
a- Deliller gerçekçi olmalıdır.....	38
b- Deliller akılcı olmalıdır.....	38
c- Deliller olayı temsil edici olmalıdır.....	39
d- Deliller ispat bakımından önemli olmalıdır.....	39
e- Deliller hukuka uygun olmalıdır.....	40
f- Deliller müşterek olmalıdır.....	41

3- Delil Türleri.....	41
a- Beyan Delilleri.....	44
i. Tanık beyanı	45
ii. Şüpheli veya sanık beyanı.....	48
iii. Şüpheli veya sanık dışında kalan tarafların beyanı.....	50
b- Belge Delilleri.....	50
i. Yazılı belgeler.....	51
ii. Şekil tespit eden belgeler.....	52
iii. Ses ve/veya görüntü tespit eden belgeler.....	52
c- Belirti delilleri ve bilimsel deliller.....	54
d- Maddi delil-Bilimsel delil.....	55
4- Dijital Deliller.....	57
a- Dijital delil kavramı.....	57
b- Dijital delillerin özellikleri ve diğer delillerden farkları.....	58
c- Dijital deliller kapsamında adli bilişim alanı.....	60
d- Dijital delillerin delil türleri arasındaki yeri.....	64
C- Türk Ceza Muhakemesinde Hukuka Aykırı Deliller.....	64
1- Kavram ve Genel İlkeler.....	65
2- Hukuka Aykırı Delillerin Değerlendirilmesi.....	67
3- Yargıtay Kararları Kapsamında Hukuka Aykırı Deliller.....	72
4- AİHM Kararları Kapsamında Hukuka Aykırı Deliller.....	78
III-Ceza Yargılamasında Dijital Delillerin Hazırlanması ve Sunulması.....	80
A- Dijital Delillerin İncelemeye Hazırlanması.....	81
B- Dijital Delillerin İncelenmesi.....	83
C- Dijital Delillerin Analiz Edilmesi.....	85
D-Dijital Delillere İlişkin Düzenlenen Raporların Sunulması ve Delillerin İbrazı.....	87
IV-Bilişim Yoluyla Elde Edilen Verilerin Delil Olarak Değerlendirilmesi.....	89
A-Ceza Muhakemesi Çerçevesinde Dijital Delillerin Kabul Edilebilirliği Meselesi.....	89
B-Dijital Delillerin Doğrulanması ve Dijital Delillere İlişkin Hukuki Kurallar....	93
1- Türk Ceza Muhakemesi Kapsamında Bilgisayar Aramalarına İlişkin Kurallar.....	94
a- CMK 134. maddenin incelenmesi.....	94
b- AİHM'in bilgisayar aramalarına ilişkin kararları.....	101
c- Bilgisayarlarda yapılacak aramalar sonucu elde edilecek tesadüfi deliller.....	103
d- CMK 134. madde kapsamında getirilen hukuki düzenlemeye aykırılık.....	105
2- Yabancı Hukuk Sistemlerinde Dijital Delillere İlişkin Kurallar.....	107
3- Dijital Delillere İlişkin Uluslararası Kurallar.....	109
C-Türk Ceza Muhakemesi Kapsamında Dijital Delillerin Değerlendirilmesi.....	111
1- Genel Olarak.....	111
2- Hukuk Muhakemesi Kapsamında Dijital Delillerin Değerlendirilmesi.....	111
3- Ceza Muhakemesi Kapsamında Dijital Delillerin Değerlendirilmesi.....	112
V- Dijital Delillerin Değerlendirilmesi Konusunda Alınması Gereken Önlemler.....	121
SONUÇ.....	125
KAYNAKÇA.....	126
EKLER.....	133
ÖZGEÇMİŞ.....	185

ŞEKİL LİSTESİ

Şekil-1- CPU (Merkezi İşlemci Birimi-Central Processing Unit-Micro İşlemci).....	20
Şekil-2- RAM.....	21
Şekil-3- ROM.....	22
Şekil-4- Çevre Giriş- Çıkış (Input-Output) Birimleri.....	23
Şekil-5- El Bilgisayarı.....	23
Şekil-6- Hafıza Kartı.....	24
Şekil-7- Cd/Dvd ve Blu-Ray.....	25
Şekil-8- Taşınabilir Bellek.....	26
Şekil-9- Dijital Kameralar.....	27
Şekil-10- Yazıcı, Faks ve Fotokopi Makineleri.....	28
Şekil-11- Cep Telefonu.....	29

KISALTMALAR

a.g.e.	: adı geçen eser
ABD	: Amerika Birleşik Devletleri
ACPO	: The Association of Chief Police Officers
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
ARPA	: Advanced Research Project Agency
bkz.	: bakınız
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CMK	: Ceza Muhakemesi Kanunu
CMUK	: Ceza Muhakemeleri Usuli Kanunu
FRE	: Federal Rules of Evidence
HMK	: Hukuk Muhakemesi Kanunu
HTML	: Hypertext Markup Language
IACIS	: International Association of Computer Investigative Specialist
ISP	: Internet Service Provider –İnternet Servis Sağlayıcısı
s.	: sayfa
ss.	: sayfadan sayfaya
TCK	: Türk Ceza Kanunu
TCP/ IP	: Transfer Code Protocol/ Internet Protocol
TDK	: Türk Dil Kurumu
TÜBİTAK	: Türkiye Bilimsel ve Teknik Araştırma Kurumu

RÉSUMÉ

Avec l'évolution des technologies, de nouvelles branches sont apparues dans le système juridique, en particulier le droit de la technologie de l'information. Le domaine des technologies de l'information constitue l'un des points les plus apparents de convergence entre la technologie et le droit, et à l'heure actuelle, il continue à se développer. Une des questions principales à l'origine de la présente analyse est de savoir comment des données acquises grâce à la technologie peuvent être appréhendées en termes de droit pénal.

La preuve est une question qui a été fréquemment étudiée dans le contexte de la procédure pénale et la question de la preuve fait l'objet de chapitres fondamentaux de manuels juridiques de procédure pénale. L'objectif principal en procédure pénale est d'atteindre au fait matériel. C'est pour cela qu'en procédure pénale, on cherche à trouver la réponse à la question : «Que s'est-il vraiment passé ?». Selon la réponse obtenue, des individus peuvent passer le reste de leur vie privés de liberté, tandis que leur vie et leur dignité ainsi que celles de leurs familles pourront être gravement compromises dans la société dont ils font partie.

Par conséquent, la question de l'utilisation de données numériques en guise de preuve et de leur évaluation du point de vue de la procédure pénale revêt une grande importance dans la théorie comme dans la pratique, en particulier dès lors que la technologie simplifie tous les aspects de la vie quotidienne et que tout un chacun l'utilise. Au-delà des avantages que cela représente, des problèmes techniques peuvent se présenter pour identifier à qui appartiennent certaines données et les caractéristiques de ces données peuvent être changées facilement. Lorsque ce genre de données constitue la base d'une décision juridique, cela peut être à l'origine de problèmes d'envergure dans la recherche du fait matériel dans la procédure pénale.

L'atteinte au principe de détermination du fait matériel a pour conséquence non seulement la violation d'un principe juridique, mais peut aussi compromettre la confiance à l'égard du système juridique dans la société. Finalement, si ce sentiment de confiance, qui est un lien essentiel entre le système judiciaire et la société, disparaît, cela peut donner lieu à la disparition des sentiments d'équité et de justice.

Pour répondre à la question du comment s'évaluent les données numériques en procédure pénale, la présente étude examinera d'abord la place du droit des

technologies de l'information dans la structure juridique générale en tentant d'expliquer certains concepts. Parce que la présente étude examine l'évaluation des données numériques obtenues par le biais d'appareils numériques, elle commencera en abordant des questions techniques touchant au concept de données, données numériques, appareils numériques collectant des données numériques, systèmes informatiques, composants d'ordinateurs, systèmes et applications internet, structure technique de l'internet et son histoire, appareils de stockage de données et valeur de hachage de ces appareils. Dans cette première partie, il s'agira de donner un aperçu de l'état de la technique avant de pouvoir faire le lien entre données numériques et procédure pénale.

La seconde partie de cette étude examine la question de la preuve dans le contexte de la procédure pénale. Tout d'abord, elle se réfère aux principes généraux de la procédure pénale. Ensuite, elle examine le principe de détermination du fait matériel et la question des preuves illégales en tant que limite à ce principe. En effet, en procédure pénale, l'idée d'atteindre l'élément matériel à tout prix est rejetée.

La question de la preuve dans le cadre de la procédure pénale sera examinée ensuite. L'examen de cette question fait le lien entre les principes généraux de la procédure pénale et la preuve, qui résulte des éléments que le système juridique considère comme probants. En procédure pénale, pour faire la preuve, il ne suffit pas d'obtenir la confiance du juge, il faut le convaincre. Tant que le juge n'est pas complètement convaincu, le principe *in dubio pro reo* prévaut.

Dans le cadre de ces principes généraux, la doctrine a élaboré certaines caractéristiques des éléments de preuve. Ils doivent être réalistes, fluides, ressembler à l'incident, être plausibles en tant que preuves, s'intégrer et surtout être légaux. La légalité des éléments de preuve est protégée par la Constitution : selon son article 38/6, les constatations recueillies illégalement ne peuvent être utilisées comme preuve.

Pour pouvoir placer les preuves numériques dans le système général de la preuve, il nous faut examiner le type de preuves utilisées dans le contexte de la procédure pénale. Pour trouver une place à la preuve numérique parmi les différents types de preuves, les preuves documentaires et les preuves matérielles scientifiques peuvent être d'importance. Après avoir été présentées au juge, les preuves

numériques peuvent être évaluées en tant que preuves documentaires, comme tout document déterminé par le son ou la vue. Pour les preuves documentaires, la question de la propriété est d'importance. En dépit d'avis contraire en doctrine, il est souligné par le Code Pénal Turc que le propriétaire d'un document doit être identifié.

Mais aussi, durant la procédure judiciaire, les preuves numériques peuvent être utilisées en tant que preuves scientifiques. Les preuves scientifiques sont les preuves qui sont obtenues dans le respect des règles et méthodes d'une discipline scientifique donnée. Par exemple, la preuve obtenue par analyse de l'ADN est une preuve scientifique. Bien que le juge se doive de prendre ce type de preuves en considération pendant la procédure et lors du verdict, elles peuvent ne pas être objectives, bien qu'obtenues scientifiquement. C'est pour quoi le juge se doit d'évaluer la valeur des preuves scientifiques. L'approbation automatique d'une preuve scientifique, même si la confession de l'accusé n'est pas considérée comme ayant force contraignante, violera les principes fondamentaux de la procédure pénale que nous essayons d'expliquer dans cette étude. Dans le cadre de cet examen par le juge, il faut examiner la validité et la fiabilité des données scientifiques invoquées et si elles sont applicables à l'espèce. Il est du ressort du juge de trouver une solution après avoir évalué ce type de recherches.

L'on essaye à l'heure actuelle de trouver une place pour les preuves numériques dans le système de la preuve. Toutefois, parce que la technologie est utilisée dans presque tous les aspects de la vie quotidienne et que ce type de données probantes aide à l'éclaircissement de beaucoup de situations, on les examine en fonction de leurs caractéristiques propres, sans discrimination doctrinale. Les preuves numériques sont définies comme de l'information stockée numériquement ou transmise numériquement qui a valeur probante. On peut les voir comme étant des preuves matérielles : toutefois, elles sont moins concrètes que d'autres preuves matérielles telles que l'analyse d'ADN ou l'analyse balistique et elles présentent plusieurs caractéristiques qui les rendent différentes des autres preuves.

On peut utiliser divers appareils pour visualiser les preuves numériques. Ainsi, pour qu'une donnée numérique soit vue en tant que preuve numérique, l'on doit examiner le système numérique dans lequel elle se trouve intégrée, car les preuves numériques sont plus fragiles que les preuves non numériques : on peut facilement les modifier ou les endommager. Une autre caractéristique des données numériques

est la possibilité de leur disparition. Contrairement à d'autres types de preuves, il est impossible de facilement les détruire, il ne suffit pas de les effacer du système numérique où elles se trouvent. Si bon nombre de systèmes font des copies de sauvegarde de leurs données, parfois l'on devra utiliser un programme spécial pour un simple effacement.

À cause des différences entre preuves numériques et autres types de preuves, il est clair que l'on doit les examiner de façon particulière. C'est pour cela que les preuves numériques sont examinées dans la sous-catégorie de l'investigation numérique. Pour la preuve numérique, l'investigation numérique représente une application de l'utilisation de techniques d'analyse informatique. Les preuves numériques doivent être présentées au juge séparées de leur média.

Donc, la préparation et la présentation des preuves numériques constituent une étape séparée dans la discipline de l'investigation numérique (digital forensics) . Dans la troisième partie de notre étude, la préparation des preuves numériques sera examinée. Dans ce contexte, les preuves digitales doivent d'abord être saisies, puis examinées et enfin elles devront être analysées après l'examen du système informatique lui-même,. Partant des résultats de l'analyse, un rapport sera préparé et présenté au juge.

Tout d'abord, il faut une saisie des données numériques qui seront utilisées comme preuve. Lors de la saisie, les appareils numériques contenant des données numériques doivent être adaptés. Parfois, dans le cadre d'un élément d'un cas spécifique, tous les appareils numériques doivent être saisis. Mais dans d'autres cas, l'analyse peut être faite avec une copie issue des appareils numériques.

Après la saisie, l'évaluation se fait selon les règles locales de chaque pays. Durant cette étape, un premier examen est effectué pour trouver une cause probable justifiant la saisie des appareils numériques. Alternativement, une image des données numériques est prise après la constitution de l'aperçu. Avec cette méthode, un «instantané» de l'appareil numérique peut être obtenu aumoment de la sauvegarde.

L'évaluation se divise elle-même en plusieurs éléments. L'un d'eux est le besoin de protéger la sécurité et la fiabilité des données qui seront utilisées comme données numériques, comme sur la scène d'un crime. Lors de cette étape, l'utilisation de méthodes qui préviennent l'échange de données pourrait aider à

sécuriser les données. La protection de données numériques est très importante pour leur présentation au juge.

Lors de l'étape de l'analyse des preuves numériques, on essaiera de déterminer si les données pouvant être utilisées comme données numériques prouvent les faits liés au procès, si les données confirment ce qui est connu à propos de l'affaire, et si ces données peuvent être qualifiées de preuves ou de début de preuve. Le savoir et l'expérience du responsable de l'analyse des données numériques sont importants ici. Parce que la saisie des données n'est pas suffisante dans le cadre de la procédure pénale, le propriétaire de l'appareil numérique qui contient les données numériques touchant au procès doit avoir connaissance de ces données.

Le code pénal turc appliquant le principe de la preuve circonstancielle, le problème de l'admissibilité de la preuve numérique ne constitue pas un problème pour le système judiciaire turc. Dans notre système judiciaire, les limites du principe de la preuve circonstancielle sont les preuves illégales. Dans cette limite, pour détecter l'illégalité aux stades de saisie des données numériques, de leur évaluation et analyse, elles ne devraient pas être considérées comme relevant des preuves interdites.

Pour pouvoir utiliser les preuves numériques en procédure pénale, elles doivent être authentifiées. Dans certains systèmes juridiques étrangers, ce système d'authentification garantit que les preuves numériques, fragiles et facilement modifiables, restent authentiques lors de leur évaluation.

Plusieurs éléments peuvent être trouvés dans la doctrine concernant ce système d'authentification. Malheureusement, contrairement aux systèmes judiciaires étrangers, il n'y a pas de réglementation sur la question en Turquie. Toutefois, en ce qui concerne l'examen juridique des données numériques, l'article 134 du Code de procédure pénale est important. Cet article dit dans quelles situations et conditions un ordinateur peut être examiné. Selon nous, les données numériques contraires à l'article 134 et obtenues parce que des précautions de sécurité n'ont pas été respectées, devraient être considérées comme illégales.

Avec l'importance croissante des preuves numériques, plusieurs règles d'examen et d'évaluation sont en train d'être développées au niveau national comme au niveau international. Toutefois, en dehors de ces règles, si l'on examine les

décisions judiciaires turques, on peut observer que - malgré la nature fragile et douteuse/incertaine des preuves numériques - elles sont considérées comme suffisant à fonder une condamnation à des peines de prison. C'est un fait que plusieurs juridictions ont commencé à considérer les preuves numériques comme de puissants instruments de preuve. Toutefois, le débat le plus important ne touche à la force des preuves numériques, mais à leur fiabilité. Dans certains systèmes juridiques, des principes détaillés ont été établis tout d'abord pour assurer leur fiabilité, mais aussi pour la protection du prestige des officiers de police, qui sont les premiers à manipuler toutes sortes de preuves,. Le problème principal en procédure pénale turque est que, malgré l'absence de principes pour l'utilisation des preuves numériques, les données numériques sont tout de même utilisées dans certains verdicts, par exemple d'emprisonnement, qui peuvent avoir de lourdes conséquences pour les droits fondamentaux.

La transparence nécessaire à l'utilisation des données numériques n'est pas atteinte. Selon nous, pour préserver une certaine confiance pour le système judiciaire, les preuves numériques ne devraient pas être considérées comme suffisantes pour condamner à la prison, au moins tant que cette transparence ne sera pas assurée.

Mot-clés:	Procédure Pénale, Preuve, Données Numeriques, Preuves Numeriques
------------------	---

ABSTRACT

As a result of technological advancements, there have emerged new directions within the legal system and hence arisen information technology law. The area of information technology constitutes one of the most apparent points of convergence between technology and law, and currently it is still developing. One of the main questions which gave birth to this study is the question of how technologically acquired data shall be assessed in terms of criminal law.

Evidence has been an issue that is frequently studied within the boundaries of criminal procedure law and evidences have constituted fundamental chapters of legal books, which deal with criminal procedure. The main question on criminal procedure is reaching the material fact. It is for this reason that in criminal procedure, one seeks to find an answer for this question; “what happened actually?”. Depending on the answer given to this fundamental question, while individuals may spend a lifetime deprived of their freedoms, the dignity of themselves and their families might be significantly damaged in front of the society that they are a part of.

Therefore, the questions of whether digital data can be used as legal evidence and how these kinds of evidence will be assessed in terms of criminal procedure law have utmost importance not only theoretically but also practically. This is especially the case because technology simplifies each and every aspect of daily lives and almost every member of the society uses it. Apart from its practical benefits for daily lives, there can emerge technical problems in identifying belongings of this kind of data and these data can be changed easily. If digital data which possesses these features constitute the basis of legal decisions on their owns, this can lead to significant problems for the principle of reaching the material fact in terms of criminal procedure law. The damage given to the principle of reaching the material fact not only results in the infringement of a legal principle, but also causes significant harm to the trust for the legal system in the society. Finally, if this feeling of trust, which constitutes one very significant bond between the society and the legal system, is destructed, this might lead to the disappearance of the social feeling of fairness and justice.

In order to find an answer for the question of how digital data is assessed in criminal procedure, this study first examines the place of information technology law

within the general legal structure, and tries to explain several main concepts. Because this study investigates the assessment of digital data that are acquired through digital devices, at the beginning it examines technical issues such as the concept of data, digital data, digital devices through which digital data are acquired, computer systems, components of computers, internet systems, technical structure of the internet and its history, data storage devices, and the hash value of these storage devices. At this initial stage, it was aimed to provide a technical overview before establishing a link between digital data and criminal procedure.

The second part of this study examines the issue of evidences in terms of criminal procedure law. Firstly, it touches upon the general principles of criminal procedure. It examines the principle of reaching the material fact, and touches upon illegal evidences as the boundary for this principle. This is because in criminal procedure, the idea of reaching the material fact at all costs is rejected.

Then, the question of proof within the scope of criminal procedure is examined. The examination of the question of proof connects the general principles of criminal procedure with evidences. Because, evidence refers to the instruments that are useful for proof and are acknowledged by the legal system. In criminal procedure, in order to provide proof, it is not sufficient to make the judge believe; it is a must to have a full persuasion of the judge. For this reason, until there is a full persuasion on the side of the judge, the principle of *in dubio pro reo* prevails.

Within the framework of these general principles several features have been developed in the doctrine regarding evidences. Evidences must be realistic, fluent, resembling the incident, significant in terms of proof, aggregative and most importantly lawful. Lawfulness of evidences is protected under the Constitution as well. According to 38/6 of the Constitution findings acquired illegally cannot be accepted as evidence.

In order to be able to place digital evidences within the general system of evidence, we need to examine the types of evidence that are dealt with within the scope of criminal procedure. From the point of finding a place for digital evidences within types of evidence, documental evidences and material-scientific evidences have significance. After being presented at the court, digital evidences can be evaluated as documental evidence just like documents that determines sound and/or

vision. In terms of documental evidence, the issue of belonging is highly significant. Despite the presence of views in the doctrine, it is underlined in Turkish Criminal Code article preamble that the belonging of the document shall be identified.

On the other hand, during the trial process digital evidences can be used as scientific evidence as well. Scientific evidence refers to the type of evidence that is acquired in accordance with the rules and methods of a scientific discipline. Evidence acquired through DNA analysis is a typical example of scientific evidence. The judge has to take into consideration this type of evidences during trial and verdict phases, but this type of evidences may not be objective albeit acquired scientifically. For this reason, the court must assess the health of scientific evidences. The automatic approval of scientific evidence, even when the confession of the accused is not accepted as binding, is going to be against the fundamental principles of criminal procedures that we try to explain throughout this study. Within the scope of this examination of the court, one must examine the validity and reliability of scientific evidences and whether they are suitable to be applied for the current incidence. It is within the judge's discretion to come to a solution after evaluating this type of research.

Digital evidences are tried to be placed under a heading within the present system of evidence. However, because technology is used in almost all areas of daily lives and these kinds of evidences are helpful to set light upon many incidences, they are examined in their owns without being subjected to any doctrinal discrimination.

Digital evidences are defined as information that is digitally stored or transmitted that has the capacity for proof. They can be seen as a type of material evidences; however, they are less concrete compared to other material evidences such as DNA examples and ballistic investigations and they contain several features that make them different from other evidences.

One can utilize many different devices in the visualization of digital evidences. Therefore, in order for a digital datum to be assessed as digital evidence, one must examine the entire digital system within which the datum is located. This is necessary because digital evidences have more delicate features compared to other evidences; they can be damaged and changed easily. Another characteristic of digital evidences is the possibility of their disappearance. Unlike other types of evidence, it is impossible to destroy them easily; it is not sufficient to delete digital data from the

digital system. While many digital systems back-up digital data, sometimes one might even need special software programs for a simple process of deletion.

Because of the different characteristics of digital evidences from the other types of evidences, it is obvious that they need to be examined specifically. That is why the digital evidences are examined under the sub category of digital forensic. From the point of digital evidence, digital forensic can be defined as an application of the usage of computer analysis techniques. Digital evidences have to be presented in the court by separating from the digital media.

Thus, the preparation and presentation of digital evidences constitute a separate stage in the digital forensic discipline. In the third part of our study, the preparation of digital evidences is examined. In this context, digital evidences must firstly be seized, then examined and after the information system examination, they must be analysed. In accordance with the consideration at the last stage, a report needs to be prepared and it has to be presented in the court.

First of all, the digital data, which will be used as the digital evidence, need to be seized. On the stage of seizing, digital devices, which contain digital data must be appropriated. Sometimes within the scope of the characteristic of concrete case, all the digital devices may be seized. But some other times, the analysis may be done with a copy coming from the digital devices.

After the accomplishment of the seizure stage, in the examination stage each country deals with this issue in accordance with its own legal regulations. Under this stage, at first basically a preview will be done. Within the scope of the preview a “probable cause” which will help to legally seize the device, must be achieved. As another method, an image of the digital data are taken after the preview. With this method, the snapshot of the digital device can be obtained in the time of back up.

Examination stage consists of different elements. One of them is the necessity to protect security and reliability of the data, which will be used as digital evidence, just like a crime scene. In this stage, the usage of methods which prevent the change on the data would help to achieve security. The protection of digital data is extremely important for their representation in the courts.

In the stage of the analysis of digital evidences, answers are tried to be found as to whether the data which will be used as digital evidence during the analysis stage prove the facts related to the trial, whether data obtained verify what is known about the trial, and whether these data qualify as proof or beginning of proof. The knowledge and experience of the information technology specialist who will conduct this analysis, is quite important. Because the seizure of a data is not enough at all, the owner of the digital device which holds the digital data should be aware of that particular data.

As the fact that Turkish Criminal Procedure system applies the principle of circumstantial evidence, the problem of admissibility of digital evidence does not constitute an issue for Turkish legal system. In our legal system, the boundaries of the principle of circumstantial evidence is driven by the illegal evidences. Within this scope, in the case of the determinations of unlawfulness in the stages of seizure of digital evidences, their examination and analysis, they should not be considered within the frame of forbidden evidences.

In order to use digital evidences in the criminal procedure, they should be verified. In foreign legal systems the verification process, which is used to determine the validity of digital evidences, ensures to prove that fragile and easily changeable digital evidences remain original during the examination stage.

Various principle can be found in the doctrine about the verification process of digital evidences. Unfortunately, unlike foreign legal systems, there is not regulated principles on this issue. However, in terms of legal examination of digital data, article 134 of Turkish Criminal Procedure Code is quite important. This article regulates under which situations and conditions a computer can be examined. According to our view, digital evidences which contradict with article 134 and which are formed because necessary security precautions are not taken, should be considered as illegal evidence.

With the enhanced importance of digital evidences, various examinations and consideration principles are being developed at both national and international levels. However, separately from these principles, when the Turkish case decisions are examined, despite the fragile and suspicious character of digital evidences, we see that they are considered alone enough for an imprisonment sentence. It is a

reality that different types of jurisdictions started to consider digital evidences as powerful proof tools. However, the most important discussion is not about the power of digital evidences, it is about their reliability. Under some legal systems, first of all in order to establish the reliability and more importantly, to protect the prestige of police officers, who are dealing first all kinds of evidence in the first instance, detailed principles are established. The main problem in Turkish Criminal Procedure is that, without developing some principles on the usage of digital evidences, digital data are considered as the basis of some court decision which can cause important results in terms of human rights, such as imprisonment sentences.

The necessary transparency is not being achieved for digital evidences. According to our view, in order to maintain the confidence towards the legal system, digital evidences should not be considered alone for an imprisonment sentence, until this transparency will be obtained.

Key Words:	Criminal Procedure, Evidences, Digital Data, Digital Evidence
-------------------	--

ÖZET

Gelişen teknolojik ilerlemelerle hukuk sistemi içerisinde yeni arayışlar oluşmuş ve bu kapsamda bilişim hukuku alanı ortaya çıkmıştır. Bilişim hukuku alanı teknoloji ve hukukun en belirgin kesişme noktalarından birini oluşturmaktadır ve günümüzde hala gelişmekte olan alanlardan biridir. Bilişim yoluyla elde edilen verilerin hukuk sistemi içerisinde ceza hukuku açısından nasıl değerlendirilecekleri ise bu çalışmanın başlamasına sebep olan temel sorulardan biridir.

Ceza muhakemesi kapsamında deliller ise çeşitli defa çalışmalara konu olmuş, temel ceza muhakemesi kitaplarının önemli bölümlerini oluşturmuşlardır. Ceza muhakemesinde temel sorun maddi gerçeğin bulunmasıdır. Bu sebeple muhakeme kapsamında “Gerçekte ne olmuştu?” sorusuna cevap aranır. İnsanlar bu sorunun cevabıyla tüm hayatlarını özgürlüklerinden yoksun geçirebilecekleri gibi kendilerinin ve ailelerinin itibarları da toplum önünde ciddi oranda zedelenecektir.

Bu sebeple bilişim yoluyla elde edilen dijital verilerin dijital delil olarak kabul edilip edilmemeleri, bu tür delillerin ceza muhakemesi açısından nasıl değerlendirilecekleri yalnızca teorik değil pratik hayatta da büyük bir öneme sahiptir. Zira teknoloji gündelik yaşamın her alanında hayatı kolaylaştırmakta ve hemen hemen herkes tarafından kullanılmaktadır. Günlük hayattaki pratik faydaları bir kenara bırakılırsa, hukuki açıdan bu tür verilerin aidiyetlerinin saptanması konusundan teknik problemlerle karşılaşılabilenekte ayrıca bu tür veriler kolayca değiştirilebilmektedir. Bu özellikleri haiz dijital verilerin ceza muhakemesi kapsamında yargı kararlarına tek başlarına esas teşkil edilmeleri, ceza muhakemesinin gerçeği bulma ilkesine aykırı sonuçlar doğurabilmektedir. Gerçeği bulma ilkesinin zedelenmesi yalnızca bir hukuki ilkenin çiğnendiği anlamına gelmemekte aksine hukuka duyulan güvenin yıkılmaya yüz tutması anlamına gelmektedir. Toplum ve hukuk arasındaki önemli bağlardan biri olan bu soyut güven duygusunun yıkılması ise bir ülkede yaşayan bireylerin her koşul altında başvuracakları hakkaniyet ve adalet kavramlarının yok olmasına sebep olmaktadır.

Dijital verilerin ceza muhakemesinde nasıl değerlendirildiği sorusuna bir cevap bulabilmek için öncelikle bilişim hukukunun genel hukuki yapıdaki yeri incelenmiş, bu kapsamda bir takım temel kavramlar açıklanmaya çalışılmıştır. Çalışma boyunca dijital cihazlardan elde edilen dijital verilerin ceza muhakemesi açısından ele

alınması incelendiği için, çalışmanın en başında veri kavramı, dijital veri kavramı, dijital verilerin elde edildiği çeşitli dijital cihazlar, bu kapsamda bilgisayar sistemleri, bilgisayarı oluşturan unsurlar, internet sistemleri, internetin teknik yapılanması ve tarihçesi, veri depolama cihazları ve bu tür depolama cihazlarının hash değeri incelemesi gibi teknik konular incelenmiştir. Bu aşamada dijital veriler ile ceza muhakemesi arasındaki bağ kurulmadan önce teknik bir genel görünüm sağlanmaya çalışılmıştır.

Çalışmanın ikinci bölümünde ise ceza muhakemesi açısından deliller konusu incelenmiştir. Öncelikle bu aşamada ceza muhakemesinin genel ilkelerine yer verilmiştir. Maddi gerçeğin araştırılması ilkesi incelenmiş ve bu ilkenin sınırı olan delil yasaklarına değinilmiştir. Zira ceza muhakemesinde ne pahasına olursa olsun gerçeğin bulunması anlayışı reddedilmiştir.

Ardından ceza muhakemesi kapsamında ispat sorunu ele alınmıştır. İspat sorununun incelenmesi ceza muhakemesinin genel prensipleri ile delilleri birbirine bağlamaktadır. Zira, ispata yarayan ve hukuk düzeninin kabul ettiği vasıtalarla delil denilmektedir. Ceza muhakemesinde ispatın sağlanabilmesi için hakimi inandırmak yeterli değildir, hakimde tam bir kanaat oluşmalıdır. Bu sebeple hakim tam bir kanaate ulaşana kadar şüpheden sanık yararlanır ilkesi uygulanacaktır. Ceza muhakemesi kapsamında sıkça dile getirilen vicdani delil sistemi de şüpheden sanık yararlanır ilkesinin bir sonucu olarak karşımıza çıkmaktadır. Günümüzde henüz tam anlamıyla bilimsel delil sistemine geçilmemiş olup, vicdani delil sistemi kapsamında delillerin serbestliği ve delillerin serbest değerlendirilmesi ilkeleri çerçevesinde hakimde tam bir kanaat oluşana kadar şüpheden sanık yararlanacaktır.

Bu temel ilkeler doğrultusunda doktrinde delillere ilişkin bir takım özellikler geliştirilmiştir. Deliller gerçekçi olmalıdır, akılcı olmalıdır, olayı temsil edici olmalıdır, ispat bakımından önemli olmalıdır, müşterek olmalıdır ve en önemlisi deliller hukuka uygun olmalıdır. Delillerin hukuka uygunluğu Anayasa tarafından da güvence altına alınmıştır. Anayasanın 38/6'ya göre hukuka aykırı olarak elde edilmiş bulgular delil olarak kabul edilemez.

Dijital delilleri ceza muhakemesinin genel delil sistemi içerisine yerleştirebilmek için ceza muhakemesi kapsamında ele alınan delil türlerini incelemek gerekmektedir. Delil türleri arasında dijital delillere bir yer bulabilmek

açısından belge delilleri ve maddi-bilimsel deliller önem taşımaktadır. Zira, dijital deliller mahkemeye sunulduktan sonra ses ve/veya görüntü tespit eden belgelerde olduğu gibi, belge delili olarak değerlendirilebilmektedirler. Belge delilleri açısından aidiyet sorunu önem taşımaktadır. Doktrinde belge delillerinin anonim olabileceği konusunda görüşlerin bulunmasına rağmen Türk Ceza Kanunu'nun madde gerekçesinde belgenin kime ait olduğunun belirlenebilmesinin altı çizilmiştir.

Öte yandan muhakeme aşamasında dijital deliller bilimsel delil olarak da incelenebilmektedir. Bilimsel deliller belirli bir bilim dalının kural ve yöntemlerine göre elde edilen delillere denilmektedir. DNA analizleri sonucu elde edilen deliller bilimsel delillerin tipik bir örneğini oluşturmaktadır. Hakim bu tür delilleri yargılama ve hüküm sırasında dikkate almak zorundadır ancak bu tür deliller her ne kadar bilimsel yöntemler kullanılarak elde edilmiş olmalarına karşın objektif olmayabilirler. Bu sebeple bilimsel delilleri sıhhati mahkemece araştırılmalıdır. Sanığın ikrarının bile bağlayıcı olmadığı ceza muhakemesinde bilimsel delillere verilecek olan otomatik onay çalışmamız boyunca açıklamaya çalıştığımız ceza muhakemesinin temel ilkelerine aykırılık oluşturacaktır. Mahkemece yapılması gereken bu araştırma kapsamında bilimsel delillerin doğruluğu ve güvenilirliği ile mevcut olaya uygulanıp uygulanmayacağı incelenmelidir. Bu araştırmaları değerlendirip bir kanaate varmak hakimnin takdirindedir.

Dijital deliller mevcut delil sistemi içerisinde bir başlığa yerleştirilmeye çalışılmaktadır. Ancak teknolojinin gündelik hayatın her alanında faaliyet göstermesi ve bu tür delillerin birçok olay bakımından aydınlatıcı özelliklerinin yadsınamaması sebebiyle bir doktrinel ayrıma tabi tutulmadan başlı başına incelenmektedir. Dijital deliller dijital formda depolanan ya da iletilen ispat gücüne sahip bilgiler olarak tanımlanabilmektedir. Maddi delillerin bir türü olarak değerlendirilebilirler ancak DNA örnekleri ve silah incelemeleri gibi diğer maddi delillere kıyasla daha az somut niteliktedirler ve diğer delillerden farklı bir takım özellikler içermektedirler.

Dijital delillerin görüntülenmesinde birçok farklı cihazdan faydalanılabilmektedir. Bu sebeple bir dijital verinin dijital delil niteliğinde değerlendirilebilmesi için içinde bulunduğu tüm dijital sistemin incelenmesi gerekmektedir. Zira dijital deliller, diğer delillere kıyasla daha hassas özelliklere sahiptirler, kolay tahrip edilebilirler, kolayca değiştirilebilirler. Dijital delillerin bir diğer özelliği ise zor yok olmalarıdır. Diğer deliller gibi kolay yollarla imhaları

mümkünken bu tür delillerin bulundukları dijital sistemden silinmesi yeterli gelmez. Çoğu sistem verileri yedeklemekle birlikte bazen basit bir silme işlemi için dahi ayrı yazılımların kullanılması gerekmektedir. Ancak dijital delillerin zor yok olmaları savunulmakla birlikte bir yandan da silme işlemi tam anlamıyla gerçekleşince bu tür deliller bir tamamen yok olmuş olurlar. Tamamen sayısal kodlamalar üzerinden ilerleyen dijital sistemlerden bir veri silindiğinde tamamen yok olmaktadır.

Dijital delillerin diğer delillerden farklı özellikleri dolayısıyla farklı bir incelemeye tabi tutulmaları gerekliliği açıktır. Bu sebeple dijital deliller adli bilişim alanı kapsamında incelenmektedir. Dijital deliller açısından adli bilişim bilgisayar inceleme ve analiz tekniklerinin kullanılmasıyla yapılan bir uygulama şekli olarak tanımlanabilmektedir. Dijital deliller bulundukları sanal dijital ortamdan ayrılarak mahkemeye sunulmalıdır.

Bu sebeple dijital delillerin hazırlanması ve sunulması adli bilişim alanında ayrı bir aşamayı oluşturmaktadır. Çalışmamızın üçüncü bölümünde dijital delillerin nasıl hazırlanıp sunuldukları incelenmektedir. Bu kapsamda dijital deliller öncelikle elde edilmeli, ardından incelenmeli, yapılan bilişim incelemesinin üzerine analiz edilmeli, yani değerlendirilmelidirler. Son aşamada yapılan bu değerlendirmeye ilişkin bir rapor düzenlenmeli ve bu rapor mahkemeye sunulmalıdır.

Dijital delil olarak kullanılacak olan dijital veriler öncelikle elde edilmelidir. Elde etme aşamasında dijital verilerin bulunduğu dijital cihazlara el konulmaktadır. Kimi zaman somut olayın özelliği çerçevesinde dijital cihazların tümüne el konulabildiği gibi kimi zaman da dijital cihazlardan alınan bir kopya ile bu inceleme gerçekleştirilmektedir.

Elde etme aşaması tamamlandıktan sonra inceleme aşamasında her ülke kendi hukuk sisteminin getirdiği kurallar çerçevesinde bu incelemeyi gerçekleştirmektedir. Bu aşamada temel olarak öncelikle bir ön izleme yapılacaktır. Yapılan ön izleme çerçevesinde cihaza hukuki sebeplerle el konulmasını sağlayacak “olası nedene” yakın bir veriye ulaşılmalıdır. Bir diğer yöntem olarak ön izlemeden sonra dijital verilerin görüntüsü (imaging) alınmaktadır. Bir diğer yöntem ise yedekleme yaparak inceleme yapmaktır. Bu yöntemle yedekleme anında dijital cihazın anlık görüntüsü ele geçirilmektedir.

Farklı yöntemler içeren inceleme aşamasındaki önemli unsurlardan biri dijital delil olarak kullanılacak verilerin güvenliğini ve güvenilirliğini sağlayabilmek amacıyla bu verilerin tıpkı bir olay yeri gibi korumaya alınması gerekliliğidir. Bu aşamada değişimi engelleyici yöntemler kullanılarak güvenlik sağlanmaya çalışılır. Dijital delillerin korunabilmesi mahkeme önüne çıkartılabilmesi açısından oldukça önemlidir.

Dijital delillerin analiz edilmesi aşamasında delil olarak kullanılacak verilerin davaya ilişkin vakıaları kanıtlıyor olup olmamaları, elde edilen bu verilerin şimdiye kadar bilinenleri doğruluyor olup olmadıkları ve bu verilerin delil mi yoksa delil başlangıcı niteliğinde mi oldukları sorularına yanıt aranmaktadır. Bu analizi yapacak bilişim uzmanının bilgi ve tecrübesi oldukça önemlidir. Zira bir verinin ele geçirilmesi başlı başına yeterli değildir, verinin ele geçirildiği dijital cihazın sahibinin de bu veriden haberdar olması gerekmektedir.

Türk Ceza Muhakemesi hukukunda delil serbestisi olması sebebiyle dijital delillerin mahkemece kabul edilebilirliği meselesi Türk hukuku açısından bir sorun oluşturmamaktadır. Hukuk sistemimiz içerisinde delil serbestisinin sınırını hukuka aykırı deliller çizmektedir. Bu kapsamda dijital delillerin elde edilmesi, incelenmesi ve analiz edilmesi aşamalarında hukuka aykırılığın tespiti halinde bu tür delillerin delil yasakları kapsamında kabul edilmemeleri gerekmektedir.

Dijital verilerden elde edilen dijital delillerin ceza muhakemesinde kullanılabilmesi için delil yasaklarının yanı sıra bu tür delillerin doğrulanması da gerekmektedir. Yabancı hukuk sistemlerinde dijital delillerin sıhhatini tespit etmek için kullanılan doğrulama aşaması kolay zarar görebilen ve değiştirilebilen dijital delillerin inceleme sürecinde aslına uygun kaldığının kanıtlanmasını sağlamaktadır.

Dijital delillerin doğrulanması hususunda yabancı doktrinlerde çeşitli kurallar bulunmaktadır. Maalesef ki Türk hukukunda yabancı sistemlerde bulunduğu gibi bu hususta düzenli bir takım kurallar bulunmamaktadır. Ancak hukuki açıdan dijital verilerin incelenmesi kapsamında Türk Ceza Muhakemesi Kanunu'nun 134. Maddesi önem taşımaktadır. Bu madde hangi şartlar altında bilgisayar incelemesine başvurulacağı ve bu incelemenin hangi şartlar dahilinde yapılacağına değinmektedir. Kanaatimizce 134. Maddede belirtilen aşamalara aykırılık teşkil eden dijital deliller

ve bu tür delillerin sıhhatine ilişkin gerekli güvenlik önemlerinin alınmaması sonucu oluşturulan dijital deliller hukuka aykırı delil olarak kabul edilmelidir.

Dijital delillerin öneminin artması üzerine gerek ulusal gerekse uluslararası düzeyde çeşitli inceleme ve değerlendirme kuralları getirilmektedir. Ancak bu kurallardan bağımsız olarak Türk hukukunda alınan yargı kararları incelenecek olursa, dijital delillerin her türlü hassas ve şüpheye yer verecek yapılarına rağmen tek başlarına mahkumiyete temel alınacak kuvvette deliller olduğu kabul edilmektedir. Dijital delillerin dünya üzerinde farklı yargılama usullerince de artık kuvvetli deliller olarak kabul edildikleri gerçeği ortadadır. Ancak dijital deliller hakkındaki en önemli tartışma ne derece kuvvetli oldukları değil ne derece güvenilebilir oldukları yönündedir. Kimi hukuk sistemlerinde öncelikle bu güveni sağlamak ve çok daha önemlisi, öncelikle dijital delillerle ilk aşamada muhatap olacak polis memurlarının meslek itibarını korumak için detaylı kurallar oluşturulmuştur. Bu aşamada Türk Ceza Muhakemesi'ndeki temel sıkıntı; dijital delillere yönelik bir takım kurallar geliştirilmeden doğrudan mahkumiyet gibi sonucu insan hakları açısından ağır olabilecek cezalara temel sayılmalarıdır.

Dijital delillere ilişkin sağlaması gereken şeffaflığa henüz ulaşılabilmiş değildir. Kanaatimizce bu şeffaflık sağlanıncaya kadar hukuka olan güveni zedelememek için dijital delillerin tek başlarına mahkumiyet kararlarına temel oluşturmamalarıdır.

Anahtar Kelimeler:	Ceza Muhakemesi, Deliller, Dijital Veri, Dijital Delil
---------------------------	---

GİRİŞ

Günümüzde teknolojinin hızlı gelişimi etkisini hukuk alanında da göstermektedir. Teknolojik araçların günlük insan hayatının hemen hemen her noktasında olması onları hukuki anlaşmazlıklar açısından da önemli kılmaktadır. Bu bağlamda dijital cihazlardan elde edilen verilerin hukuki değeri tartışmalıdır.

Söz konusu bu verilerin hukuki niteliğine ilişkin çeşitli değerlendirmeler özel hukuk açısından mevcuttur. Ancak bu çalışmada dijital cihazlardan elde edilen verilerin ceza hukuku kapsamında delil niteliği tartışılacaktır. Zira ceza hukuku açısından kabul edilmekte olan delil serbesti kapsamına dijital delillerin bir takım katı değerlendirme kurallarından yoksun olarak mahkeme kararlara esas alınmaları hakkaniyete ve kamu vicdanına aykırı sonuçlar oluşturabilmektedir. Toplumun en büyük sığınağı olması gereken hukuk sistemlerine yönelik güveni zedelememek için hukuki kararlara temel oluşturacak dijital deliller titizlikle incelenmeli ve bu konuda şüpheye ver vermeyecek standartlar geliştirilmelidir. Ancak hukuk sisteminde henüz bu nevi standartlar bulunmamakla birlikte bu verilerin hukuki kararlara esas alınırken mahiyetleri konusunda da bir görüş birliği olmayışı dijital verileri delil değeri konusunu mutlaka incelenmesi gereken bir alan haline getirmektedir. Bu çalışma, dijital verilerin delil değeri konusunu toplumun hukuka olan güveni açısından son derece önemli olması sebebiyle seçmiştir. Bu doğrultuda hukukçuların ve uygulayıcıların bu konuya dikkatlerini çekmek ve ileride bu hususta atılacak adımlar için incelenebilecek bir genel bakış sunmayı amaçlamaktadır.

Bu çalışmada, dijital verilerin ne olduğu, dijital verilerin ceza hukuku açısından nasıl ele alındığı, bu verilerin delil değerini haiz olup olmadıkları ve bu kapsamda genel delil teorisi içerisinde bu verilerin yerinin ne olduğu sorularına cevaplar aranmaktadır. Bu çalışma bu soruların cevaplarına yanıt ararken aynı zamanda dijital verilerin esasında ne olduklarına yönelik temel bir inceleme de yapmaktadır. Öte yandan bu çalışma dahilinde dijital verilerin nasıl değerlendirildikleri, teknik ölçümlerinin nasıl yapıldığı, bu konudaki uluslararası standartlar ve konuyla ilgili yabancı hukuk sistemlerinden örneklere de yer verilmektedir.

Bu doğrultuda, çalışma öncelikle bilişim hukukuna ilişkin temel kavramları tartışarak başlayacaktır ve veri kavramına ilişkin inceleme bu kapsamda

yapılacaktır. Ardından ceza muhakemesi açısından deliller incelenecektir, delil türleri ve dijital deliller ceza muhakemesinin genel delil sistemi içinde ele alınacaktır. Böylece dijital verilerin dijital delil olarak ceza muhakemesi ile ilişkilendirilmesi açıklanmaya çalışılacaktır. Çalışma dijital verilerin delil olarak hazırlanması ve sunulması konularına da ver verecek olup ardından dijital verilerin delil olarak nasıl değerlendirildikleri incelenecektir.

I-Bilişim Hukukuna İlişkin Genel Bilgiler

A- Kavram ve Tanımlar

1- Bilişim Hukuku kapsamında yer alan temel terimler

Gelişen teknoloji günümüzde etkisini her alanda hissettirmektedir. Günlük hayatta teknolojinin sıkça kullanılması hukuku da etkilemiştir. Teknoloji ve hukukun en belirgin kesişme noktalarından biri olan bilişim hukukuna ilişkin daha detaylı bilgiler vermeden önce gelişmekte olan bu alan dahilindeki çeşitli kavramların tanımlarını vermekte fayda vardır.

Türk Dil Kurumu’nun getirdiği tanıma göre bilişim “insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik¹” ifadesiyle tanımlanmıştır. Türk Dil Kurumu’nun tanımında yer verdiği “enformatik” kelimesinin biraz daha incelenmesinde fayda vardır. Enformatik terimi “enformasyon” ve “otomatik” kelimelerinin bir araya gelmesinde oluşturulmuş olup bir disiplin olarak enformatik; bilimsel enformasyonun yapısını, özelliklerini ve aynı zamanda bilimsel enformasyonun düzeni, teorisi ve metodolojisini araştıran bir bilim dalı olarak görülmektedir².

¹ Türk Dil Kurumu, **Güncel Sözlük**, <http://www.tdk.org.tr>, (Erişim Mart 2013)

² Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara: Adalet Yayınevi, Ocak 2008, s. 10.

Bilişim disiplinde bilişim teknolojisi terimi de önem arz etmektedir. Bilişim teknolojisi³ verileri otomatik işleme tabi tutan, bilgi-işlem ve iletişim kavramlarının her yönüyle bir araya geldiği bir elektronik teknolojiyi ifade etmekte olup bilişim cihazlarının geliştirilmesi ve kullanılması faaliyetini tanımlayan en genel ibaredir⁴.

Bilişim ağı kavramına da değinmek gerekmektedir. Bilişim ağı teknik, ekonomik ve toplumsal alanlardaki iletişim sistemi şeklinde tanımlanabilmektedir⁵. Öte yandan “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı”nın 2. maddesinin e bendinde bilişim ağı; “en az iki bilişim sistemi arasında veya bir bilgisayar ile bir çevre birimi arasında veri iletişimini ve karşılıklı etkileşimi her türlü iletişim tekniği ile sağlayan ortam” sözleri ile tanımlanmaktadır⁶.

Bir diğer bahsedilmesi gereken kavram ise bilişim sistemidir. Bilişim sistemleri 5237 sayılı Türk Ceza Kanunu’nun gerekçesinde şu şekilde tanımlanmıştır: “Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.”⁷ Bilişim sisteminin enformasyonun otomatik makineler aracılığıyla ve otomatik olarak işlenmesini sağlayan sistemler olarak da tanımlanması mümkündür⁸.

Bilişim sistemi donanım ve yazılımlardan oluşur. Donanım bir bilişim cihazının maddi yapısı ve parçalarına denmektedir⁹. Donanım terimine örnek verilecek olursa bir bilgisayarın klavyesi, anakartı ve ekran kartı, bir ATM cihazının tuş takımı, ekranı veya bir cep telefonunun elle tutulur tüm kısımları donanımdır¹⁰.

Bilgisayar komutları veya verilerine genel olarak yazılım denilmektedir. Elektronik olarak depolanabilen, toplanabilen her türlü veri yazılım olarak geçmektedir.¹¹ Bazı bilişim cihazları sadece imalatçı tarafından yüklenmiş tek bir

³ Türk Dil Kurumu’nun Genel Türkçe Sözlüğü’nde belirttiği üzere bilişim teknolojisi bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistem olarak tanımlanmaktadır. Bkz. dipnot 1.

⁴ Hatice Akıncı, A. Emre Alıç, Cüneyd Er, “Türk Ceza Kanunu ve Bilişim Suçları”, **İnternet ve Hukuk**, Derleyen Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004, s. 170.

⁵ Ketizmen, a.g.e., s. 13.

⁶ **Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı**, <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>, (Erişim Mart 2013).

⁷ **Türk Ceza Kanunu Gerekçesi**, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim Mart 2013).

⁸ Ketizmen, a.g.e., s. 11.

⁹ İsmail Malkoç, **Açıklamalı İctihatlı Türk Ceza Kanunu**, Ankara: Turhan Kitabevi, 2001, s. 1256.

¹⁰ Akıncı, Alıç, Er, a.g.e., s. 171.

¹¹ **Webopedia Online IT Dictionary**, yazılım, <http://www.webopedia.com/TERM/S/software.html>, (Erişim Mart 2013).

sistem yazılımı ile çalışırken bilgisayar dahil çeşitli bilişim sistemlerinin hem uygulama yazılımlarının hem de sistem yazılımlarının kullanıcı tarafından değiştirilmesi mümkündür¹².

Yazılımlar sistem yazılımları ve uygulama yazılımları olmak üzere ikiye ayrılırlar. Sistem yazılımları, bir bilişim sisteminin çalışmasını sağlayan işletim sistemi ve yardımcı uygulamaları ifade eder¹³. İşletim sistemi adıyla ifade edilen sistem yazılımları bilişim sistemlerinin olmazsa olmaz bir parçası olup, eşyanın bütünleyici parçasından (mütemmim cüz) kabul edilmelidir¹⁴.

Uygulama yazılımları ise bilişim sistemi kullanıcısı için tasarlanan bir grup programdır. Uygulama yazılımları (diğer adıyla programlar) bilişim sisteminde mevcut sistem yazılımı dahilinde çalışan ve belirli bir işlemi icra amacıyla önceden hazırlanmış komut dizileri bütünü olmakla birlikte uygulama yazılımları bilişim verileri oluşturmak, işlemek, bilgiler meydana getirmek gibi amaçlarla kullanılabilir¹⁵.

Yer ayrılması gereken bir diğer kavram ise tamamlayıcı cihazlardır. Tamamlayıcı cihazla kurulu düzenin, bilişim sisteminin çalışmasını sürdürebilmesini sağlayan cihazlardır¹⁶. Bir bilgisayarın ekranı, klavyesi ve faresi tamamlayıcı cihazlara örnek olarak gösterilebilir.

Mevcut çalışmanın devamında çalışmanın konusu gereği sıkça yer verilecek olan son olarak açıklanacak kavram ise adli bilişim terimidir. Adli bilişim dalı yukarıda açıklanan tanımların hepsinden farklı ve kendi başına bir disipline aittir. Yukarıda detaylı olarak açıklanan bilişim teknolojilerinin gündelik hayatın hemen hemen her alanında kendini bolca göstermesinin bir sonucu olarak bu teknik gelişme hukuk düzeninde de bir takım değişikliklere sebep olmuştur. Günümüzde hakim, savcı ve avukatlar önlerine gelen olaylarda öyle durumlarla karşılaşmaktadırlar ki kimi zaman söz konusu isnadın tek bir delili bir bilgisayar dosyası olabilmektedir. Bu hallerde eskiden beridir alışlagelmiş keşif anlayışı yerini bilgisayar delillerinin incelenmesine bırakmaktadır. Artık somut olayları aydınlatmak amacıyla bilgisayar,

¹² Akıncı, Aliç, Er, **a.g.e.**, s. 171.

¹³ **Webopedia Online IT Dictionary**, sistem yazılımları, <http://www.webopedia.com/TERM/S/software.html> , (Erişim Mart 2013).

¹⁴ Akıncı, Aliç, Er, **a.g.e.**, s. 171.

¹⁵ **A.g.e.**, s. 171 vd.

¹⁶ **A.g.e.**, s. 173.

telefon, hard disk, USB gibi çeşitli elektronik aletlerin incelenme gereksinimi adli bilişim (computer forensic) diye tabir edilen bir alanın doğmasını tetiklemiştir.

Adli bilişim (computer forensic) yasal delillerin elde edilmesi amacıyla bilişim aygıtları üzerinde inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama olarak tanımlanabilmektedir¹⁷. Başka bir deyişle adli bilişim depolanmış ya da şifrelenmiş bilgi veya delillerin tanımlanması, toplanması, incelenmesi ve korunması için analitik ve araştırmacı tekniklerin kullanılmasıdır¹⁸.

2- Bilişim suçları açısından kavram ve terim tartışması

Sıkça karşılaşılan terim bilişim suçları terimi olmasına rağmen gerek yerli gerekse yabancı doktrinde bilişim vasıtasıyla işlenen suçlara verilecek ad konusunda farklı görüşler vardır. Mevcut çalışma esasen bilişim yoluyla elde edilmiş olan bilgi ve belgelerin ceza muhakemesi kapsamında delil olarak değerlendirilmesi sorunu incelenecek olmasına karşın doktrinde yer alan bu isim tartışması çalışmanın devamında sıkça belirtilecek olan terimlere ışık tutacağı açısından incelemeye ve yer vermeye değerdir.

Bilişim daha önce de belirtildiği gibi iletişim amacıyla bilginin elektronik makineler vasıtasıyla işlenmesi demektir. Tanımdan da anlaşılacağı üzere bilişim denildiğinde elektronik makinelerin hepsi akla gelmektedir. Ancak bilişim alanının gelişmesi bilgisayarların ortaya çıkması ve yaygınlaşmasıyla bağlantılı olmuştur¹⁹. Bu sebeple bilişim sistemlerini bilgisayarlar olmadan düşünmek son derece güçtür.

Bilgisayarların gelişmesi ve yaygınlaşması ile ortaya çıkan bu ilişki internet kullanımı ile de kuvvetlenmiştir. Bilişim, bilgisayar ve internet arasındaki bu ilişki bilişim suçlarına verilecek isim konusunda da farklı görüşler ortaya çıkarmıştır. “Bilgisayar suçları”, “bilişim suçları”, “internet suçları” ve “siber suçlar” terimleri ile karşılaşılmıştır. Esasen belirtilen terimlerden her biri içerik olarak birbirinden

¹⁷ Leyle Keser Berber, **Adli Bilişim (Computer Forensic)**, Ankara: Yetkin Yayınları, 2004, s. 39.

¹⁸ Bu teknikler için Bkz. **Computer Forensics World**, <http://www.computerforensicsworld.com/> , (Erişim Mart 2013)

¹⁹ Ayrıntılı bilgi için bkz. Martin Campbell-Kelly, “Origin of Computing”, **Scientific American**, Eylül 2009, Cilt 301, Sayı 3. Ayrıca bkz. Michael S. Mahoney, “The History of Computing in the History of Technology”, **Annals of History of Computing**, Cilt 10, Sayı 2, 1998, s. 113 vd.

farklı kavramlar olmakla birlikte kanaatimizce hepsini içine alan en geniş kavram bilişim suçları deyimidir²⁰. Bu sebeple çalışmanın devamında da bilişim suçları terimi tercih edilecek olmasına rağmen bu aşamada belirtilen tüm terimleri açıklamak isabetli olacaktır.

İfade edildiği üzere yukarıda belirtilen kavramlardan her biri esasen farklı içerikleri karşılamaktadır. Yazıcıoğlu bilişim ve bilgisayarın farklı anlamlarda olduğu belirterek “bilgisayar suçu” ile “bilişim suçunun” farklı şeyleri ifade ettiğini öne sürmekle birlikte pratikte bilgisayarın en yaygın bilişim aracı olması nedeniyle bilişim suçları yerine bilgisayar suçları terimini kullanmayı tercih ettiğini açıklamıştır²¹.

Bilgisayar suçlarına ilişkin üzerinde fikir birliğine varılmış bir tanım mevcut değildir²². OECD’nin 1983 tarihli yapmış olduğu bir tanıma göre “bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemle gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır” şeklinde tanımlanmıştır²³. Bu tanım bilgisayar suçları için getirilen en geniş tanımlar arasındadır.

Öte yandan bilişim suçları ise yine geniş bir tanımla verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkihi ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem olarak tarif etmek mümkündür²⁴.

Siber suçlar olarak adlandırılan suçlar da çeşitli defalar tanımlanmaya çalışılmış olmasına rağmen üzerinde uzlaşılmış bir tanım burada da yoktur. Siber

²⁰ Ayrıntılı için bkz Caner Yenidünya ve Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, Nisan 2003, s. 31, 32, 33. Yazarlar bilgisayar suçları ile bilişim suçları arasındaki ayrımın açıkça ortaya koydukları gibi aynı zamanda siber suç deyimıyla aslında bilişim suçlarının ifade edildiğini ancak siber suç kavramının içine daha ziyade internet aracılığıyla işlenen suçlar girdiği için bilişim suçları teriminin siber suçları da kapsadığını belirtmektedirler. Yine aynı görüş için bkz. Ketizmen, **a.g.e.**, s. 34. ve Yüksel Ersoy, “Genel Hukuki Korum Çerçevesinde Bilgisayar Suçları”, **Prof. Dr. Yılmaz Günel’a Armağan**, Ankara: Ankara Üniversitesi S.B.F. Dergisi, Cilt.49, No. 3-4, Haziran-Aralık 1994, s, 153 vd.

²¹ Yılmaz Yazıcıoğlu, “Bilişim Suçları”, **Hukuki Perspektifler Dergisi**, Sayı 2, Sonbahar 2004, ss.142-146, s. 142.

²² Farklı tanımlar için bkz. Levent Kurt, **Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara:Seçkin Yayınevi, 2005.

²³ Ulrich Sieber, **Legal Aspects of Computer Related Crimes**, <http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf>, Ocak 1998, (Erişim tarihi Mart 2013)

²⁴ Kurt, **a.g.e.**, s.53.

suçlar bilgisayarlar ve internetin kullanılarak işlendiği suçlardır. Bu suçlar yasadışı müzik indirmekten internet bankacılığı aracılığıyla binlerce lira para çalmaya kadar her şeyi içerir. Siber suçlar aynı zamanda virüs oluşturup başka bilgisayarlara gönderme ya da internet üzerinde gizli iş bilgilerini gönderilmesi gibi parasal olmayan suçları da içerir²⁵.

Avrupa Konseyi'nin Siber Suçlar Sözleşmesi'nde siber suçun ne olduğunun tanımı yapılmamıştır. Ancak sözleşme; telif hakları ihlalleri, bilgisayarlarla ilişkili sahtecilik fiilleri, ağ güvenliği ihlalleri, çocuk pornografisi ve siber suçlarda kullanılacak olan yetki ve prosedürleri konu edinmektedir²⁶. Sözleşmenin içeriğinden anlaşıldığı üzere Avrupa Konseyi'nin de yukarıdaki tanımla örtüşür bir siber suç anlayışına sahip olduğu çıkarımı yapılabilir.

Bu çerçevede tartışılan kavramlardan biri de internet suçlarıdır. İnternet suçları kavramı da bilişim suçlarının ifade ettiği geniş yüzeyi kapsayamamaktadır. İnternet suçları çoğu zaman siber suçlar kapsamında incelenmektedir²⁷. İnternet suçları genel olarak bazı suçları hususi olarak internet yoluyla işlenmesi olarak incelenebilmektedir²⁸. Bu çerçevede internet suçları deyiminin de bilişim suçlarını karşılamadığı ortada olduğu gibi başlı başına ayrı bir dal olarak incelemek dahi güçlük yaratmaktadır. Zira internet aracılığıyla işlenen suçlar söz konusu olduğunda siber suçlar kavramı kapsamında kalan korumalar gündeme gelecek olup, mevcut meseleler bu çerçevede çözülebilecektir.

²⁵Ileana Stephan, "Cybercrime", **Curentul Juridic**, http://revcurentjur.ro/arhiva/attachments_201103/recjurid113_13F.pdf, (Erişim tarihi Mayıs 2012) ss. 115-120, s. 115.

²⁶ Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümlerin İncelenmesi", **İnternet ve Hukuk**, Derleyen Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004, s. 279. Ayrıca sözleşmenin İngilizce metni için Council of Europe, **Convention on Cybercrime**, <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> , (Erişim Mart 2013)

²⁷ Ayrıntılı bilgi için bkz. Ian Walden, "Harmonizing Computer Crime Laws in Europe", **European Journal of Crime, European Journal of Crime, Criminal Law and Criminal Justice**, Cilt 12, Sayı 4, 2004, ss.321-336, s. 321 vd.

²⁸ Internet Crime Forum Paper, **Reform of the Computer Misuse Act 1990 (June 2003)**, <http://www.internetcrimenforum.org.uk>, (Erişim Mart 2013).

B- Bilişim yoluyla elde edilen veriler

Çalışmamızın konusu dijital verilerin delil değerinin incelenmesi olması sebebiyle “veri” kavramının neyi içerdiği, “dijital veri” kavramı ve bu kavrama seçenek olarak kullanılan diğer kavramlardan da bahsetmekte fayda vardır.

1- Veri Kavramı

Türk Dil Kurumu’nun vermiş olduğu tanımlara göre veri bilgi demektir. Yine TDK’nın açıklamasına göre bilişim alanında veri “kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi” olarak tanımlanmıştır²⁹.

Veri kavramı daha ziyade kişisel verilerin korunması başlığı altında karşımıza çıkmaktadır. Gelişen teknoloji ve bilgisayarlar kullanım sıklığının artması üzerine kişisel bilgilerin hızla yayılması ve kötüye kullanması artmıştır. Böylece kişisel verilerin korunması zorunluluğu ortaya çıkmıştır. Dijital veri kavramı kişisel verilerin korunmasına kıyasla görece daha yeni bir kavramı olması sebebiyle veri kavramını açıklamada kişisel verilerin korunması bağlamında yapılan çalışmalardan sıkça yararlanmak gerekmektedir.

Avrupa Topluluğu 1995 yılında kişisel verilerin işlenmesi ve bu türden verilerin serbest dolaşımı bakımından bireylerin korunması hakkında 95/45/AT numaralı direktifi kabul etmiştir³⁰. Bu direktifin öncesinde İngiltere’de verilerin korunması yönünde 1984 tarihli kanun kullanılmakta idi. Bu direktifle birlikte İngiltere 1998 tarihli yeni bir verilerin korunması kanunu çıkarmış ve bu kanun 2000 yılında yürürlüğe girmiştir. 1998 tarihli İngiltere’nin veri korunması kanunun 1. bölümünde veri tanımı yapılmıştır. Aydınlatıcı olabileceğini düşündüğümüz bu tanımda göre;

“veri;

²⁹ Türk Dil Kurumu, **Güncel Sözlük**, veri kavramı, <http://www.tdk.org.tr>, (Erişim Mart 2013).

³⁰ Avrupa Birliği hukukunda iki tür yasama faaliyeti önem taşır. Bunlar yönetmelikler ve direktiflerdir. Yönetmelikle üye ülkelerin iç hukukunda doğrudan uygulanır. Üye devletlerin Avrupa Birliği kapsamında yapılan bu yasama faaliyetini kendi iç hukuklarına çevirmeye ihtiyaçları yoktur. Zira yönetmelikler doğrudan uygulanabilir niteliktedir. Ancak bir diğer yasama faaliyeti olarak çıkarılan direktiflerin üye devletlerin iç hukukunda uygulanabilmesi için üye devletlerin bu belgeleri hukuk sistemlerine dahil etmeleri gerekmektedir. Bu süreç her üye devlette farklılık gösterebilir. Bu konuda kısa bilgi için bkz. Peter Carey, **Data Protection A Practical Guide to UK and EU Law**, New York: Oxford University Press, 2009, s. 9.

bu amaç için verilmiş yönlendirmelere karşılık otomatik çalışan donanımlar aracılığıyla işlenen,

bu donanımlar aracılığıyla işlenmesi amacıyla kayıt edilen,

ilgili bir dosyalama sisteminin parçası olmak ya da ilgili bir dosyalama sisteminin bir parçası olması amacıyla kayıt edilen,

belirtilen (a), (b) veya (c) paragraflarına girmeyen ama ulaşılabilir bir kayıdn bir parçasını oluşturan ya da

(a) paragrafından (d) paragrafına kadar hiç birine girmeyen ve bir kamu otoritesi tarafından tutularak kayıt edilen bilgilere” denmektedir³¹.

Bu noktada yer verilmesi gereken bir diğer tanım da Kişisel Verilerin Korunması Kanun tasarısında getirilen kişisel veri tanımıdır. Kanun tasarısının tanımları içeren 3. maddesinin (ç) bendinde kişisel veri “*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin tüm bilgiler*” olarak tanımlanmıştır³².

Veri kavramına ilişkin açıklanan farklı tanımlar kapsamında veri kelimesinin en genel şekilde bilgi anlamına geldiği kanaati oluşmaktadır.

2- Dijital Veri Kavramı ve Bu Terime Seçenek Olarak Kullanılan Diğer Terimler

Bilişim sistemlerinin gelişmesi ve bu sistemlerin hayatın içine gün geçtikçe daha çok dahil olması sonucu artık bu sistemler aracılığıyla işlenen suçlar olduğu gibi kimi bazı suçlar da bu sistemlerden elde edilen deliller yoluyla aydınlatılmaktadır.

Delil teorisine ve dijital verilerin delil değerine çalışmamızın ilerleyen bölümlerinde ayrıntılı olarak değinilecektir. Ancak burada öncelikle dijital verinin ne olduğu ve bu kavrama alternatif olarak kullanılan başka kavramlar arasında neden dijital veri kavramını tercih ettiğimizin izahı yapılacaktır.

³¹ Carey, a.g.e., s. 13.

³² **Kişisel Verilerin Korunması Kanun Tasarısı ve madde gerekçeleri**, <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> , (Erişim Mart 2013).

Kelime olarak dijital, sıfat haliyle “sayısal” anlamındadır. Bir diğer anlamında ise dijital, “verileri bir ekran üzerinde elektronik olarak gösteren” demektir³³. Bu takdirde dijital veri kavramı ile sayısal veriler, bir diğer deyişle sayısal bilgiler kastedilmektedir. Dijital veri kavramı esasen metin, resim, ses kaydı ve videoyu da içeren çeşitli bilgileri temsil eden bir sayılar tertibidir³⁴.

Dijital veri kavramına alternatif olarak doktrinde “elektronik veri” kavramının da kullanıldığına rastlanmaktadır³⁵. Amerika Birleşik Devletleri’nin (ABD) Kalifornia eyaletinde çıkarılan Elektronik Delillerin Ortaya Çıkarılması Kanunu kapsamında elektronik kelimesi; “elektrik akımı geçiren, iletken, yarı iletken, üstün iletken, direnç, kondansatör, indüktans, vakum tüpleri ve nano ölçekli yapılarla imal edilen elemanların ve bu elemanların montajıyla meydana gelen cihazların geliştirilmesiyle ilgilenen mühendislik dalıdır” ifadesiyle tanımlanmıştır³⁶. Elektronik cihazların temel özelliği elektronik yolların kullanılarak yapılmış olmalarıdır. Göksu’nun belirttiği üzere elektronik cihazlar analog veya dijital sinyaller işleyebilirler ve bu marifetle çalışırlar. Bu iki sinyal türü arasındaki asıl fark analog sinyallerin sürekli, dijital sinyallerin ise sürekli olmayan bir ölçekte var olmalarıdır. Bu sebeple analog cihazlar bu sinyalleri doğrudan işlerken dijital cihazlar bu sinyalleri sayılara çevirerek işlerler³⁷. Yine Göksu’nun çalışmasında önemle belirttiği üzere analog cihazların yarattıkları veya sakladıkları verilerin büyük ölçüde sabit ve duyu organları ile doğrudan sıranabilir olmaları söz konusudur. Buna karşın dijital cihazlar yarattıkları veya sakladıkları verileri sayısal hale getirmeleri sebebiyle teknik anlamda orijinalliklerini kaybederler. Bu sebeple dijital veriler, analog verilere kıyasla, bozulma veya değiştirilmeye daha açıktır³⁸.

Açıklanan kavramlar kapsamında dijital kelimesinin sayısal sistemleri daha geniş olarak kapsadığı çıkarımına varmaktayız. Mevcut çalışmamız çerçevesinde delil değerini sorguladığımız verilerin sayısal tabanlı sistemlerin hemen hepsinde karşılaşılan bilgileri içerdiğini belirterek “elektronik veri” deyimini yerine “dijital

³³ Türk Dil Kurumu, **Güncel Sözlük**, sayısal kavramı, <http://www.tdk.org.tr>, (Erişim Mart 2013).

³⁴ Eoghan Casey, **Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet**, London: Academic Press, 2004, s. 1.

³⁵ Türk Dil Kurumu tarafından elektronik kelimesi electron temeline dayanan, elektronikla ilgili olarak tanımlanmıştır. Bkz. Türk Dil Kurumu, **Güncel Sözlük**, elektronik veri kavramı, <http://www.tdk.org.tr>, (Erişim Mart 2013).

³⁶ Mustafa Göksu, **Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde)**, Ankara: Adalet Yayınevi, Nisan 2011, s. 7.

³⁷ A.g.e., s. 7.

³⁸ A.g.e., s. 8.

veri” kavramını kullanmanın daha isabetli olacağına inanmaktayız. Ancak belirtmekte fayda vardır ki, gerek ulusal gerekse uluslararası doktrinde her iki terim çoğu zaman aynı içeriği karşılamaktadır. Bu sebeple doktrinde bu iki terim de birbirine seçenek olarak kullanılmaktadır.

3- Dijital Veri ve Dijital Belge Kavramları

Veri ve belge kavramları birbirinden farklı anlamlara sahiplerdir. Veri kavramının kapsamı çalışmamızın yukarıdaki bölümlerinde detaylıca işlenmiştir. En geniş ifade ile veri dilimize yerleşmiş data kelimesinin tekili olup bilgi anlamına gelmektedir. Belge ise veri kavramından farklı olarak “bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb., vesika, doküman” anlamına gelmektedir³⁹.

Veri tek başına bilgiyi işaret eder. Dijital veriler ise maddi anlamda var olan bilgilerin sayısal düzende ifade edilmesini içerir. Dijital ortamda bilginin tüm unsurları bir ve sıfırlarla ifade edilir ve bu rakamların her biri birer veridir. Bu sebeple her bir verinin belge gibi bir anlam içermesi beklenmez. Ancak belge başlı başına bir bütün halinde bir “şey”i tanımlayan, açıklayan bir araçtır. Esasen belge verilerden oluşan bir bütünü işaret eder⁴⁰.

Belgenin bu tutarlı bütünlüğü onun doğrudan delil olarak kullanılmasına imkan sağlarken verilerin delil niteliği tartışmalıdır. Verilerin belge gibi başlı başına delil olarak kabul edilmediği doktrinde öne sürülmektedir. Zira veriler çoğu zaman olayın tamamını temsil niteliğini taşıyor olabilmektedirler. Ancak veriler mevcut vakıya ilişkin diğer delilleri destekler nitelikte oldukları için verilerin emare olarak kullanılmaları da mümkündür. Bununla birlikte yine veri mevcut olayı başlı başına temsil edici özelliği haiz ise verinin delil olarak kullanılabilmesi de söz konusu olabilmektedir⁴¹.

Dijital belge kavramına değinmeden önce ceza hukuku kapsamında belge kavramını açıklamak gerekmektedir. Ceza hukuku anlamında belge kavramı en sık

³⁹ Türk Dil Kurumu, **Güncel Sözlük**, belge kavramı, <http://www.tdk.org.tr>, (Erişim Mart 2013)

⁴⁰ Göksu, **a.g.e.**, s. 12.

⁴¹ **A.g.e.**, s. 12.

resmi evrakta sahtecilik suçu incelenirken irdelenmiştir. Bu suçun incelemesi kapsamında oluşan doktrinde belge kavramına ilişkin çeşitli özellikler belirlenmiştir.

Belgede sahtecilik suçunun oluşabilmesi için sahtecilik fiilinin hukuki anlamda bir belgede işlenmiş olması gerekir. Bu durumu tespit edebilmek için doktrinde belgede sahtecilik suçları incelenirken belge kavramına da değinilmiştir. Sahir Erman varaka kavramı ile delil teşkil edebilme kavramları arasında sıkı bir bağlantı olduğunu ileri sürmektedir ve varaka kavramının hukuki anlamını ve ayırıcı özelliklerini belirlemeye çalışmıştır⁴². Erman varaka kavramına yalnızca yazıların girebildiğini savunmaktadır⁴³. Bu kapsamda bir kimsenin bir duyguyu bir düşüncüyü, bir olayı veya olguyu, bir nesnede, bilinen bir dilde , anlaşılır olarak, yazı, sayı, çizgi ve şekille ifade edilmesi yazılılıktır⁴⁴. Ayrıca yine Erman’a göre önemli olan ikinci husus ise yazının kimin tarafından yazılmış olduğu bizzat yazıdan anlaşılmalıdır⁴⁵. Hafizoğulları ve Özen bu önemli durumu belgeden söz edilebilmesi için onun bir kimseye mal edilebilir olması gerektiğini belirterek ifade etmektedir ve ayrıca yazının bir içeriğe sahip olması gerektiğinin de altı çizilmiştir⁴⁶. Yazının bir aidiyet unsurunun bulunması gerekir. Erman’ın evrak kavramına ilişkin bu unsurları dile getirmesinin sebebi yazının delil teşkil edebilme değeridir. Zira bir diğer adıyla evrakta sahtecilik suçunun oluşabilmesi için sahtecilik fiilinin varaka üzerinde işlenmiş olması ve varakanın gerekli şartları barındırması gerekmektedir.

TCK’nın resmi belgede sahtecilik suçunu düzenleyen 204. maddesinin gerekçesinde belge kavramı ile ilgili şu açıklamalar yapılmıştır:

“Belge, eski dilimizdeki “evrak” kelimesi karşılığında kullanılmakta olup, yazılı kağıt anlamına gelmektedir. Bu bakımdan, yazılı kağıt niteliğinde olmayan şey, ispat kuvveti ne olursa olsun, belge niteliği taşımamaktadır.

Kağıt üzerindeki yazının, anlaşılabilir bir içeriğe sahip olması ve ayrıca, bir irade beyanını ihtiva etmesi gerekir.

Bu yazının belli bir kişiye veya kişilere izafe edilebilir olması gerekir. Ancak, bu kişilerin gerçekten mevcut kişiler olması gerekmez. Bu itibarla, gerçek veya

⁴² Sahir Erman, **Sahtekarlık Cürümleri**, İstanbul: Sulhi Garan Matbaası, 1970 s. 285-286.

⁴³ **A.g.e.**, s. 286

⁴⁴ Zeki Hafizoğulları, Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar**, Ankara: Us-A Yayıncılık, Ağustos 2012, s. 162.

⁴⁵ Erman, **a.g.e.**, s.293.

⁴⁶ Hafizoğulları ve Özen, **a.g.e.**, s. 164.

hayalî belli bir kişiye izafe edilemeyen yazılı kağıt, belge niteliği taşımaz. Kağıt üzerindeki yazının belli bir kişiye izafe edilebilmesi için, bu kişinin ad ve soyadının kağıda eksiksiz bir şekilde yazılması ve kağıdın bu kişi tarafından imzalanmış olması şart değildir.”⁴⁷

Kanunun madde gerekçelerinde yer verilen açıklamaların yanı sıra Yargıtay da belge kavramına ilişkin bir tanımlama getirmiştir. Yargıtay belgeyi hukuki bir hüküm ifade eden bir hakkın doğmasına ve bir olayın kanıtlanmasına yarayan yazılar olarak tanımlamaktadır⁴⁸.

Türk Ceza Kanunu’nun açıkça belge kavramını tanımlamaması sebebiyle bu kavramın içini doldurmak içtihatlarla ve doktrinle olmaktadır. Her ne kadar TCK böyle bir tanım vermese de dünya genelinde çeşitli ceza kanunları belge tanımı yapmışlardır. Farklı hukuk sistemlerinde yapılmış çeşitli belge tanımları şu şekildedir:

“1932 tarihli Polonya Ceza Kanununa göre bir hakkın, bir hukuki ilişkinin veya hukuki hükmü haiz olabilecek bir hal ve durumun varlığını ispata yarayacak her şey varakadır.

1930 tarihli Danimarka Ceza Kanununa göre evraktan yazı sahibinin ismini taşıyan ve bir hakkın, bir borcun veya bir borçtan ibranın delili olmak üzere kullanılan veya bu surette kullanılmaya tahsis edildiği kanaatini veren her yazı anlaşılır.

1902 tarihli Norveç Ceza Kanununa göre varaka deyiminden, el yazısı olsun veya olmasın, bir hak, bir borç, bir ibrayı tespiti elverişli bir beyanı ihtiva eden veya bir hususun ispatına tahsis edildiği kanısını uyandıran her belge anlaşılacak istenir.

⁴⁷ **Türk Ceza Kanunu Madde Gerekçeleri**, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim Mart 2013)

⁴⁸ Yargıtay 6. CD. 4.7.1983, 2707/3846, Ayrıca bkz. Erol Çetin ve İsmail Malkoç, **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara: Adalet Yayınevi, Mart 1995, s. 130.

1973 tarihli Japon Ceza Kanununa göre bir hakkın, bir borcun veya bir fiilin ispatına yarayacak bir yazı veya işareti sahte olarak meydana getiren herkesi cezalandırmaktadır.”⁴⁹

Belirtilen yabancı hukuklarda verilen belge tanımlarının yanı sıra İsviçre Ceza Kanununda evrak, hukuki açıdan önemli olan olguları ispat etmek için belirlenmiş olan işaret veya bunun için belirlenmiş ve buna elverişli yazılardır. İsviçre Ceza Kanununun belirttiği tanımda aynı amaca hizmet eden bilgisayar veya bant kayıtları yazılı biçime eşit tutulur⁵⁰.

TCK’nın gerekçesinde belirtilen açıklamalar ve yabancı hukukların düzenlemelerinin incelenmesiyle doktrinde belge kavramına ilişkin çeşitli görüşler de ileri sürülmüştür. Toroslu ceza hukuku yönünden belgeyi olayları nakleden veya irade beyanlarını içeren ve bir kimse tarafından oluşturulan her türlü yazılı belge olarak tanımlamıştır⁵¹.

Gerek doktrindeki belge tanımları gerekse kanun gerekçesinde ve Yargıtay’da geliştirilen yaklaşım kapsamında belgeden söz edilebilmesi için aranan Sahir Erman’ın da ortaya koyduğu üç temel özellik göze çarpmaktadır.

- Belge yazılı olmalıdır. Bir olayın veya bir hakkın kanıtını teşkil eden yazılar belge sayılmaktadırlar⁵². Belge ile tespiti istenen durumun bunu tespiti elverişli araç ve alfabe ile ifade edilmiş olması gerekmektedir. Yazının veya harflerin herhangi bir şekilde tespiti yeterlidir, kullanılan dilin önemi yoktur, içeriğinin anlaşılması yeterlidir⁵³. Aynı şekilde yazının bilgisayar, daktilo veya el yazısı ile yazılmasının da bir önemi yoktur. Önemli olan belgeden bahsedilebilmek için açık bir yazının söz konusu olmasıdır. Doktrinde bir görüş kapsamında fotoğraf ve bilgisayar programı gibi oluşumların varaka olarak kabul edilmediği görülmektedir⁵⁴. Ancak bir diğer görüş kapsamında ise bir olayın veya olgunun fotoğrafla tespiti de yazılılık sayılmaktadır⁵⁵.

⁴⁹ Ahmet Gündel, **İçtihatlı-Açıklamalı Zimmet, Sahtecilik, Hırsızlık, Gasp, Dolandırıcılık, Emniyeti Suistimal Suçları**, Ankara: Seçkin Yayıncılık, Eylül 2002, s. 198.

⁵⁰ Durmuş Tezcan ve Mustafa Ruhan Erdem, **Teorik ve Pratik Ceza Hukuku**, İzmir: Şafak Matbaacılık, 2002, s. 281.

⁵¹ Nevzat Toroslu, **Ceza Hukuku Özel Kısım**, Ankara: Savaş Yayınları, Ekim 2008, s. 220.

⁵² Çetin ve Malkoç, **a.g.e.**, s. 130.

⁵³ İsmail Malkoç, **Açıklamalı Yeni Türk Ceza Kanunu Özel Hükümler (170-345), II. Cilt**, Ankara: Malkoç Kitabevi, 2006, s. 1280.

⁵⁴ Tezcan ve Erdem, **a.g.e.**, s. 282.

⁵⁵ Hafizoğulları ve Özen, **a.g.e.**, s. 162.

- Belgeyi düzenleyen belli olmalıdır. Bu husus TCK'nın gerekçesinde de şu şekilde belirtilmiştir: *"Bu yazının belli bir kişiye veya kişilere izafe edilebilir olması gerekir. Ancak, bu kişilerin gerçekten mevcut kişiler olması gerekmez. Bu itibarla, gerçek veya hayalî belli bir kişiye izafe edilemeyen yazılı kağıt, belge niteliği taşımaz. Kağıt üzerindeki yazının belli bir kişiye izafe edilebilmesi için, bu kişinin ad ve soyadının kağıda eksiksiz bir şekilde yazılması ve kağıdın bu kişi tarafından imzalanmış olması şart değildir."*⁵⁶ Gerekçede de açıklandığı üzere yazı ile ifade olunan irade beyanının sahibinin belirli bir kişi ya da makam olarak anlaşılmakta olması gerekmektedir birlikte yazının somut olarak bir kimseye, bir makama aidiyeti anlaşılabiliriyorsa yazının kimliği olduğu kabul edilmektedir⁵⁷. Belge kişisel bir delil olarak ortaya koyanın kimliğinden delil değeri elde ettiği için belge onu düzenleyeni kişiselleştirebilmeli ve en azından teşhis edilebilir hale getirmelidir⁵⁸. Bu sebeple anonim nitelikteki yazılar belge olarak kabul edilmemektedir⁵⁹.

- Belgenin belli bir içeriğinin bulunması gerekmektedir. Belgenin içeriği bir olayın naklinden veya bir irade beyanından ibaret olabilir⁶⁰. Belgenin düzenlendiği aşamada bu amaç gözetilerek yazılması gerekmez ancak işin doğası gereği belgeden bahsedebilmek için bir süreklilik gerektiği için kolayca yok olacak zeminlere (kara veya kuma yazı yazmak gibi) yazılan yazılar da belge özelliği teşkil etmezler⁶¹. Bir anlayışa göre belgeden söz edilebilmek için nakledilen olayın veya irade açıklamasının hukuki sonuçlar doğurmaya elverişli olması aranmaktadır⁶². Bu görüşe göre belge kanıtını oluşturduğu olayın hukuk düzeni ile ilgili olması, hukuksal bir önem ve etkiye sahip olunabilmesi gerekmektedir⁶³.

Belge ve veri kavramlarına ilişkin belirtilen açıklamalar doğrultusunda dijital belge kavramından dijital verilerin bir araya gelerek veya tek başlarına bir anlam bütünlüğü dahilinde bir olayı temsil niteliğini taşıyan belge oluşturmaları

⁵⁶ **Türk Ceza Kanunu Madde Gerekçeleri**, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc , (Erişim Mart 2013).

⁵⁷ Çetin ve Malkoç, **a.g.e.**, s. 132.

⁵⁸ Tezcan ve Erdem, **a.g.e.**, s. 282.

⁵⁹ **A.g.e.**, s. 282. Ayrıca bkz. Hafizoğulları ve Özen, **a.g.e.**, s. 163.

⁶⁰ Toroslu, **Ceza Hukuku Özel Kısım**, s. 222.

⁶¹ Tezcan ve Erdem, **a.g.e.**, s. 283

⁶² Toroslu, **Ceza Hukuku Özel Kısım**, s. 223.

⁶³ Aynı görüş için bkz. Çetin ve Malkoç, **a.g.e.**, s. 132.

anlaşılmaktadır⁶⁴. Bir kez daha tekrar etmekte fayda vardır ki verilerin tek görevi bir araya gelerek belgeleri oluşturmak değildir. Veriler belgeleri tanımlama, ifade etme, gerçekliğini sınama, özelliklerini belirtme gibi daha farklı fonksiyonları da barındırmaktadır⁶⁵.

Dijital belge kavramı kapsamında tartışılması gereken en önemli husus bu belgelerin aidiyet unsurunun nasıl tespit edileceğidir. Burada belirtmekte fayda vardır ki, belgenin aidiyet unsuru taşınması görüldüğü üzere çok katı kurallara bağlanmamakla birlikte bir yazının belge niteliğini haiz olması için elzemdir. Aidiyet unsuru dijital delillerin değerlendirilmesi bakımından da oldukça önemlidir. Zira yapılan adli bilişim incelemeleri sırasında elde edilen dijital verilerin belge olarak kabul edilebilmeleri ve muhakemeyi etkileyebilmeleri için aidiyetlerinden kuşku duyulmamalıdır. Belgenin kimliğinin tespit edilmesi uygulamada oldukça önemli bir sorundur. Bir kişinin bilgisayarında bulunan bir word dosyası acaba belge sayılabilecek midir? O dosyanın gerçekten o kişi tarafından oluşturulduğu delil doğruluğu ve bütünlüğü sağlanacak biçimde nasıl tespit edilebilecektir? Kanaatimizce bir bilgisayar incelemesi sonucunda ele geçirilen verilerin bilgisayarın sahibine ait olduğu yönündeki bir inanış peşin hüküm vermeye sebep olacaktır. Çalışmamızın ilerideki bölümlerinde de değineceğimiz üzere dijital deliller hususunda bir verinin doğruluğundan emin olunmadığı sürece onun hukuki anlamda belge olarak değerlendirilmesi kabul edebileceğimiz bir görüş değildir.

Dijital belge kavramına ilişkin olarak son aşamada değinilmesi gereken mesele belge kavramında aranan yazılı olma koşuludur. Bilindiği üzere dijital ortamda verilerin bir araya gelmesi ile oluşan belgelerin yazıcılar aracılığıyla çıktıları alınabilmekte ve böylece dijital formatta içeriği oluşturulan belgeler klasik anlamda yazılı halde temin edilebilmektedir. Ancak bu noktada sorun dijital verilerin bir anlam bütünlüğü dahilinde oluşturduğu ve söz konusu olayı temsil edebilme özelliğine sahip ancak bilgisayar ya da benzeri olacak şekilde bilişim sistemlerinde kullanılan cihazlar aracılığıyla görüntülenen dijital formattaki belgelerin belge özelliği taşıyıp taşımadığıdır. Bu soru kapsamındaki esas tartışma konusu dijital belge deyimi kullanılırken örneğin bir yazılım programı da belge olarak kabul edilebilecek midir? Bu noktada uluslararası doktrinde göze çarpan bir ayırımına yer vermekte fayda vardır. Bu ayırım dahilinde gelişen teknoloji ve

⁶⁴ Elektronik belge tanımı için bkz. Göksu, **a.g.e.**, s. 13.

⁶⁵ **A.g.e.**, s. 13.

imkanlar göz önüne alınarak belge tanımı bir klasik anlamda bir de işlevsel anlamda yapılmaktadır. Klasik anlamda belgeden bahsedebilmek için yazıllık şartının arandığına değinmiştik. İşlevsel anlamda ise belge kavramının kapsamına göstergeler de dahil edilmektedir. Böylece sadece yazılı metinlerden değil fiziksel ya da sembolik işaretler de belge kavramına dahil edilmektedir.

Bu görüşün karşısında yazıllık özelliğini sağlayan belgelerin delil değeri içermeleri sebebiyle önemli olduklarını iddia eden görüşler de vardır. Ancak bu düşünceye karşılık işlevsel anlamda belge kavramını savunanlar bilgi sistemlerinin iki özelliğini öne sürerek karşı çıkmaktadırlar. Öncelikle bilgi sistemleri bir sav dahilinde ileri sürülen herhangi bir delilin depolanması ve erişiminin sağlamakla görevlidir. Bir diğer açıdan ise yazılı olmayan diğer nesnelerin belge olarak kabul edilmesiyle bilgi sistemleri bunları düzenleyip başka durumlarda tekrar delil olarak öne sürülebilmelerini sağlama görevini de içermektedir⁶⁶.

İlk bakışta belirtilen işlevsel belge anlayışı oldukça radikal bir yaklaşım olarak değerlendirilebilse de gelişen teknolojinin artık akıllara yer etmiş belge kavramını da sorgulattığı açıktır. Bu sebeple dijital verilerin bir bütün olarak oluşturduğu dijital belgelerin tanımlanması ve hukuk sistemi içerisine yerleştirilmesi günümüz için yeni ve tartışmalı konular arasında yer almaktadır. Yukarıda açıklandığı üzere klasik belge anlayışının benimsenmesi değişen güncel koşullarda tatmin edici olmayan sonuçlar ortaya çıkarabilse de işlevsel belge anlayışında da farklı teknolojilerle ortaya çıkartılmış farklı formlardaki oluşumların “belge” olarak kabul edilebilmesi mümkün kılınmaktadır.

C- Dijital verilere erişebilme açısından bilişim sisteminde kullanılan cihazlar

Bilişim sistemlerinde kullanılan dijital cihazlar çok çeşitlilik göstermektedir. Sayısız olan bu cihazların her birini açıklamak mevcut çalışmamızın kapsamı dışında kalmaktadır. Bu sebeple söz konusu bu çalışmanın kapsamına uygun bir

⁶⁶ İşlevsel belge kavramı için bkz. Michael Buckland, "What is a 'document'?" **Journal of the American Society for Information Science**, Cilt 48, Sayı 9, Eylül 1997, ss. 804-809, <http://people.ischool.berkeley.edu/~buckland/digdoc.html>, (Erişim Mart 2013).

şekilde dijital delil olarak ileride kullanılabilecek dijital tabanlı cihazlara yer verilecektir.

Bilgisayar, internet ve veri depolama cihazlarını da kapsayacak şekilde önemli olarak gördüğümüz cihazları şu şekilde sıralayabiliriz:

- *“Bilgisayarların sabit diskleri ya da veri depolamak amacıyla kullanılan diğer parçaları,*
- *Bilgisayar ve diğer cihazlar arasında veri taşımak ve depolamak amacı ile kullanılan, manyetik, optik veya katı hal teknolojisini kullanan hafıza kartı, cd-rom, dvd-rom, usb bellek vb. gibi taşınabilir cihazlar,*
- *Tüm dijital cihazlarda bulunan ve cihazın açılıp kapanması ile silinen, cihazların anlık çalışmasını düzenleyen ve “ram bellek” adı verilen cihazlar,*
- *Kullanıcının cihaza ulaşmasını sağlayan her türlü ekran vb.’dir.”⁶⁷*

1- Bilgisayar Sistemleri

Bilgisayar İngilizce’de “computer” kelimesi ile ifade edilmektedir. Computer kelimesi “compute” fiilinde gelir ve bu fiil hesaplamak anlamındadır. Bu fiilden türeyen computer kelimesi ise hesap yapan anlamına gelmektedir⁶⁸.

Bilgisayarların teknolojik gelişmelerle birlikte gün geçtikçe daha kapsamlı ve karmaşık hale gelmeleri tanımlarının yapılmasını zorlaştırmaktadır. Teknolojinin ilerlemesi ile gelişen bilgisayarların oluşturduğu bu tanımlama güçlüğü’nün yanı sıra bilgisayarlar kullanılarak işlenen suçların gün geçtikçe artması sebebiyle bir tanımlamanın yapılmasına duyulan ihtiyaç da yine bu ölçüde artmaktadır. Öte yandan yine gelişen teknik imkanlar doğrultusunda bilgisayar olarak kabul edilmeyen cihazların artık bilgisayar özelliklerine oldukça yaklaştıkları da görülmektedir. Bu çerçevede biometrik tanımlayıcılar ve akıllı evler bilgisayar özelliklerine çok yaklaşan elektronik cihaz örnekleri olarak sıkça gösterilmektedir⁶⁹.

⁶⁷ A.g.e., s. 10.

⁶⁸ Sözcüğün İngilizce etimolojik kökeni için bkz. **Online Etymology Dictionary**, <http://www.etymonline.com/>, (Erişim Mart 2013).

⁶⁹ Bkz. Caner Yenidünya ve Olgun Değirmenci, a.g.e., s. 17 vd. Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara: Seçkin Yayıncılık, Mayıs 2005, s. 32-33.

Bilgisayarı dış ortamdan aldığı verileri içerisinde bulundurduğu programlar sayesinde depolayan, işleyen, aldığı verilerle yeni sonuçlar üreten, bu sonuçları tekrar kullanıcıya sunan ve bu yolla veri iletişimi sağlayan bir makine olarak tanımlamak mümkündür⁷⁰.

Bu tanımın yanı sıra bilgisayarları fonksiyonlarına ve yaptığı işlere göre ve fiziksel özellikleri ile birlikte yaptığı işlere göre olmak üzere iki farklı tabanda tanımlamak da mümkündür. Bilgisayarlar fonksiyonlarına ve yaptığı işlere göre ele alındığında öncelikle yazılımları göz önünde bulundurulur. Bu çerçevede bilgisayarları her türlü yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş problem üzerinde çalışan genel amaçlı aygıtlar olarak tanımlamak mümkündür⁷¹.

Öte yandan bilgisayarlar fiziksel özellikleri ve yaptığı işler dikkate alınarak tanımlandığında bilgisayarların yazılımlarıyla birlikte donanımları da göz önüne alınmaktadır. Bu çerçevede bilgisayarlar içerisine yüklenen programlar yardımıyla bilgileri saklayan, işleyerek yeni sonuçlar üreten, üretilen bilgileri başka yerlere ileten ve yine başka yerlerdeki bilgilere ulaşmak amacıyla kullanılan cihazlar olarak tanımlanabilmektedir⁷².

Verilen tüm tanımlar çerçevesinde ilk başta belirtilen tanımın bilgisayarların hem donanım hem de yazılımlarını da kapsaması sebebiyle daha ayrıntılı görülmekte ve doktrinde başka yazarlarca da kabul edilmektedir⁷³.

2- Bilgisayarı oluşturan unsurlar

Bilgisayar yukarıda verilen tanımlar doğrultusunda belirtilen işlevleri yerine getirebilmek için birden farklı unsurun birleşimi ile çalışmaktadır. Çalışmamızın başında belirtilen bilişim sistemlerini oluşturan donanım ve yazılımlar bilgisayarlar için de geçerlidir. Bu çerçevede bilgisayarlar somut olarak varlıkları mevcut olan,

⁷⁰ Yenidünya ve Değirmenci, **a.g.e.**, s. 19.

⁷¹ Murat Volkan Dülger, **Bilişim Suçları**, Ankara: Seçkin Yayıncılık, Kasım 2004, s. 37.

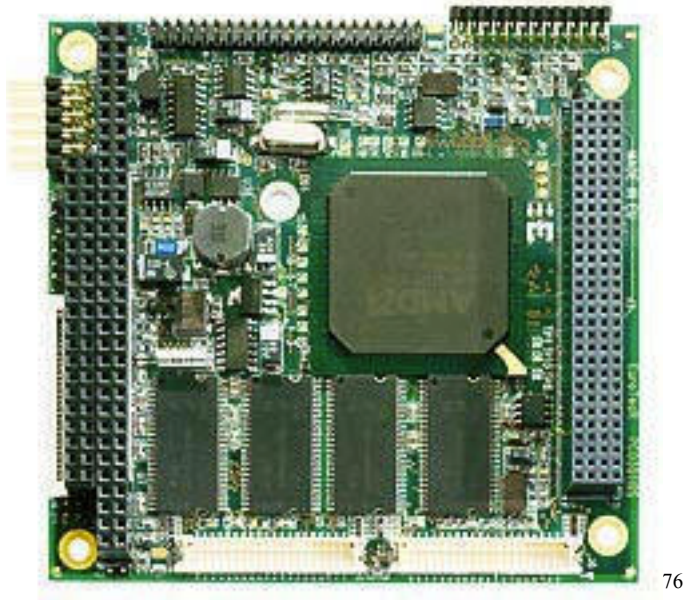
⁷² **A.g.e** , s. 38.

⁷³ Benzer görüş için bkz. Dülger (2004), s. 38. Dülger çalışmasında özellikle belirtilen tanımın bilgisayarların depolama işlevi üzerinde durması sebebiyle önemli olduğunu belirtmektedir. Zira Dülger'in açıklamalarına göre bilgisayarların verileri depolama işlevi sanal arşivler oluşturmakta ve bu sanal arşivler birçok bilişim suçunun işlenme yeri olabilmektedir. Öte yandan ceza muhakemesinde deliller açısından da sanal arşivlerin önemi büyüktür. Sanal arşivlerden erişilen bilgiler muhakeme hukuku kapsamında da delil olarak öne sürülebilmektedir.

elle tutulan ve gözle görülen fiziki parçaların yanı sıra sayısal tabanlarla yazılan ve verilerin işlenmesini sağlayan soyut yazılımlardan oluşmaktadır⁷⁴. Çalışmamızın başında da belirtildiği üzere bilgisayarın somut parçaları donanımı, soyut parçaları ise yazılımları oluşturmaktadır.

Günümüz bilgisayarlar sistemleri CPU (merkezi işlemci ünitesi- central processing unit), ağa bağlı diğer bilgisayarlarla veri akımını sağlayan diğer cihazlar, disk sürücü ve dahili bellekten oluşmaktadır. Dahili bellek kapsamında RAM (random access memory- rastgele erişimli bellek), ROM (read only memory- salt okunur bellek) ve veri depolama hafızası (disk space) adı verilen bilgi depolama kısımları mevcuttur⁷⁵.

a- CPU (merkezi işlem birimi- central processing unit-mikro işlemci)



Şekil-1

Ana işlemci olarak da bilinen CPU, bilgisayarın tüm birleşik devrelerinin bağlı bulunduğu ve ana kartın üzerinde yer alan bir tümleşik devre, yongadır⁷⁷. Bilgisayarın tüm birimleri mikro işlemciden aldıkları komuta göre hareket eder bu

⁷⁴ Dülger (2004), **a.g.e.**, s. 39.

⁷⁵ Mustafa Topaloğlu, **Bilişim Hukuku**, Adana: Karahan Kitabevi, Mayıs 2005, s. 3.

⁷⁶ **Central Processing Unit**, <http://letisialinares.blogspot.com/2010/10/central-processing-unit-cpu.html>, (Erişim tarihi Mart 2013).

⁷⁷ Dülger (2004), **a.g.e.**, s. 39. Bir tümleşik devre içinde binlerce devreyi barındıran devreler bütününe verilen addır. Bunlar yonga yani *chip* olarak adlandırılır. Yonga ismi tümleşik devreyi oluşturan devrelerin silisyumdan yapılmış yonganın üzerine monte edilmelerinden gelir. Bkz. Yenidünya ve Değirmenci, **a.g.e.**, s. 22.

sebeple mikro işlemci bilgisayarın beyni anlamına gelmektedir⁷⁸. Bu birim gerçek komutları işleten bir denetim birimi, komut biriminin doğrudan bağlandığı yazmaç adlı bellek birimleri, matematiksel hesaplamaların yapılmasında rol oynayan matematiksel yardımcı işlemci, komutları sıraya sokmak suretiyle komut birimine gönderen komut besleme birimi, sık kullanılan komutların tutulduğu dahili ön bellek, dış dünya ile bağlantıyı sağlayan adres yolu ile veri yolu deneticilerinden oluşur⁷⁹.

b- Dahili bellek

i. RAM (random access memory- rastgele erişimli bellek)



Şekil-2

Bilgisayar çalıştığı sürece çalışmaya devam eden, bilgisayara gelen gücün kesintiye uğraması halinde içerdiği bilgileri silen, erişimin ardışık olmadığı, rastgele düzenlendiği, ancak veri okuma hızının fazla olduğu bir bellektir⁸⁰. Başka bir ifade ile rastgele erişimli bellek, bilgisayara girilen verilerin üzerine yazıldığı ve saklandığı, üzerindeki verilerin silinebildiği ya da değiştirilebildiği, bilgisayarın üzerinde işlem yaptığı bellektir⁸¹. RAM’de depolanan bilgilere uçucu veriler de denilmektedir. Adından da anlaşıldığı üzere bu tür veriler sabit diskte depolanmaz ve bilgisayarın güç akımı kesildiği anda silinir ve kurtarılamazlar. Uçucu veriler

⁷⁸ Yenidünya ve Değirmenci, **a.g.e.**, s. 23.

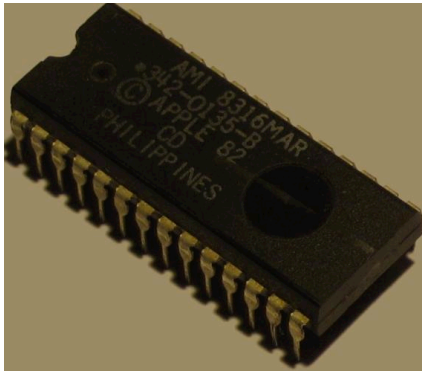
⁷⁹ Dülger (2004), **a.g.e.**, s. 39-40.

⁸⁰ Yenidünya ve Değirmenci, **a.g.e.**, s. 24.

⁸¹ Dülger (2004), **a.g.e.**, s. 40.

kullanılan bilgisayar bir ağ veya internete bağlı ise bilgisayarın internet protokol adresini, bağlı olduğu diğer bilgisayarları ve bağlantı kapıları gibi bilgileri içerir⁸². Uçucu veriler aracılığıyla geçerli kullanıcı, geçerli gün ve saat, bilgisayarın ne kadar süre için açık konumda, kaldığı işletim sisteminin kurulma tarihi ve kayıtlı sahibinin kim olduğu belirlenebilir⁸³.

ii. ROM (read only memory- salt okunur bellek)



Şekil- 3

Bilgisayarın işlevini yerine getirebilmesi için ihtiyaç duyduğu ve içeriği değiştirilemeyen, sadece okunabilen verilerin bulunduğu bellektir⁸⁴. Rastgele erişimli belleğin (RAM) tersine bilgisayara gelen gücün kesilmesi halinde salt okunur bellek (ROM) etkilenmez ve üzerine tekrar bir veri kaydedilmediği için bozulmaya uğramaz. Merkezi işlem birimi tarafından sadece okunmak için ulaşılır⁸⁵. Bilgisayarın ilk açılışı sırasında işletim yazılımının yüklenip çalışmaya başlamasından önce gerekli komutları verip bilgisayarı çalıştıran ve işletim yazılımının yüklenmesini sağlayan yazılım bu belleğe yüklü olarak bulunmaktadır⁸⁶. Bilgisayarın en temel işlevlerini yapabilmesini sağlayan bu programlar topluluğuna BIOS (Basic Input/Output System) yani temel giriş çıkış sistemi denilmektedir ve bu sistemin temel görevi bilgisayarla kullanıcı arasında bilgi alışverişini sağlamaktır⁸⁷. Örneği bilgisayarın klavyesindeki (A) tuşuna basıldığında ekranda (A) harfinin

⁸² Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Ankara:Seçkin Yayıncılık, Kasım 2013, s. 680.

⁸³ Dülger (2013), **a.g.e.**, s. 680

⁸⁴ Yenidünya ve Değirmenci, **a.g.e.**, s. 23.

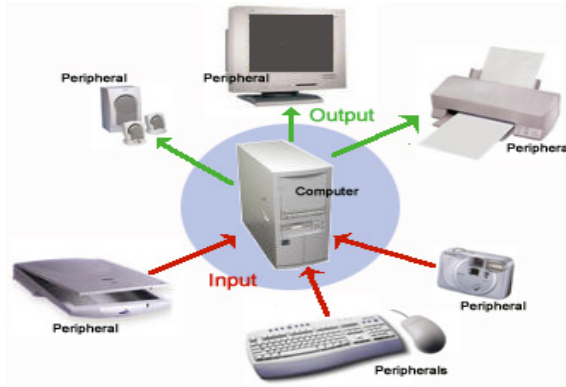
⁸⁵ **A.g.e.**, s. 23.

⁸⁶ Dülger (2004), **a.g.e.**, s. 40.

⁸⁷ Yenidünya ve Değirmenci, **a.g.e.**, s. 24.

görünmesini sebebi ROM’da bulunan programlardır. Aksi takdirde kullanıcı (A) tuşuna bastığında her seferinde bilgisayar dilinde “(A) tuşuna basıldığında ekranda (A) harfini göster” komutunun yazılması gerekirdi⁸⁸.

c- Çevre Giriş (Input) – Çıkış (Output) Birimleri



Şekil- 4

Çevre giriş- çıkış birimleri, bilgisayara veri girişinin yapıldığı klavye, fare, disket sürücü, CD-ROM sürücü, tarayıcı, kamera gibi cihazlardan oluşur ve bu cihazlar bilgisayarın dış ortamla iletişim kurmasını sağlarlar⁸⁹. Çevre giriş- çıkış birimleri teknolojinin gelişmesi ile doğru orantılı olarak gelişmekte ve çeşitlenmektedir⁹⁰.

3- El bilgisayarları



Şekil- 5

⁸⁸ A.g.e., s. 24.

⁸⁹ Dülger (2004), a.g.e., s. 40.

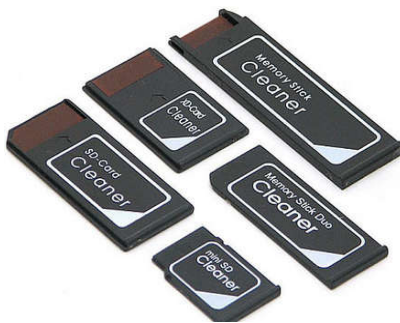
⁹⁰ Yenidünya ve Değirmenci, a.g.e., s. 25.

Günlük hayatı daha da kolaylaştırmak amacıyla kullanılan bu cihazlar normal bir bilgisayarın özelliklerinin çoğu taşımaktadırlar. İnternete de erişimlerinin olması halinde çeşitli ofis programlarını çalıştırmalarının yanı sıra adres ve telefon bilgileri, ajanda, internet erişim kayıtları ve silinmiş verileri barındırabilirler⁹¹.

4- Dijital verilerin (bilgilerin) depolandığı cihazlar

Günlük hayatta bilgisayar ve diğer cihazlar arasında veri taşımak ve mevcut verileri depolamak amacıyla hafıza kartı, cd-rom, dvd-rom ve usb bellek gibi çeşitli taşınabilir cihazlara sıkça başvurulmaktadır. Çalışmamızın devamında açıklanacak hususlar dikkate alındığında bu bölümde kısaca bu cihazları, bu cihazlarına çalışma sistemlerini ve hash değeri incelemelerini de ele almakta fayda vardır.

a- Hafıza Kartı



Şekil- 6

Hafıza kartları günümüzde hemen her dijital makinada bulunan, eski analog makinalarda sıkça kullanılan filmlerin dijital halidir⁹². Hafıza kartları güç kaynağından ayrıldıktan sonra içlerindeki veriyi kaybetmeme ve hatta silinmiş verileri kurtarma özelliğine sahip veri depolama cihazlarıdır⁹³.

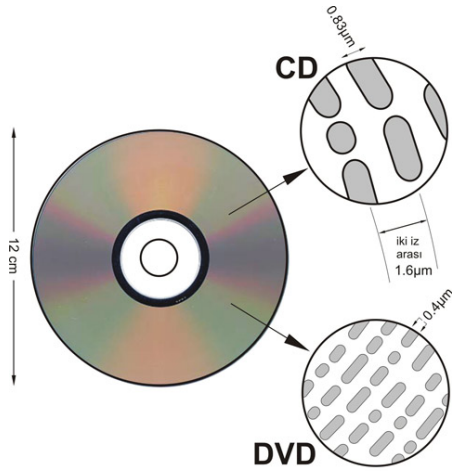
⁹¹ Dülger (2013), **a.g.e.**, s. 682.

⁹² **Hafıza Kartı Nedir?**, <http://bilgipaylas.com/hafiza-karti-nedir.html>, (Erişim Mayıs 2012).

⁹³ Ali Osman Özdiş, *Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku*, İstanbul: Vedat Yayıncılık, Eylül 2006, s. 211.

Bilgisayarlara ilişkin dijital malzemelerin satış noktalarında *memory stick*, *flash card in PCMCIA*, *floppy disk adaptor*, *compact flash card*, *smart media cart*, *smart media floppy*, *memory card* isimleriyle bulunmaktadır⁹⁴.

b- Cd / Dvd ve Blu-Ray



Şekil-7

Cd (Compact disk) ve Dvd (Digital versalit disk) de elektrik, manyetik ve dijital veriyi depolama için kullanılan cihazlardır⁹⁵. Daha eski teknolojiye bugün sıkça kullanılan cd ve dvdlerin yerine disket ve kasetler kullanılmakta idi. Bu cihazlar da cd ve dvd ile aynı işlevi görüp verilerin depolanması amacıyla kullanılmaktadır.

Blu-Ray ise 2000'li yılların başında ortaya çıkmış lazerle veri kaydedilmesine yarayan bir optik disk biçimidir. CD ve DVD'den farkı daha yüksek miktarda veri depolayabilmesi ve depoladığı verilerin çözünürlük kalitesinin daha yüksek (HD) olmasıdır. Blu-Ray teknolojisi mavi-mor lazer ışınları ile yazılıp okunabilir.

Hem CD/ DVD'lerde hem de Blu-Ray'lerde RW uzantısı varsa kaydedilen veriler üzerinde değişiklik yapılabilir. Ancak RW uzantısı bulunmayan CD/DVD ve Blu-Ray'lerde kayıt bitip yazma işlemi sonuçlandırıldıktan sonra kaydedilen veriler üzerinde değişiklik yapılamaz.

⁹⁴ A.g.e, s. 211.

⁹⁵ A.g.e, s. 215.

c- Taşınabilir Bellekler



Şekil-8

Harici diskler başta olmak üzere taşınabilir bellek formatında çeşitli cihazlar mevcuttur. Bunlardan en sık kullanılanlardan bir tanesi ise USB'lerdir. Günümüzde verilerin taşınması genellikle taşınabilir bellekler aracılığıyla gerçekleştirildiği için bu cihazlar önemli bir delil elde etme aracı olarak görülmektedir⁹⁶.

İngilizce Universal Serial Bus (evrensel seri veriyolu) kelimelerinin bir kısaltması olan usb bellekler veri depolama cihazlarından biridir. Usb bellekler dışarıdan bilgisayara ya da uyumlu girişi bulunan bir diğer cihaza entegre edilerek kullanılır.

Evrensel seri veriyolu cihazları kendilerine uyumlu girişe sahip cihaza takıldıkları anda o cihaz tarafından tanınır ve işlem görmeye başlar. USB'ler basit bir dört telli bağlantıdan oluşmaktadır bu sebeple takıldıkları cihaza uyumları kolay olur.

Usb belleklerin taşıyabileceği veri kapasitesi cihazın kapasitesi ile orantılıdır. Gelişen teknoloji ile birlikte 250 GB'lık veriyi dahi taşımaya olanak sağlayan usb'ler bulunmaktadır⁹⁷.

d- Veri depolama cihazlarının hash değeri incelemesi

Dijital veriler kendi içlerinde bir "hash değeri" içerirler. Dijital verilerin incelenmesinde hash değeri verinin değiştirilip değiştirilmediğinin tespitinde kullanılır. Bir verinin yapılan işlemin başındaki hash değeri ile işlem sonundaki hash değeri farklı ise bu, verinin değiştirilmiş olduğunu gösterir.

⁹⁶ Dülger (2013), **a.g.e.**, s. 682.

⁹⁷ Usb bellekler hakkında ayrıntılı bilgi için bkz: **USB Bellekler**, http://www.arce24.com/index.php?option=com_content&view=article&id=215:usd&catid=5:ueruen&Itemid=13, (Erişim tarihi Mayıs 2013)

Hash değerinin alınması (hashing) o veriyi temsil eden sayısal bir verinin matematiksel algoritmalar kullanılarak üretilmesi sürecidir⁹⁸. Dijital veri depolama cihazlarında bulunan tüm veriler hash değeri gibi üst veriler (metadata) içerebilirler⁹⁹.

Verilerin hash değerlerinin tespit edilmesi ve işlemlerin bu doğrultuda yapılması veri güvenliği açısından önemlidir. Ancak tek güvenlik önemli olarak hash değerine itibar edilmesi de her zaman doğru sonuçları çıkarmamaktadır. Bozuk sektörler, kullanılan yazılım ve donanım ve RAM arızası gibi durumlarda veri üzerinde herhangi bir değişiklik yapılsa dahi farklı zamanlarda alınan hash değerleri birbirinden farklı çıkabilmektedir¹⁰⁰.

Bu gibi bazı teknik sebeplerle hash değerlerinde farklılıkların gözlemlenebilmesi ihtimali olsa dahi yine de verilerin hash değerlerinin işlemlere başlamadan tespit edilmesi veri güvenliği açısından yüksek öneme sahiptir.

5- Dijital Kameralar, Dijital Fotoğraf Makineleri ve Mp3 Çalarlar



Şekil- 9

Dijital Kamera ve fotoğraf makineleri, fotoğraf ve video görüntülerinin oluşturulması, düzenlenmesi ve depolanmasına olanak sağlarlar. Bu cihazlar ayrıca bilgisayar ve televizyon gibi diğer dijital cihazlara da bağlanarak veri aktarımında kullanılabilirler. Dijital kamera ve fotoğraf makinelerinde bulunan veriler taşınabilir,

⁹⁸ John Ashcroft, Deborah J. Daniels, Sarah V. Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", **U.S. Department of Justice, Office of Justice Programs**, National Institute of Justice, Nisan 2004, s. 40.

⁹⁹ **A.g.e.**, s.40.

¹⁰⁰ Yunus Balı, **Hash Değerinin Aynı Olmadığı Durumlar**, <http://www.dijitaldeliller.com/hash.html>, (Erişim Mayıs 2012)

düzenlenebilir ve tarih ve zaman bilgileri içerebilir olmaları sebebiyle potansiyel deliller olarak değerlendirilmişlerdir¹⁰¹.

Mp3 çalarlar hafızaları sebebiyle aynı zamanda taşınabilir bellek gibi kullanılabilirler. Mp3 çalarların bu özelliği gereği hafızalarında delil olarak nitelendirilebilecek verileri bulundurabilirler¹⁰².

6- Yazıcı, Faks ve Fotokopi Makineleri



Şekil- 10

Yazıcı, faks ve fotokopi makineleri de veri depolama özelliğine sahiptirler. Bu cihazların da hafızaları vardır ve buradan delil oluşturulabilecek verilere ulaşılabilir. Bu cihazlar yine hafızaları yardımıyla son yazdırılan belgeleri ve giden/gelen faks kayıtlarını da saklamaktadırlar¹⁰³.

¹⁰¹ Dülger (2013), **a.g.e.**, s. 681.

¹⁰² Dülger (2013), **a.g.e.**, s. 681.

¹⁰³ Dülger (2013), **a.g.e.**, s. 682.

7- Cep telefonları



Şekil- 11

Gelişen teknoloji ile birlikte cep telefonları da tıpkı bilgisayarlar gibi özellikler içermeye başlamıştır. Cep telefonları; arama kayıtları, rehber bilgileri, mevcut veya silinmiş kısa mesajlar, hafızası oranında fotoğraf ve video görüntüleri ve yine işlemcisi oranında bilgisayarlarda kullanılan programları içerebilirler. Özellikle akıllı telefonlar bilgisayarlara benzerlikleri sebebiyle bilgisayar incelemelerinde kullanılan metotlara tabi tutulabilirler¹⁰⁴.

8- İnternet Sistemleri

İnternetin ortaya çıkmasından bu yana tüm dünya üzerinde önemli bir ağ kurması ve günlük hayatın neredeyse her anında göz ardı edilemeyecek bir yere sahip olması sebebiyle bilişim sistemleri incelenirken internet, üzerinde önemle durulması gereken bir konu olmuştur. En genel ifade ile internet bilgisayarların birleşerek oluşturduğu bilgisayar ağıdır ve bu ağ sayesinde bilgisayarlar birbirlerindeki verilerden yararlanabilmektedir¹⁰⁵.

a- İnternetin Tarihi Gelişimi

İnternet yoluyla veri aktarımının teknik açıklamalarına geçmeden önce internetin nasıl ortaya çıktığı ve nasıl geliştiği gibi tarihsel sürece değinmekte fayda vardır. İnternet Amerika Birleşik Devletleri'nde ortaya çıkmıştır. Amerika Birleşik Devletleri Savunma Bakanlığı 1957 yılında Rusya Sputnik uydusunu uzaya

¹⁰⁴ Dülger (2013), **a.g.e.**, s. 681.

¹⁰⁵ Akıncı, Alıç ve Er, **a.g.e.**, s. 166.

göndermesinin ardından Advanced Research Project Agency (ARPA) adı altında bir birim kurmuştur¹⁰⁶. Bu birimin kurulmasının altında yatan sebep Amerikan Hükümetinin tek bilgisayardan bağımsız olarak çalışabilen bir ağ kurma fikrini ulusal güvenlik gerekçesi ile geliştirmesidir¹⁰⁷. Esasen ARPA, savaş sırasında veya savaştan önce mutlak haberleşme kanallarının kullanılmayacak şekilde tahrip edilmesinde dahi, ulusal komuta merkezi olan Başkanlık'tan balistik füze üslerine gereken emirlerin verilmesini ve savaşın sevk ve idaresini sağlayacak bir haberleşme sistemi oluşturulması için kurulmuştur¹⁰⁸.

Amerikan Hükümeti, Savunma Bakanlığı'na bağlı olan ve birbirinden uzakta olan bazı askeri birliklerin geliştirdiği projelerin ortak bir ağ üzerinden birleştirilmesi temeline dayanan ARPA'nın faaliyetleri çerçevesinde daha sonraki süreçte bu farklı sistemleri birbirine bağlamak için ARPANET adlı bir askeri bilgisayar kurulmuştur¹⁰⁹. APRANET, silahlı kuvvetler ile birlikte, savunma sanayii müteahhitlerinin ve savunma konuları ile ilgili araştırmaları yürüten üniversitelerin bilgisayar merkezlerini de içine alacak şekilde geniş bir ağ (network) kurulmasına imkan sağlamıştır¹¹⁰. 1980'li tarihlere gelindiğinde dünyanın önde gelen ülkeleri de bu ağa en azından akademik alanda dahil olmuşlardır ve 1990'lı yılların başından itibaren internet hızla yayılmıştır¹¹¹. Türkiye'de ise ilk internet bağlantısı 12 Nisan 1993 tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje kapsamında Orta Doğu Teknik Üniversitesi (ODTÜ) tarafından gerçekleştirilmiştir¹¹².

İnternetin tarihi gelişimine bakıldığında, iletişim araçları arasında en hızlı yaygınlaşan sistem olduğu çıkarımı yapılabilir. Zira, Uluslararası Telekomünikasyon Birliği'nin 1999 yılı verilerine göre, telefonun 50 milyon kişiye ulaşması 74 yıl, radyonun 38 yıl, televizyonun 13 yıl sürmesine rağmen internetin bu kitleye ulaşması 4 yıl gibi kısa bir süre almıştır¹¹³.

¹⁰⁶ İnternet ve Hukuk Workshop Çalışması, İstanbul, 2001, s. 11.

¹⁰⁷ Şaban Cankat Taşkın, **Bilişim Suçları**, İstanbul: Beta Yayıncılık, Kasım 2008, s. 13.

¹⁰⁸ İnternet ve Hukuk Workshop Çalışması, **a.g.e.**, s. 11.

¹⁰⁹ Taşkın, **a.g.e.**, s. 13.

¹¹⁰ İnternet ve Hukuk Workshop Çalışması, **a.g.e.**, s. 12.

¹¹¹ Akıncı, Alıç ve Er, **a.g.e.**, s. 169.

¹¹² Taşkın, **a.g.e.**, s. 14.

¹¹³ Dülger (2004), **a.g.e.**, s. 51.

b- İnternetin Teknik Yapısı

İnternetin bilgisayarlar arasında veri akımı sağladığından çalışmamızda bahsetmiştik. Bu veri akımı, internete bağlı bilişim cihazlarının uymak durumunda bulunduğu kurallar olarak adlandırabileceğimiz veri aktarım protokollerinden bahsetmek gerekmektedir¹¹⁴. Bu protokollerden en önemlisi TCP/IP'dir (Transfer Code Protocol/Internet Protocol). İnternet hizmetlerini kullanmak için gerekli olan tüm yazılımlar ve bağlantı yazılımları TCP/IP protokollerine uygun olarak iletişim kurar ve işlem görürler¹¹⁵. Bir diğer ifade ile TCP/IP dört katmanlı (uygulama katmanı, ulaşım katmanı, yönlendirme katmanı ve fiziksel katman) bir yapıya sahip olan internet ağ oluşumunun protokol kümelerine verilen addır¹¹⁶. Bu protokoller kümesinin ulaşım katmanında TCP, yönlendirme katmanında ise IP protokolü bulunmaktadır¹¹⁷.

İnternet üzerinden veriler küçük paketlere ayrılıp değişik sıralardan değişik yollarla gönderilirler. TCP esasen bu paketlerin sıralanmasını sağlayan protokolün adıdır. Bu sistem çerçevesinde bir kullanıcıya gönderilecek veri önce TCP tarafından paketlenir. TCP aynı zamanda bu paketleri doğru sırada numaralandırır ve adreslendirerek IP katmanına gönderir. Gönderme işlemi ile birlikte veri paketleri yola çıktığında birbirinden ayrılır ve farklı yönleri takip ederler. Kullanıcının bilgisayarına ulaşan veri paketlerinin bir bütün halinde ve tam sırasıyla görüntülenmesini sağlayan yine TCP'dir. TCP/IP protokolünün diğer protokollerden daha güvenilir olmasının sebebi ise veri paketlerini sağlam olması halinde TCP'nin onay vermesidir. Veri paketlerinde bir sorun olması durumunda ise TCP, kullanıcıya onay vermez ve kullanıcı eksikliğin farkında olup bu eksikliğini gidererek kesin iletişimi sağlamış olur¹¹⁸.

TCP/IP protokolü dahilinde her bilgisayarın tanınmasını sağlayan ve birbirinden ayıran bir IP adresi vardır. IP adresleri 32 bitlik düzende yazılırlar ancak kolay okunmaları için 8 bitlik 4 gruba ayrılırlar. İnternet üzerinde yapılan veri

¹¹⁴ Akıncı, Aliç ve Er, **a.g.e.**, s. 167.

¹¹⁵ Dülger (2004), **a.g.e.**, s. 52.

¹¹⁶ Yenidünya ve Değirmenci, **a.g.e.**, s. 39.

¹¹⁷ **A.g.e.**, s. 39-40.

¹¹⁸ **TCP/IP Protokolü**, <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html> (Erişim Mayıs 2012)

alışverişinde mutlaka göndericinin IP adresi veri tarafından taşınır. Alıcının adresi de bu sistemde çözümlenir ve gönderim gerçekleşir¹¹⁹.

IP adreslerinin iki bölümü vardır. Birinci bölüm bilgisayarın bağlı olduğu özel bir ağın numarasını ikinci bölüm ise bilgisayarın özel numarasını içerir¹²⁰. Veri dolaşımı sırasında *router*¹²¹ denilen yönlendiricilerden geçerken yalnızca bu özel ağın numarası dikkate alınır¹²².

İnternetin teknik yapısı altında bahsedilmesi gereken bir diğer önemli husus da *World Wide Web* (www) sistemidir. Sözcük anlamı itibariyle dünyayı saran ağ anlamına gelen ve kısaca web denen bu sistem tarayıcı olarak adlandırılan istenilen verilerin bulunmasını sağlayan ve web sayfası olarak adlandırılan istenilen verilerin görüntülenmesini sağlayan uygulama yazılımlarının bir araya gelmesinden oluşur¹²³.

Web sayfaları bilgisayar programlama dillerinde HTML (Hypertext Markup Language) ile yazılır. HTML dili ile çeşitli metinleri, resimleri, animasyon grafiklerini, ses dosyalarını ve video dosyaları web sayfasına aktarmak mümkündür¹²⁴.

¹¹⁹ **TCP/IP Protokolü**, <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html> (Erişim Mayıs 2012)

¹²⁰ Bilgisayarların IP adresleri aynı zamanda internet yoluyla işlenen suçlarda faili tespit etmek amacıyla sıkça kullanılmaktadır. Nereye ve kime ait olduğu bilinmeyen bir IP numarası için önce "whois" adlı bir sorgulama yapılacaktır. Whois sorgulaması internetteki alan adlarının ya da IP numarasının ait olduğu kişi ya da kuruluşlara ilişkin bilgi içerir. Bir IP numarası için yapılmış olan "whois" sorgulaması sonucunda bu IP adresinin servis sağlayıcısına ulaşılmış olunur. İlk etapta yapılacak bu basit sorgulama herkes tarafından yapılabileceği gibi sonucunda da IP adresinin hangi ülkeden ve hangi şehirden olduğu tespit edilmiş olur. Ancak araştırılan IP'nin kim tarafından kullanıldığı ortaya çıkarılmak isteniyorsa bu takdirde yasal yollardan bir araştırılma yapılması gerekmektedir. Bu bilgiye ulaşmak yargı makamlarının yaptırdıkları tespitlerle mümkündür. Böyle bir aşamada araştırılan IP numarasının belirli gün ve saate ilişkin bilgileri de verilerek numaranın kime ait olduğu servis sağlayıcıdan sorulur. Burada sorgulamanın sadece IP numarası ile yetinilmeyip mutlaka belirli gün ve saati de ekleyerek yapılması çok önemlidir. Zira aynı IP adresi bir gün içinde onlarca kişi tarafından kullanılmış olabilir. Doğru sonuçlara ulaşabilmek için sadece IP numarasının yanı sıra daha özel bilgileri de eklemek gerekmektedir. Bu sorgulamanın ardından servis sağlayıcı belirtilen IP numarasının belirtilen gün ve saate kime tahsis edildiğinin bilgilerini çıkartır. Eğer bu bilgiler bir ev bağlantısını işaret ediyorsa internet kullanıcılarına ulaşmak görece daha olasıdır. Ancak bu bağlantı bir kafe, işyeri, kütüphane gibi internet kullanımının yüksek ve kişi kontrolünün az olduğu bir yere ait ise, kullanıcıya ulaşmak oldukça güçtür. Ayrıntılı bilgi için bkz. Yunus Balı, **IP Numarası Tespiti**, http://www.dijitaldeliller.com/ip_tespiti.html, (Erişim tarihi Mayıs 1012)

¹²¹ Router internet üzerinde kullanılan paketleri varış okalarına giderken bir sonraki uğrak noktalarını belirleyen bir donanım veya kimi zaman bir yazılımdır. Router en az iki ağı birbirine bağlar ve paketlerin hangi yönde gideceğine bağlı olduğu ağların yapılarına ve durumlarına göre belirler. Routerlar olası her türlü yön hakkında ilgileri ve durumlarına ilişkin bir tablo oluştururlar. Bu bilgiyi paketlerin iletilmesi sırasında en güvenli ve en masrafsız yolu hesaplayarak yönlendirme işlemini gerçekleştirir. Bkz. TCP/IP Protokolü, <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html> (Erişim 17 Mayıs 2012)

¹²² **TCP/IP Protokolü**, <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html> (Erişim Mayıs 2012)

¹²³ Dülger (2004), **a.g.e.**, s. 52.

¹²⁴ Topaloğlu, **a.g.e.**, s. 92.

Bu başlık altında son olarak internet servis sağlayıcılarından bahsedilecektir. İnternetin oluşturduğu uluslararası ağın merkezinde birbirine bağlanmış, yüksek hızlı iletişime sahip bilgisayarlar vardır. Bu bilgisayarlara ISP (internet service provider- internet servis sağlayıcı) denilmektedir ve internete bağlanmak için öncelikle bu bilgisayarlara bağlanılmaktadır¹²⁵. İnternet servis sağlayıcılar kullanıcıların internete bağlanmalarını, internet üzerinden iletişim kurmalarını ve internetin sağladığı imkanları kullanmalarını temin eden aracı unsurlar olmaları sebebiyle internetin anahtarını elinde tutan sűjeler olarak kabul edilebilirler¹²⁶.

Türk hukuku açısından ISP'leri düzenleyen özel bir hüküm bulunmamakla birlikte ISP'lerin Türk Telekom İdaresi'nden özel bir hat temin etmeleri gerekmektedir¹²⁷. Bu şartın dışında ISP'lerin Türk Ticaret Kanunu açısından bir ticari işletme teşkil edecekleri kabul edilmekte olup mevzuatın ticari işletme veya bir ticaret şirketi kurulması ve idaresi ile ilgili hükümleri çerçevesinde belirtilen şartlara uygun olacak şekilde ISP işletmesi kurulması mümkündür¹²⁸.

II- Türk Ceza Muhakemesi Açısından Deliller

A- Genel olarak

Ceza muhakemesinde, medeni muhakemeden farklı olarak gerçekte ne olduğu araştırılır¹²⁹. Ceza muhakemesi şekli gerçekte yetinmeyip işin esasını araştırır. Bu özelliğe ceza muhakemesinde maddi gerçeğin araştırılması ilkesi denilmektedir. Ceza muhakemesinde söz konusu olan bu ilke savcılık ve mahkemenin, işin esasını bizzat araştırması ve bunu yaparken de kural olarak muhakemeye katılanların istek

¹²⁵ Yenidünya ve Değirmenci, **a.g.e.**, s. 37.

¹²⁶ İnternet ve Hukuk Workshop Çalışması, **a.g.e.**, s. 18.

¹²⁷ Topaloğlu, **a.g.e.**, s. 101.

¹²⁸ İnternet ve Hukuk Workshop Çalışması, **a.g.e.**, s. 19.

¹²⁹ Faruk Turhan, **Ceza Muhakemesi Hukuku**, Ankara: Asil Yayınevi, 2006, s. 22.

ve açıklamalarıyla bağlı olmamasını ifade eder¹³⁰. Nitekim, Yargıtay bu ilke kapsamında bazı hükümleri eksik soruşturma yapıldığı gerekçesiyle bozmaktadır.¹³¹

Bu ilke çerçevesinde ceza yargılamasının merkezine kuşkunun ortadan kaldırılması oturtulmuş ve varsayımlara dayanılarak sonuca ulaşılamaması evrensel bir ceza yargılaması ilkesi olmuştur.¹³²

Bu noktada, medeni muhakeme ile farkları daha net vurgulamak açısından söz konusu ilkenin özelliklerini belirlemekte fayda vardır. Öncelikle ceza yargılamasında mahkeme muhakemeye katılanların iddiaları ile bağlı olmadığı gibi sanığın itirafı ile de bağlı değildir (CMK 225/2). Yine bu bağlamda, sanığın duruşmaya gelmemesi halinde aleyhte sonuç çıkarılmaz. Ceza yargılamasında ispat yükü yoktur zira sanığa susma hakkı tanınmıştır. Ayrıca, medeni yargılamada tarafların ileri sürmediği iddiaları hakim kendiliğinde dikkate alamamasına rağmen ceza yargılamasında mahkeme ileri sürülen delillerle bağlı değildir, kendiliğinden delil araştırabilir.¹³³

Ceza muhakemesinde gerçekte ne yaşandığının bulunması hususunda temel ilke olan maddi gerçeğin araştırılması ilkesinin sınırını delil yasakları oluşturur. CMK m. 160'a göre Cumhuriyet savcısı ihbar veya başka bir şekilde bir suçun işlendiği şüphesi veren bir hali öğrenince kamu davası açmaya yer olup olmadığına karar vermek üzere işin gerçeğini araştırmaya başlar. Maddenin ikinci fıkrasında belirtildiği üzere, Cumhuriyet savcısı maddi gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için emrindeki adli kolluk görevlileri marifetiyle şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür. Görüldüğü üzere maddi gerçeğin bulunması ilkesi kapsamında tahkikatı yürüten savcıya bile ne pahasına olursa olsun gerçeği bulma yetkisi verilmemiş, bir hukuk devletinde olması gerektiği gibi delil yasaklarıyla bu hususa sınırlar getirilmiştir¹³⁴.

Maddi gerçeğin araştırılması ilkesine Avrupa İnsan Hakları Mahkemesi'nin verdiği kararlarda da kendini rastlanmaktadır. Bu ilke kapsamında yaşam hakkına

¹³⁰ A.g.e. s. 22.

¹³¹ Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin Saygılar, Esra Alan, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayıncılık, Ekim 2010, s. 136.

¹³² A.g.e. s. 136.

¹³³ A.g.e. s. 136.

¹³⁴ A.g.e. s. 137.

ilişkin olan Sözleşme'nin 2. maddesi çerçevesinde bireylerin hayatlarını kaybetmeleri durumunda yetkililerin etkili bir soruşturma yapma yükümlülükleri de dahil olarak kabul edilmektedir. AİHM birçok kararında Türkiye'de yaşanan ölüm olaylarında mahkemelerin etkili bir soruşturma yapmadıkları gerekçesiyle Türkiye aleyhine kararlar vermiştir¹³⁵. AİHM çeşitli kararlarda ölüm olayının yeteri kadar aydınlatılmaması¹³⁶ gerekçesiyle AİHS'nin 2. maddesinin ihlal edildiğine karar verirken çeşitli kararlarında da gözüaltına alınan kişilerin akıbetlerine ilişkin yetkili kişilerce yeterli şekilde araştırma yapılmadığını gerekçe göstererek AİHS'nin 5. maddesinin ihlal edildiğine karar vermiştir¹³⁷.

B- Türk Ceza Muhakemesinde İspat Sorunu ve Deliller

Ceza muhakemesinde, esas olarak, fiilin fail tarafından işlendiği veya işlenmediği konusunda, hukuk düzenince kabul edilen vasıtalarla, yargılama makamının tam bir kanaate ulaşmasını temin işine ispat denir¹³⁸. İspata yarayan ve hukuk düzeninin kabul ettiği vasıtalarla ise delil adı verilir¹³⁹. Delil tanımları ve delillerin özellikleri mevcut çalışmanın devamında detaylı olarak incelenecek olup burada ispat hukukunun esasları hakkında bilgi vermek daha isabetli olacaktır.

İspat hukukunun temelinde, yargılama makamlarından mahkemeyi işgal eden hakimin somut olay üzerindeki araştırması sonucunda o maddi hususu sabit görmesi

¹³⁵ Durmuş Tezcan, Mustafa Ruhan Erdem, Oğuz Sancaktar, **Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu**, Ankara: Seçkin Yayıncılık, 2002, s. 179.

¹³⁶ Bu hususa örnek olarak AİHM'nin 19 Şubat 1998 tarihli 22535/93 başvuru numaralı kararı örnek gösterilebilir. Bu kararda Komisyon Cumhuriyet Savcısı'nın ölenin güvenlik güçleriyle çatışma sırasında ölen bir terorist olduğu önyargısından hareket ettiğini belirterek ölüm olayının yeteri kadar aydınlatılmaması gerekçesiyle Sözleşme'nin 2. maddesinin ihlal edildiği kanaatine varmıştır. Ayrıntılı bilgi için bkz. **Kaya-Türkiye Kararı**, http://www.tohav.org/aihm/kaya_turkiye.pdf (Erişim tarihi Mayıs 2012) ve Turhan, **a.g.e.**, s. 23.

¹³⁷ Sözleşmenin 5. Maddesinin bu çerçevede ihlaline ilişkin olaran 14 Kasım 2000 tarihli ve 24396/94 başvuru numaralı Taş/Türkiye kararı örnek gösterilebilir. Muhsin Taş'ın gözüaltına alındıktan sonra kaybolması üzerine Mahkeme yeterli araştırma yapılmadığı gerekçesiyle AİHS'nin 5. maddesinin ihlal edildiğine karar vermiştir. Kararın ayrıntıları için bkz. **Taş-Türkiye Kararı**, www.inhak-bb.adalet.gov.tr/aihm/karar/tas.doc (Erişim tarihi Mayıs 2012) ve Faruk Turhan, "Avrupa İnsan Hakları Mahkemesi (AİHM) Kararları Işığında Kişi Özgürlüğü ve Türkiye, Gözüaltında Kayıplar, Hakim Önüne Çıkarma ve Gözüaltı Süreleri", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Haziran-Aralık 2000, Cilt:IV, Sayı 1-2, s. 204-258, http://www.hukuk.gazi.edu.tr/editor/dergi/4_10.pdf (Erişim tarihi Mayıs 2012)

¹³⁸ Veli Özer Özbek, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayınları, Ekim 2013, s. 620.

¹³⁹ **A.g.e.**, s. 620.

veya görememesi üzerine hüküm vermesi yatar¹⁴⁰. İspat hususunda öncelikle belirtilmesi gereken husus ceza muhakemesinde ispatın sağlanabilmesi için hakimi inandırmanın yeterli olmadığıdır. Hakim tam bir kanaate ulaşacaktır¹⁴¹. Yine yukarıda da açıklandığı gibi ispat hukuku çerçevesinde ceza yargılamasında ispat külfeti yoktur¹⁴². Sanığa susma hakkı veren ve sanığın kendini aklama zorunluluğu olmadığı bir sistemde ispat yükünün bulunması muhakeme sisteminin temeline ters düşecektir. Ayrıca hakimin tam bir kanaate ulaşması gerektiği için şüpheden sanık yararlanır ilkesi uygulanacaktır¹⁴³. Şüpheden sanık yararlanır ilkesinin bir sonucu olarak vicdani delil sistemi uygulanmaktadır. Günümüzde henüz tam anlamıyla bilimsel delil sistemine geçilmemiş olup vicdani delil sistemi kapsamında delillerin serbestliği ve delillerin serbest değerlendirilmesi ilkeleri söz konusudur¹⁴⁴. Vicdani delil sistemi içerisinde şüpheden sanık yararlanır ilkesi son derece önemlidir zira hakim serbestçe takdir ettiği deliller sonucunda hala bir şüpheye sahipse o takdirde bu şüphe sanığın lehine kullanılmalıdır.

Vicdani delil sistemi dahilinde ceza hakimi ne tarafların ileri sürdüğü delillerle bağlıdır ne de kanun belli hususların belli delillerle ispat edilmesi gerektiği zorunluluğu getirmiştir. Vicdani ispatın geçerli olduğu bir sistemde, ne zaman ispata ulaşılmış sayılacağı kanunla önceden tespit edilemeyeceği gibi delil araçlarının değerlendirilmesinin ölçütü de önceden hüküm altına alınmamıştır¹⁴⁵. Ceza muhakemesinde her şey delil olabilmekle birlikte delil olarak ortaya çıkarılanları ispat değerini hakim takdir edebilmektedir¹⁴⁶. Pek tabii, bu durum hakimin keyfi karar verebileceği anlamına gelmemektedir¹⁴⁷. Yetkili makamın delil araçlarını hem akıl yürütme hem de tecrübe kurallarına başvurarak değerlendirmesi sebebiyle vicdani kanaat sezgilerle değil akıl yoluyla ulaşılan bir kanaattir.¹⁴⁸ Vicdani delil

¹⁴⁰ Nurullah Kunter, Feridun Yenisey, Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, İstanbul: Beta Basım Yayım Dağıtım A.Ş., Ekim 2010, s. 1325.

¹⁴¹ Öztürk ve diğerleri, **a.g.e.**, s. 264. Anglo-Amerika hukukun bu kriteri belirtmek için makul şüphenin ötesinde (beyond reasonable doubt) terimi kullanılarak ceza yargılamasında hakimde tam bir kanaat yaratılması gerektiğinin altı çizilmiştir.

¹⁴² **A.g.e.**, s. 264.

¹⁴³ Özbek ve diğerleri, **a.g.e.**, s. 621.

¹⁴⁴ Öztürk ve diğerleri, **a.g.e.**, s. 265.

¹⁴⁵ Metin Feyzioğlu, **Ceza Muhakemesinde Vicdani Kanaat**, Ankara: Yetkin Yayınları, 2002, s. 147.

¹⁴⁶ Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1327.

¹⁴⁷ Öztürk ve diğerleri, **a.g.e.**, s. 265.

¹⁴⁸ Feyzioğlu, **a.g.e.**, s. 139.

sistemi ile ifade edilen hem delil serbestliği hem de delillerin değerlendirilmesi serbestliğidir¹⁴⁹.

Pek çok defa dile getirildiği üzere bir ceza yargılamasının temel amacı maddi gerçeğe ulaşmaktır. Bu amaç doğrultusunda öncelikle isnat edilen fiilin işlenip işlenmediği, işlenmişse söz konusu bu fiilin suç sayılıp sayılmadığı, suç teşkil ettiği halde bunun sanık tarafından mı işlendiği belirlenmeye çalışılacaktır.¹⁵⁰ Yargıç maddi gerçekliğe bu sorulara cevap vererek ulaşacaktır. Yargıç karar verirken delillere dayanacaktır. Bu sebeptendir ki, yargıcın ceza muhakemesi sonucunda maddi olayı çözmesine hizmet eden araçlara delil denir.¹⁵¹ Başka bir deyişle, yargılama konusu olayın açıklığa kavuşturulması ve maddi gerçeğin bulunabilmesi amacıyla ispat için kullanılan araçlara delil denir.¹⁵² Görülmektedir ki, ispat meselesinde hukuk düzeninin kabul ettiği vasıtalar delillerdir¹⁵³.

1- Temel İlkeler

Ceza yargılamasında deliller açısından benimsenen ve birbiriyle iç içe geçmiş iki temel ilke bulunmaktadır. Bunlar delil serbestisi ve delillerin serbest değerlendirilmesidir. Her iki kavram da ceza muhakemesi kapsamında ispat hukukunun bir ilkesi olan vicdani delil sisteminin birer parçasını oluşturmaktadır.

Yukarıda da değinildiği üzere delil serbestisi kavramı çerçevesinde ceza muhakemesinde belli hususların belli delillerle ispatı zorunlu tutulmamıştır¹⁵⁴. Delil serbestisi çerçevesinde, delillerin tüm hukuksal özellikleri taşımaları kaydıyla her şeyin ceza yargılamasında delil olarak kabul edilebileceği anlamındadır.¹⁵⁵ Öte yandan ceza yargılaması kapsamında sunulan delillerin ispat yeteneği hakim tarafından takdir edilmektedir. Bu ilke ise bilindiği üzere delillerin serbest değerlendirilmesi ilkesini oluşturacaktır.

¹⁴⁹ Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1327.

¹⁵⁰ Nevzat Toroslu, Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, Ankara: Savaş Yayınları, Eylül 2009, s. 169.

¹⁵¹ **A.g.e.**, s. 169.

¹⁵² Yener Ünver, Hakan Hakeri, **Ceza Muhakemesi Hukuku 2. Cilt**, Ankara: Adalet Yayınevi, Mayıs 2013, s. 104.

¹⁵³ Öztürk ve diğerleri, **a.g.e.**, s. 265.

¹⁵⁴ Nur Centel, Hamide Zafer, **Ceza Muhakemesi Hukuku**, İstanbul: Beta Basım Yayım Dağıtım A.Ş., Ekim 2012, s. 197.

¹⁵⁵ Ünver, Hakeri, **a.g.e.**, s. 104.

Gör÷lmektedir ki, ceza muhakemesinde medeni yargılamanın aksine somut vakıa delil yasaklarını aşmamak kaydıyla her şeyle ispat edilebilecek ve ispat amacıyla sunulan delillerin ispat yeteneęi hakim tarafından takdir edilecektir. Bu noktada çalışmanın başından beri üzerinde durulduęu üzere delil yasakları ceza muhakemesinde ispat meselesi bağlamında getirilen ilkelerin önemli bir sınırını oluşturmaktadır. Belirtilenler kapsamında öncelikle hangi özellikleri taşıyan vasıtaların delil olarak nitelendirilebileceğine bakmak isabetli olacaktır.

2- Delillerin Özellikleri

Ceza muhakemesinde somut olayı aydınlatmak amacıyla ortaya çıkarılan vasıtaların delil olarak kabul edilebilmesi için aşağıda açıklanan özellikleri taşımaları gerekmektedir.

a- Deliller gerçekçi olmalıdır.

Deliller gerçeğin bir parçası olmalı ve beş duyu ile algılanabilir olmalıdır¹⁵⁶. Deliller iç dünyada değil, elle tutulabilen dış dünyanın bir kelime ile gerçeğin (realitenin) bir parçasını oluşturmalıdır¹⁵⁷. Bu kapsamda beyan ve belgelerin varlığı ve delil olarak kabul edilebileceğinden şüphe yoktur. Aynı şekilde belirtilerin (emare) de dış dünyada varlığı nedeniyle aranılan özelliğe sahip olduklarına tereddüt edilmemelidir. Belirtilerin yargılanacak uyuşmazlık konusu olaydan daha fazla olarak daha başka olayları da temsil etmesi, genel nitelikte olması, sadece onların değerlendirmelerinin farklı olmasını gerektirir, bu durum onların delil olmalarına engel taşımaz¹⁵⁸.

¹⁵⁶ Toroslu ve Feyzioęlu, **a.g.e.**, s. 171.

¹⁵⁷ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 1328.

¹⁵⁸ **A.g.e.**, s. 1328.

b- Deliller akılcı olmalıdır.

Delil olarak kabul edilebilecek şeylerin rasyonel ve bilimsel olması gerekmektedir¹⁵⁹. Bu itibarla hükmü verecek olan hakim kanaatini gerçek dışı kanaatlere dayandıramaz. Bu bağlamda sıkça verilen bir örnekte de belirtildiği üzere hakim hükme ilişkin kanaatini bir falcının kehanetlerine dayandıramaz.

İspat hukukunda geline bu noktada delillerin akılcı olması gerektiği yönündeki anlayış insanlık tarihinin evrimi sonucu oluşmuştur. İspat vasıtalarının hiç bir düzene bağlanmadığı “ilkel safhadan” sonra dini delil safhasına geçilmiştir. Bu safhada hukuk ve din henüz ayrılmadığından masumların ilahi güçler tarafından korunacağı inancı yaygın olarak uygulanmıştır. Kızgın demir sanığın elini yakarsa suçlu olduğuna inanılmış yahut itham edenle sanık düello ettirilerek kazananın ilahi güçler tarafından korunduğu gerekçesiyle haklı olduğuna inanılmıştır¹⁶⁰. İnsanlık bu acı deneyimlerden sonra din ve hukuku ayırarak kanuni delil sistemine geçmiş ve sonraki safhada da vicdani delil sistemini uygulamaya başlamıştır.

c- Deliller olayı temsil edici olmalıdır.

Ceza muhakemesinde delillere başvurmadaki amaç maddi gerçeği bulmak olduğu için öne sürülen delillerin olayı yansıtmayı beklenir. Eğer ileri sürülen delil mevcut olayı temsil etmiyor, olayın parçalarını yansıtmıyorsa delil değeri olmadığı kabul edilir.

Delillerin olayın tamamını veya bir kısmını yansıtmayı özelliği Mülga Ceza Kanunu’nda “maksada elverişlilik” olarak yer almakta idi (CMUK m. 238/2/b,d). Eski kanunun deyişiyle delillerin maksada elverişli olması sağlam ve güvenilir olması gerekir. Bu hususları araştırarak kişi yargıya varacak olan hakimdir¹⁶¹.

¹⁵⁹ Maddi gerçeğe ulaşmada mantık yolunun izlenmesinin önemini Yargıtay 19.04.1993 tarihli bir kararında şu şekilde ifade etmiştir: “Ceza yargılamasının amacı hiç bir duraksamaya yer vermeden maddi gerçeğin ortaya çıkarılmasıdır. Bu araştırmada, yani gerçeğe ulaşmada mantık yolunun izlenmesi gerekir. Gerçek; akla uygun ve realist, olayın bütünü veya bir parçasını temsil eden kanıtlardan veya kanıtların bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa bir takım varsayımlara dayanılarak sonuca ulaşılması, ceza yargılamasının amacına kesinlikle aykırıdır” (Yargıtay CGK. 19.04.1993, 6-79/108).

¹⁶⁰ A.g.e., s.1330.

¹⁶¹ Toroslu ve Feyzioğlu, a.g.e., s. 171.

d- Deliller ispat bakımından önemli olmalıdır.

İspatına ihtiyaç duyulan hususlarla ilgili olan deliller muhakeme için önemlidir. Bu görüş CMK m. 206'da da delille ispat edilmek istenen olayın karara etkisi olması gerektiği ifadesiyle vurgulanmıştır.

e- Deliller hukuka uygun olmalıdır.

Delillerin hukuka uygun olma zorunluluğu Anayasa ile güvence altına alınmıştır. Anayasanın 38. Maddesinin 6. fıkrasına göre hukuka aykırı olarak elde edilmiş bulgular delil olarak kabul edilemez. Benzer mahiyetteki hükümlere CMK'da da yer verilmiştir. CMK m. 206/2,a'ya göre ortaya konulması istenen bir delil hukuka aykırı olarak elde edilmişse reddedilir. Yine aynı şekilde CMK m. 217/2'ye göre yüklenen suç hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir ifadesine yer verilerek ceza muhakemesinde hükme esas alınacak delillerin yalnızca hukuka uygun deliller olduğu belirtilmiştir.

Delillerin hukuka uygunluğu zorunluluğu daha ziyade temel hak ve özgürlüklerle alakalı bir meseledir¹⁶². Ceza Muhakemesi Kanunu, bir yandan devletin menfaatlerini göz önünde bulundururken bir yandan da delil elde etmek bahanesiyle temel hak ve özgürlüklerin zedelenmemesine özen göstermektedir. Böylece ispata hizmet edebilecek durumda olsa bile bazı delillerin yasaklanması cihetine gidilmiştir¹⁶³.

Bazı delillerin yasaklanması bakımında çeşitli sınıflandırmalar mevcuttur. Bazıları konu bakımından yasaklanmıştır. Örneğin CMK m. 47/3 gereğince alt sınırı 5 yıl ve daha az hapis cezasını gerektiren suçlarda devlet memurları devlet sırlarında tanıklık yapamaz. Bazıları insan haklarını ve anayasal hakları korumak için yasaklanmıştır. Örneğin çekinme hakkı olan tanık bu hakkını sonradan kullanırsa beyanı delil olamaz. Bazıları ise elde edildikleri yöntem dolayısıyla

¹⁶² Bu sebeple delillerin hukuka uygunluğu zorunluluğu Anayasanın Temel Hak ve Ödevler başlığı altında düzenlenmiştir.

¹⁶³ Toroslu ve Feyzioğlu, **a.g.e.**, s. 172.

yasaklanmışlardır¹⁶⁴. CMK m. 148’de belirtildiği üzere yasak usullerle verilmiş ifadelerin rıza dahilinde verilmiş olsa bile delil olarak kabul edilemeyeceği ifade edilmiştir.

f- Deliller müşterek olmalıdır¹⁶⁵.

Delillerin müşterek olmasından kasıt delillerin sadece hakim tarafından değil tüm taraflar tarafından bilinmesidir. Bu da delillerin ortaya konulup tartışılmasıyla sağlanır¹⁶⁶. Bu sebeple hakim olay hakkında şahsi bilgisine dayanarak karar veremez. “Hakimin olay hakkındaki şahsi bilgisine dayanmaması prensibi” delillerin müşterekliğinin bir sonucudur¹⁶⁷.

Hakimin olay hakkındaki şahsi bilgisine¹⁶⁸ dayanarak karar vermesi savunma hakkına zarar verecek bir durum oluşturur. Bu sebeple doktrinde de sıkça belirtildiği üzere CMK m. 217/1’de belirtildiği gibi şahsi bilgi sahibi olan hakim, hakimlikten çekinmeli ve tanık olmalıdır¹⁶⁹.

3- Delil Türleri

Deliller tarihten beri farklı tasniflere konu olmuşlardır. Bunların en eskilerinden biri genel ve özel nitelikteki deliller ayrımıdır. Bu ayrım kapsamında suçun maddi olarak varlığını gösteren deliller genel nitelikte deliller olarak

¹⁶⁴ Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1331.

¹⁶⁵ Yukarıda beş başlık altında incelenen delillerin özellikleri hususunda doktrinde farklı sınırlandırmalara da başvurulduğu gözlemlenmiştir. Doktrinde bazı yazarlar delillerin temelde iki özelliği haiz olmasını aramıştır. Bu kapsamda deliller (1) olayı temsil etmelidir, (2) olayı temsil eden vasıta akla, maddi gerçeğe ve hukuka uygun olmalıdır. (Ayrıntılı bilgi için Bahri Öztürk ve Mustafa Ruhan Erdem, **Uygulamalı Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayıncılık, Kasım 2008, s. 265 vd.)

¹⁶⁶ Toroslu ve Feyzioğlu, **a.g.e.**, s. 173.

¹⁶⁷ Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1332.

¹⁶⁸ Olay hakkındaki şahsi bilgiden kastedilen herkesçe bilinmeyen hususlara ait bilgilerdir. Herkesçe bilinen, maruf ve meşhur şeylere ilişkin bilgilerini hakim şu şartlarla kabul edebilir: 1) Bilginin mefruz hüküm ve soyut kaide olmayıp somut olması, 2) Hakikat olduğunun tartışılmayacağıının yerleşmiş ve yayılmış bulunması. Bu belirtilenleri Yargıtay hakimleri de bilebilecekleri için bu hususların denetimi de mümkün olacaktır. (Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1333)

¹⁶⁹ Toroslu ve Feyzioğlu, **a.g.e.**, s. 173.

adlandırılmış; suçun kim ve hangi vasıtalarla işlendiğini gösteren deliller ise özel nitelikteki deliller olarak adlandırılmıştır¹⁷⁰.

Bir diğer ayırım kapsamında deliller maddi ve şahsi deliller olarak iki grupta toplanmıştır. Maddi deliller şeylerden kaynaklanan deliller (belge gibi) olarak gösterilmiş, şahıslardan kaynaklanan deliller de şahsi deliller olarak tabir edilmiştir¹⁷¹.

Deliller hakkında değerleri bakımından yapılan bir inceleme ile ikiye ayrıldıkları da görülmektedir¹⁷². Muhakeme sırasında ispatına ihtiyaç duyulan asıl olayı ispat eden delillere doğrudan doğruya deliller denilmektedir. Bunu yanı sıra esas olaya bağlı yan olayları aydınlatmaya yarayan vasıtalar ise dolaylı delil veya belirti olarak adlandırılmaktadır¹⁷³.

Delillerin doğrudan doğruya ve dolaylı olarak tasnifiyle bağlantılı olarak deliller temsil bakımından somut olaya münhasır deliller ve genel mahiyette temsili deliller olarak ikiye ayrılmışlardır¹⁷⁴. Somut olaya münhasır deliller (tarihi deliller) ispat olunacak olayı doğrudan doğruya ispat ederler. Bunlar beyan ve belge delilleridir. Hakimin huzurunda geçmişteki olayın yerine geçilerek verilen bilgiler beyan delillerini oluştururlar. Ancak temsil hakimin gıyabında ve fakat olayı huzurunda olduğu durumlarda da delil belge delili olarak adlandırılır¹⁷⁵. Genel mahiyetteki temsili deliller ise sadece ispatı zorunlu olan olayı değil başka hususları da aydınlatan bilgiler verirler¹⁷⁶. Başka bir deyişle bu mahiyetteki deliller olaydan geriye kalan iz ve eserlerdir¹⁷⁷. Bu tür deliller ispat edilecek hususun dışında başka hususları da gösterdikleri için sağlamlıklarını araştırmak gerekmektedir¹⁷⁸. Bu tür delillere belirtiler denilmektedir. Belirti delillerine yan delil veya delil başlangıcı da denilmektedir ve ancak başka delillerle desteklendikleri takdirde hakim daha kolay vicdani kanaate ulaşabilecektir¹⁷⁹. Belirtiler dava konusu olayı açıklığa

¹⁷⁰ Toroslu ve Feyzioğlu, **a.g.e.**, s. 175.

¹⁷¹ Toroslu ve Feyzioğlu, **a.g.e.**, s. 176.

¹⁷² Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 1344.

¹⁷³ Centel ve Zafer, **a.g.e.**, s. 200.

¹⁷⁴ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 1343.

¹⁷⁵ **A.g.e.**, s. 1344.

¹⁷⁶ **A.g.e.**, s. 1344.

¹⁷⁷ Centel ve Zafer, **a.g.e.**, s. 200.

¹⁷⁸ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 1344.

¹⁷⁹ Centel ve Zafer, **a.g.e.**, s. 200.

kavuşturmada vasıta olarak kullanıldıklarından belirtilerin de bir delil çeşidi olarak kabul edilmeleri gerekmektedir¹⁸⁰.

Yukarıda belirtilenler ve yapılan farklı tasnifler ışığında doktrinde yapılan farklı ayırmalar şu şekilde özetlenebilir: Bazı yazarlar delilleri 1)Beyan, 2) Belge, 3) Belirtili şeklinde üç gruba ayırarak incelemişlerdir¹⁸¹. Bazı yazarlar 1) Sanık açıklamaları, 2) Tanık açıklamaları, 3) Sanık ve tanıktan başka kişilerin açıklamaları, 4) Yazılı açıklamalar, 5) Görüntü veya ses kaydeden açıklamalar, 6) Belirtiler şeklinde bir tasnife başvurmuşlardır¹⁸². Bazı yazarlar 1) Yasal deliller, 2) Vicdani deliller, 3) Bilimsel deliller şeklinde ayırmışlardır¹⁸³. Bazı yazarlar 1) İtiraf, 2) Şahadet, 3) Belge delilleri ve bilimsel deliller şeklinde bir tasnifi benimsemiştir¹⁸⁴. Bazı yazarlar ise 1) Sanık beyanı, 2) Tanık beyanı, 3) Belge delilleri, 4) Belirti delilleri ve bilimsel deliller, 5) Bilirkişi mütalaası ve 6) Keşif olarak sınıflandırmışlardır¹⁸⁵.

Delilleri beyan, belge ve belirti olmak üzere üç başlık altında inceleyen Kunter'e göre tüm delillerin ispat edilecek hususu temsil ettikleri baştan kabul edilmektedir. Bu kapsamda deliller temsil yönünden a) somut olaya ilişkin temsili deliller ve b) genel nitelikte temsili deliller olmak üzere iki başlığa ayrılmaktadır¹⁸⁶. Somut olaya ilişkin temsili deliller ispat olunacak olayı doğrudan doğruya temsil eden delillerdir. Bu deliller beyan ve belge delili olmak üzere iki çeşittir¹⁸⁷. Geçmişte yaşanan olayı doğrudan doğruya temsil etmeleri sebebiyle bu delillere "tarihi deliller" de denilmektedir.

Geçmişte yaşanmış bir olayı hakimnin hayalinde canlandırmayı sağlayan temsil görevi iki şekilde yerine getirilebilir. Birinci durumda beyan delilleri aracılığıyla geçmişteki olayın yerine geçiş hakimnin huzurunda ve daima olayın gıyabında olacaktır. Tanık beyanı örneğinde olduğu gibi, tanığın olaya ilişkin anlattıkları her zaman hakimnin huzurunda ancak olayın gıyabında olacaktır. İkinci durumda ise

¹⁸⁰ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 1344 vd.

¹⁸¹ Bkz. Kunter, Yenisey, Nuhoglu, Yener ve Hakeri ve Toroslu ve Feyzioğlu kitaplarında bu konuda yazarlar üçlü ayırımı benimsemiştir.

¹⁸² Bkz. Öztürk ve diğerleri, **a.g.e.**, s. 266 vd.

¹⁸³ Öztekin Tosun, **Türk Suç Muhakemesi Dersleri**, I. Cilt, İstanbul: İstanbul Üniversitesi Yayınları, 1981, s. 585.

¹⁸⁴ Faruk Erem, **Diyaletik Açından Ceza Yargılaması Hukuku**, Ankara: Işın Yayıncılık, 1986, s. 290 vd.

¹⁸⁵ Centel ve Zafer, **a.g.e.**, s. 201 vd. Sınıflandırmaların çeşitliliği konusunda ayrıntılı bilgi için bkz. Özbek ve diğerleri, **a.g.e.**, s. 621.

¹⁸⁶ Toroslu ve Feyzioğlu, **a.g.e.**, s. 176.

¹⁸⁷ Nurullah Kunter, **Ceza Muhakemesi Hukuku**, İstanbul: Yaylacık Matbaası, 1989, s. 628.

geçmişteki olayın yerine geçiş hakimın gıyabında ancak pek çok defa olayın huzurunda belge delilleri aracılığıyla olabilir¹⁸⁸.

Genel nitelikteki temsili deliller ise sadece ispat edilecek hususu değil, bunun yanı sıra başka hususları da ispat edebilecek delillerdir. Bunlar ceza muhakemesi sisteminde belirtiler (emareler) olarak anılmaktadır. Belirtiler genel mahiyette ve başka hususları da ispat edebilecek özellikte oldukları için ceza muhakemesi süreçlerinde bu delillerden faydalanmak için tenkidi bir araştırma yapmak gerekliliğe işaret edilmektedir. Belirtilerin, ispatı istenen hususu da temsil edip etmediklerini yani sağlamlıklarını araştırmak lazımdır. Belirtilerin sağlamlıkları araştırma gereği olduğunda onlara bir diğer ifade ile “tenkidi deliller” de denilmektedir¹⁸⁹.

Belirtilen açıklamalar doğrultusunda mevcut çalışmamızın devamında deliller beyan, belge ve belirti ayırımına sadık kalınarak incelenecektir. Bu kapsamda çalışmamızın esas konusu olan dijital delillerin beyan, belge veya belirti delillerinden hangi kategoriye dahil olduğunu incelemeye geçmeden önce bu üç türün kısaca açıklamalarına yer vermekte fayda olacağı kanaatindeyiz.

a- Beyan Delilleri

Beyan delilleri çalışmamızda ifade edildiği üzere doğrudan doğruya mevcut olayı ispat gücüne sahip delillerden kabul edilmektedir. Beyan delilleri tanık beyanı, şüpheli veya sanık beyanı ve şüpheli ve sanıktan başka tarafların (katılanın, mağdurun, şikayetçinin, malen sorumlunun) beyanı olmak üzere üç başlık altında incelenmektedir¹⁹⁰.

¹⁸⁸ A.g.e., s. 628.

¹⁸⁹ A.g.e., s. 628.

¹⁹⁰ Toroslu ve Feyzioğlu, a.g.e., s. 176.

i. Tanık beyanı

Tanıklar, uyuşmazlığın konusunu oluşturan olay hakkında suç muhakemesinde beş duyuları aracı ile bildiklerini hakime açıklayan taraflardan başka kişilerdir¹⁹¹. Tanık beyanı ise, olayın tanığı olan kişinin olayla ilgili bilgilerini dinlemeye yetkili makam ve kişiler önünde sözlü olarak açıklamasıdır. Tanık beyanı esasen tanığın yetkili mahkeme veya hakim huzurunda sözlü olarak yaptığı açıklamalar olsa da CMK m. 54'e göre soruşturma evresinde Cumhuriyet savcısının da tanık dinleyebileceği kabul edilmiştir. Tanığın, tanık dinlemeye yetkili olmayan makamlar veya kişiler önünde yaptığı sözlü açıklamaların tutanağa geçirilmesi halinde bu tutanaklar belge delili olarak kabul edilirler¹⁹².

Tanıklık kurumuna ilişkin kanuni düzenlemeler 5271 sayılı Ceza Muhakemesi Kanunu'nun 45 ve devamında yer alan maddelerde düzenlenmiştir. Bu maddeler kapsamında belirtilen şekilde çağrılan tanık kendisi çağırılan mahkeme veya hakim önüne gelmek zorundadır. Usulüne göre çağırılmasına rağmen mazeret bildirmeksizin gelmeyen tanık zorla getirilir ve gelmemesi üzerine sebep olduğu giderler kamu alacaklarının tahsili usulü gereğince tanığa yüklenir (CMK m. 44).

Esasen ehliyet şartı aranmaksızın herkesin tanık olabileceği kabul edilmiştir. Ancak kanunda tanıklık görevini üstelenecek kişilere sanık veya şüpheliyle olan yakınlık derecesi veya meslekleri sebebiyle bu görevden çekinme imkanları tanınmıştır. Sanık veya şüpheliyle olan yakınlığı sebebiyle çekinme hakkı tanınanlar kanunda şu şekilde sıralanmıştır:

Madde 45 - (1) Aşağıdaki kimseler tanıklıktan çekinebilir:

- a) Şüpheli veya sanığın nişanlısı.*
- b) Evlilik bağı kalmasa bile şüpheli veya sanığın eşi.*
- c) Şüpheli veya sanığın kan hısımlığından veya kayın hısımlığından üstsoy veya altsoy.*
- d) Şüpheli veya sanığın üçüncü derece dahil kan veya ikinci derece dahil kayın hısımları.*

¹⁹¹ Kunter, **a.g.e.**, s. 742. Ayrıca bkz. Toroslu ve Feyzioğlu, **a.g.e.**, s. 176.

¹⁹² Toroslu ve Feyzioğlu, **a.g.e.**, s. 177.

e) Şüpheli veya sanıkla aralarında evlâtlık bağı bulunanlar.

(2) Yaş küçüklüğü, akıl hastalığı veya akıl zayıflığı nedeniyle tanıklıktan çekinmenin önemini anlayabilecek durumda olmayanlar, kanunî temsilcilerinin rızalarıyla tanık olarak dinlenebilirler. Kanunî temsilci şüpheli veya sanık ise, bu kişilerin çekinmeleri konusunda karar veremez.

(3) Tanıklıktan çekinebilecek olan kimselere, dinlenmeden önce tanıklıktan çekinebilecekleri bildirilir. Bu kimseler, dinlenirken de her zaman tanıklıktan çekinebilirler.

Meslek ve sürekli uğraşları sebebiyle kanunen tanıklıktan çekinme imkanı tanına kimseler ise yine CMK madde 46'da şu şekilde ifade edilmiştir:

Madde 46 - (1) Meslekleri ve sürekli uğraşları sebebiyle tanıklıktan çekinebilecekler ile çekinme konu ve koşulları şunlardır:

a) Avukatlar veya stajyerleri veya yardımcılarının, bu sıfatları dolayısıyla veya yüklendikleri yargı görevi sebebiyle öğrendikleri bilgiler.

b) Hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğer bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler.

c) Malî işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişiler hakkında öğrendikleri bilgiler.

(2) Yukarıdaki fıkranın (a) bendinde belirtilenler dışında kalan kişiler, ilgilinin rızasının varlığı halinde, tanıklıktan çekinemez.

Meslekleri sebebiyle tanıklıktan çekinebilme imkanı bulunanlar ile sanık veya şüpheliyle olan yakınlık dereceleri sebebiyle tanıklıktan çekinme imkanı bulunanlar arasında önemli bir fark bulunmaktadır. Bu kapsamda CMK madde 46'da belirtilen mesleklere sahip kişilerin kural olarak tanıklıktan çekinmesi zorunludur. Ancak sır sahibinin rızasının varlığı halinde ise bu kişilerin tanıklık yapması zorunlu tutulmuştur¹⁹³.

¹⁹³ A.g.e., s. 184.

CMK’da belirtildiği üzere tanıklar yemin altında dinlenmektedir. tanıklara öncelikle gerçeği söylemesi gerektiği, söylememesi halinde TCK’da düzenlenen yalan tanıklık suçunun oluşacağı belirtilir (CMK m. 53). Böylece tanığa yapacağı işin önemi hatırlatılmış olur. Bunlar belirtildikten sonra tanığa doğruyu söyleyeceğine dair yemin ettirilir. Tanıklar “Bildiğimi dosdoğru söyleyeceğime namusun ve şerefim üzerine yemin ederim” ifadesini kullanarak mahkemede yemin ederler (CMK m. 55). CMK 54. madde kapsamında gerektiğinde ya da bir kimsenin tanık olarak dinlenmesinin uygun olup olmadığı konusunda tereddüt varsa yemin tanığın beyanını vermesinin sonrasına da bırakılabilir.

CMK m. 60’a göre kanuni bir sebep olmaksızın yemin etme zorunluluğunu yerine getirmeyen tanık için iki tür müeyyide öngörülmüştür: (a) Yemin etmekten çekinmesi sebebiyle doğan giderler tanığa yüklenir, (b) Yemine zorlamak amacıyla disiplin hapsi uygulanır. Uygulanacak disiplin hapsi tanığın dinleneceği dava hakkında hüküm verilinceye kadar devam edebilir ancak her halde üç ayı geçemeyecektir. Bu müeyyideler ancak mahkemeler veya hakimler tarafından uygulanacağı gibi aynı zamanda söz konusu müeyyidenin uygulanması esnasında tanık yemin ederse derhal serbest bırakılacaktır¹⁹⁴.

Tanığın yükümlülükleri olduğu gibi hakları da mevcuttur. Tanıklıktan çekinme imkanı özel durumları sebebiyle kanunda belirtilen kişilere tanınmış bir haktır. Bunun yanı sıra CMK madde 51 kapsamında beyan vermekten çekinme hakkı bulunan tanığın yeminden çekinme hakkı da mevcuttur. Ayrıca tanık CMK madde 61’de belirtildiği üzere, devlet tarafından ödenecek, tanığın kaybettiği zamanı, seyahat ve konaklama giderlerini karşılayacak bir tazminat alma hakkına da sahiptir. Ancak tanıklara tanınmış haklar arasında en önemlisi CMK’da belirtilen hakların yanı sıra 5726 sayılı Tanık Koruma Kanunu kapsamında tanığın tanıklık görevini yerine getirmesi nedeniyle karşılaşılabileceği tehlikelerden korunması hakkıdır¹⁹⁵.

¹⁹⁴ A.g.e., s. 180.

¹⁹⁵ A.g.e., s. 182 vd.

ii. Şüpheli veya sanık beyanı

CMK madde 2’de belirtilen tanımlar çerçevesinde şüpheli soruşturma evresinde suç şüphesi altında bulunan kişiyi; sanık ise kovuşturmanın başlamasından itibaren hükmün kesinleşmesine kadar suç şüphesi altında bulunan kişiyi ifade eden kavramlardır. Bu tanımlardan çıkarıldığı üzere suç şüphesi altında bulunan kişiye kovuşturma evresinde şüpheli adı verilirken kovuşturma evresine geçildiğinde suç şüphesi altında bulunan kişinin sıfatı sanık olmakta ve bu sıfat hüküm kesinleşinceye kadar devam etmektedir.

Sanık veya şüpheli kişi istisnai bazı durumlar haricinde suç teşkil eden fiili işeyip işlemediğini en iyi bilen kişidir. Bu sebeple eğer ki açıklamaları doğruysa çok değerlidir¹⁹⁶. Ancak pek çok zaman sanık beyanında doğruyu söylememektedir, zira sanık veya şüpheli suçlu ise gerçeği gizlemesinde fayda olacağı görüşü ile de doktrinde karşılaşılmaktadır¹⁹⁷. Sanık veya şüpheli suçu işlediği sabit görüldüğünde bir ceza ile karşılaşacağı bilincinde olduğu için bu cezadan kaçma eğilimi sergiler ve bu sebeple de doğruyu söylemekten kaçınması sıkça karşılaşılan bir durum oluşturmaktadır¹⁹⁸. Tam ters bir yönde sanık muhakeme süreci boyunca istikrarlı bir şekilde suçu kabul de edebilir. Ancak sanığın her beyanını takdir yetkisi yine mahkemeye veya hakime aittir. Zira şüpheli veya sanığın başkasının işlediği suçu çeşitli nedenlerle üstlenme eğilimi göstermesi ve bu sebeple de sürekli olarak suçu kabul etmesi de hakimlerin birçok durumda karşısına çıkmaktadır.

Esasen TCK kapsamında da sanığa doğruyu söyleme yükümlülüğü yüklenmemiştir. Sanık olayla ilgili olarak doğruyu söylemek ve aleyhinde beyanda bulunmak zorunda değildir. Bu kapsamda şüpheli veya sanığa beyanıyla ilgili yüklenen tek yükümlülük kimliğini doğru olarak söylemesidir (CMK m. 147).

Şüpheli veya sanık yalnızca hakim tarafından sorguya çekilebilir. Şüpheli veya sanığın savcılık veya kollukta verdiği beyan ifade olarak kabul edilmektedir. İfadesi alınacak veya sorgusu yapılacak olan şüpheli veya sanığın öncelikle kimliği tespit edilir. Ardından kendisine isnat edilen suç açıklanır. Şüpheli veya sanığa müdafî tutma hakkı olduğu belirtilir. Müdafinin ifade ve sorgusunda yanında bulunabileceği

¹⁹⁶ Tosun, **a.g.e.**, s. 753.

¹⁹⁷ Toroslu ve Feyzioğlu, **a.g.e.**, s. 191.

¹⁹⁸ Tosun, **a.g.e.**, s. 753.

açıklanır. Eğer şüpheli veya sanığın müdafî tutacak durumu yoksa ancak bir müdafiden faydalanmak istiyorsa kendisine barodan görevli bir müdafî atanır. Sanığa kendisine isnat edilen suç hakkında açıklamada bulunma zorunluluğu olmadığı, susma hakkının olduğu açıklanır. Yine bu kapsamda sanığa şüpheden kurtulması için somut delillerin toplanmasını isteyebileceği hatırlatılır ve kendisi aleyhine var olan şüphe nedenlerini ortadan kaldırmak ve lehine olan hususları ileri sürmek olanağı tanınır.

Şüpheli veya sanığın beyanı özgür iradesine dayanmalıdır. Özgür iradeye dayanmadan verilen beyan rıza dahilinde verilmiş olsa bile delil olarak değerlendirilemeyecektir (CMK m. 148). Yine şüpheli veya sanık hakim önünde ikrarda bulunsa bile bu ikrarın da şüpheli veya sanığın özgür iradesine dayanması gerekmektedir. Ancak özgür iradeyle verilmiş olan ikrar dahi vicdani delil sistemi çerçevesinde hakimi bağlamayacaktır.

Şüpheli veya sanık susma hakkını kullanmayıp beyanda bulunmayı tercih ettiği takdirde şüpheli veya sanığın beyanı üç farklı şekilde değerlendirilmektedir. Söz konusu bu beyan öncelikle Anglosakson hukuk sistemlerinde olduğu gibi “yeminli beyan” olarak değerlendirilebilir. Bu kapsamda şüpheli veya sanık isnat edilen suçu kabul etmezse kendi aleyhindeki davada tanık gibi yeminli olarak beyanda bulunacaktır. Bu sistem dahilinde sanık, tanık gibi yeminli beyanda bulunmakla susma hakkını kullanmak arasında bir tercihte bulunacaktır. Ancak yemin altında beyanda bulunan tanık yalan tanık durumuyla da karşı karşıya kalabileceği için bu sistem tanığın beyana bulunma imkanını kısıtlamakta ve hakim veya mahkemeyi de mevcut olayın aydınlatılması açısından önemli olan şüpheli veya sanık beyanından da mahrum edebilmektedir.

Bir diğer sistemde şüpheli veya sanık beyanı çekinme yetkisi olup yeminsiz dinlenen tanık beyanı gibi kabul edilmektedir. Bu sistemde de yine şüpheli veya sanığın beyanı yalan tanıklık suçu tehlikesinde kaldığı için aynı sakıncaları içermektedir.

Üçüncü olarak ise tanık beyanı yeminli ya da yeminsiz her türlü sanık beyanından farklı değerlendirilmektedir. Ülkemizde ve diğer kıta Avrupası hukuk sistemini kullanan ülkelerde olduğu gibi bu sistemde tanık beyanı ile sanık beyanı birbirinden ayrıştırılmış ve sanığa yemin ettirilmeden ve doğruyu söyleme

yükümlülüğü yüklenmeden beyanda bulunma imkanı tanınmaktadır. Böylece sanık doğruyu söylemediği takdirde bir cezalandırma ile karşılaşmamaktadır¹⁹⁹.

iii. Şüpheli veya sanık dışında kalan tarafların beyanı

Ceza muhakemesinde şüpheli veya sanık dışında kalan taraflar deyiminin içine mağdur, şikayetçi, katılan ve malen sorumlu olan kişiler girmektedir. CMK madde 233'e göre bu kişilere çağrı yönünden tanıklara ilişkin hükümler uygulanmaktadır. Ayrıca bu kişiler tanık olarak da dinlenebilir. Ancak bu kişiler tanık değildir, bu sebeple yeminsiz dinlenirler ve yalan beyanda bulundukları takdirde yalan tanıklık suçundan değil, ancak katılanın karşılaşacağı iftira suçu gibi başka suçlarla karşılaşabilirler²⁰⁰.

b- Belge Delilleri

Belge, somut bir olayı temsil eden ve insan yapısı olan bir ispat vasıtası olarak kabul edilmektedir²⁰¹. Suç teşkil eden olay hakkında insanların açıklamaları olduğu kadar o olayı temsil edici yazılı açıklamalar da olmaktadır²⁰². Belge delilleri sadece yazılı deliller olmakla sınırlandırılmamıştır. Belge delilleri (a) yazılı belgeler, (b) şekil tespit eden belgeler, (c) ses ve/veya görüntü tespit eden belgeler olarak üçe ayrılarak incelenmektedir²⁰³.

¹⁹⁹ Şüpheli veya sanık beyanına ilişkin uygulanan üç sisteme dair detayı bilgi için bkz. Kunter, **a.g.e.**, s. 646 vd.

²⁰⁰ Toroslu ve Feyzioğlu, **a.g.e.**, s. 194.

²⁰¹ **A.g.e.**, s. 195.

²⁰² Tosun, **a.g.e.**, s. 759.

²⁰³ Centel ve Zafer belge delillerinin bu tasnifini şu şekilde açıklamaktadır: “Belge delilleri, somut olayı birebir temsil eden delillerdir. Olayın taşıyıcısı insan olduğunda *tanıktan*; bir nesne olduğunda ise *belgeden* söz etmekteyiz. Olay yazıya döküldüğünde olayın taşıyıcısı yazılı bir belge, ses olarak tespit edildiğinde ses bandı, hem şekil hem ses olarak taşındığında taşıyıcı dar anlamda bir film şeridi veya CD olacaktır.” Bu ifadeleri kullanmakla birlikte Centel ve Zafer CMK 214’de bir belgenin okunmasından bahsediyor olması sebebiyle bu tür delilleri belirti olarak kabul etmiştir. Center, Zafer, **a.g.e.**, s. 244-245

Belgenin mevcut olayı temsil ediři çok defa olay anında ve huzurunda olarak kabul edilmektedir. Suret ve fotokopi gibi belgenin belgesi de yine belge delili olarak görülür çünkü bunlar da olayı gıyabında temsil ederler²⁰⁴.

Belgeler çoğunlukla olay anında ve huzurunda düzenlendiği için hata ihtimali daha azdır ve bu sebeple belgeler içerikleri açısından beyandan daha sağılan görülürler²⁰⁵. Doktrindeki bir görüşe göre belge delillerinin kim ya da kimler tarafından yazıldığının bir önemi yoktur. Bunlar anonim de olabilirler²⁰⁶. Ancak bu konudaki asıl sorun belgenin sağıamlığının tespit edilmesidir. Bunun için belgenin sağıamlık derecesi onu düzenleyenin uyandırdığı güven derecesine bağılanmaktadır²⁰⁷.

Türk Ceza Kanunu'nun gerekçesinden belgenin kime ait olduğunun belli olması gerektiğinin altı çizilmiştir²⁰⁸. Belgenin aidiyetinin tespiti dijital deliller içinde büyük bir önem arz etmektedir. Çalışmamızın yukarıdaki bölümlerinde de değindiğimiz üzere, aidiyeti tespit edilemeyen yazıların belge niteliğiyle muhakemeye etki etmesi hukuka aykırı sonuçlar çıkartabilmektedir²⁰⁹.

i. Yazılı belgeler

Yazılı belgeler bir olayı nakleden veya bir irade beyanını içeren her türlü yazıdır²¹⁰. Yazılı belgeler resmi belge ve özel belge olmak üzere iki gruba ayrılır. Bir memurun görevi nedeniyle düzenlediği yazılı belgeye resmi belge denmektedir²¹¹. Resmi belgeler (a) aksi sabit oluncaya kadar geçerli resmi belge ve (b) sahteliği sabit oluncaya kadar geçerli resmi belgeler olmak üzere ikiye ayrılır²¹².

²⁰⁴ Kunter, **a.g.e.**, s. 651.

²⁰⁵ **A.g.e.**, s. 651.

²⁰⁶ Öztürk ve diğerleri, **a.g.e.**, s. 295.

²⁰⁷ Kunter, **a.g.e.**, s. 651.

²⁰⁸ **Türk Ceza Kanunu Madde Gerekçeleri**, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim tarihi Mayıs 2012)

²⁰⁹ Bkz. Dipnot 53.

²¹⁰ Toroslu ve Feyzioğlu, **a.g.e.**, s. 195.

²¹¹ Toroslu ve Feyzioğlu, **a.g.e.**, s. 195.

²¹² Kunter, **a.g.e.**, s. 652.

Resmi belgelerin dışında kalan yazılı belgeler ise özel belge olarak kabul edilmektedir²¹³.

ii. Şekil tespit eden belgeler

Şekil tespit eden belgeler belli bir olayı temsil etmek üzere olayın şeklinin tespit edildiği belgelerdir²¹⁴. Yazılı belgeden bilgi edinme okuma aracılığıyla olduğu halde şekil tespit eden belgelerde bilgiye ulaşma görme ve inceleme ile olur. Bu tür belgelerin içine fotoğraf, resim, alçı ya da sair malzemelerle alınan kalıplar gibi şekiller girmektedir. Şekil tespit eden belgelerin de hileli olabileceği söz konusu olduğundan (Örneğin; çeşitli fotoğraf programları kullanılarak değiştirilen fotoğraflar) sahtelik iddiasında bulunulabilir²¹⁵.

iii. Ses ve/veya görüntü tespit eden belgeler

Ses ve/veya görüntü tespit eden belgelerin ceza muhakemesindeki yeri oldukça tartışmalıdır. Doktrinde bazı yazarlar bu tür belgeleri delil olarak kabul etmekte iken bazı yazarlar ise bunların belirti olduğunu ileri sürmektedir²¹⁶.

Bu tür belgeler hakkındaki en büyük sıkıntı bunlar üzerinde kolayca değişiklik yapılabilmesidir. Bu sebeple ses ve/veya görüntü tespit eden araçlarla elde edilmiş belgelerin ispat gücünün zayıf olduğu kabul edilmektedir²¹⁷. Öte yandan bu tür belgelerin kişilerin kişilik haklarına zarar vermesi de söz konusudur. Bu noktada ses ve/veya görüntü kaydeden bantların usulüne uygun olarak alınmış ve mahkemeye sunulmuş olması ile bu tür bantların usulüne uygun olmadan alınmış ve mahkemeye sunulmuş olması arasında bir ayırım yapılmalıdır²¹⁸.

²¹³ Toroslu ve Feyzioğlu, **a.g.e.**, s. 195.

²¹⁴ Toroslu ve Feyzioğlu, **a.g.e.**, s. 196.

²¹⁵ Kunter, **a.g.e.**, s. 653.

²¹⁶ Belirti olarak kabul edenler için bkz. Center ve Zafer, **a.g.e.**, s. 244. Delil olarak kabul edenler için bkz. Öztürk ve diğerleri, **a.g.e.**, s. 297.

²¹⁷ Toroslu ve Feyzioğlu, **a.g.e.**, s. 196.

²¹⁸ Öztürk ve diğerleri, **a.g.e.**, s. 297.

Usulüne uygun olarak doldurulup muhafaza altına alınmış ve usulüne uygun olarak mahkemeye delil olarak sunulmuş²¹⁹ olan ses ve/veya görüntü içeren belgelerin delil olarak kabul edilmesi söz konusudur. Zira ceza muhakemesinde vicdani delil sistemi uygulandığı için hukuka uygun her şey delil olabilmektedir ve hakim de bu delilleri serbestçe değerlendirme yetkisi bulunmaktadır²²⁰.

Bu doğrultuda, Öztürk'ün değerlendirmesine göre, usulüne uygun olarak alınmış, muhafaza edilmiş ve mahkemeye sunulmuş ses ve/veya görüntü bantlarındaki tespitler tek başlarına mahkumiyet kararı verilmesi için yeterli görülmemektedir. Bunların başka delillerle de desteklenmeleri gerekmektedir. Usulüne uygun olmadan oluşturulmuş ve mahkemeye sunulmuş ses ve/veya görüntü bantları ise hiç bir şekilde delil vasfını taşıyamazlar. Ancak bu tür bantlar sadece belirti olarak değerlendirilebilir²²¹.

Öztürk usulüne uygun olmadan oluşturulmuş ses ve/veya görüntü bantlarının delil değeri olmadığını ancak sadece belirti olarak değerlendirilebileceklerini belirtmiştir. Fakat kanaatimizce bu görüş isabetli değildir. Öncelikle belirtiler de bir delil türüdür ve belirtiler olayların dolaylı olarak ispatına yardımcı olurlar. Çalışmamızın delil türleri başlığında da belirttiğimiz üzere dolaylı olarak ispat amacıyla kullanılan belirtileri tamamen delil türleri arasından çıkartmanın sıhhatli sonuçlar oluşturmayacağı kanaatindeyiz²²².

Öte yandan Öztürk delil türlerini sanık açıklamaları, tanık açıklamaları, yazılı açıklamalar, sanık ve tanıktan başka kişilerin açıklamaları, görüntü veya ses kaydeden açıklamalar ve belirtiler şeklinde altı başlık halinde incelemektedir²²³. Dolayısıyla usulüne uygun olarak oluşturulan ve sunulan ses ve/veya görüntü kaydeden açıklamalar bu altı başlıktan beşincisine girecek olup delil serbestisi gereği delil olarak değerlendirilebilecektir. Ancak usulüne uygun olmayarak oluşturulan ses ve/veya görüntü kaydeden açıklamalar yine delil türleri arasında yer alan altıncı başlık olarak belirti delilleri kapsamında ele alınabilecektir.

²¹⁹ Örneğin; 298 Sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanunun 55. maddesinde ses veya görüntü bantlarının nasıl doldurulup muhafaza edilmesi gerektiği açıkça belirtilmektedir. Burada belirtilen usullerle alınan, saklanan ve mahkemeye sunulan belgeler delil olarak kabul edilebilecektir. Bkz. Öztürk ve diğerleri, **a.g.e.**, s. 297.

²²⁰ **A.g.e.**, s. 429.

²²¹ **A.g.e.**, s. 430 vd.

²²² Bkz. s. 39-42. Çalışmamızda delil türleri Kunter'in benimsediği beyan, belge ve belirti delilleri ayırımına sadık kalınarak incelenmiştir.

²²³ Öztürk ve diğerleri, **a.g.e.**, s. 266.

Bu noktada belirtmekte fayda vardır ki usulüne uygun olmayan ses ve/veya görüntü tespit eden belgeler hukuka aykırı delil niteliği taşır ve hukuka aykırı olan delillerin hangi delil türü başlığı altında yer aldığının bir önemi olmamalıdır. Zira “zehirli ağacın meyvesi de zehirli olur” anlayışının hakim olduğu hukuka aykırı deliller, çalışmamız kapsamında ileride de değineceğimiz üzere, yok hükmünde kabul edilirler. Belirtilen bu sebeplerden ötürü ses ve/veya görüntü tespit eden belgelerin usulüne uygun olmaması halinde yalnızca belirti olarak değerlendirilmeleri onlara hukuk sistemi içerisinde görece az bir rol vermiş olduğu için adalet yaratmaz. Usulüne uygun olarak oluşturulan ses ve/veya görüntü tespit eden belgelerin içerdikleri güven sorunu sebebiyle başka delillerle desteklenmesi gerektiği savunuluyorsa, o halde usulüne uygun olmayan bu tür belgeler hukuka aykırı olmaları sebebiyle yok hükmünde kabul edilmeli ve hiçbir şekilde delil ve/veya belirti olarak değerlendirilmemeleri gerekmektedir.

c- Belirti delilleri ve bilimsel deliller

Belirti delilleri olaydan geriye kalan her türlü iz ve eserlerdir²²⁴. Başka bir deyişle, ispat edilecek olayın dolaylı olarak ispatına yardımcı olan vakıalara ve izlere belirti denmektedir²²⁵.

Ceza muhakemesi hukukunda belirtilerin delil olup olmadığı konusunda bir tartışma mevcuttur. Erem belirtilerin deliller ile aynı anlamı taşımadığını iddia etmiş ve belirtilerin hüküm için yeterli olmadığını belirterek belirtilerin asla delil olmadığını vurgulamıştır²²⁶. Bu görüşün tam tersine doktrinde belirtilerin delil olduğu kabul edilmektedir²²⁷. Ayrıca delil serbestisi kuralları olan ve delillerin serbestçe takdiri söz konusu olan ceza muhakemesi hukukunda belirti delilleri son derece önemlidir ve gerçeği aydınlatmaya yardımcı olmaktadır²²⁸.

²²⁴ Centel ve Zafer, **a.g.e.**, s. 247.

²²⁵ Öztürk ve diğerleri, **a.g.e.**, s. 301

²²⁶ Erem, **a.g.e.**, s. 325.

²²⁷ Bkz., Tosun, **a.g.e.**, s. 769 vd. ve Kunter, **a.g.e.**, s. 653 vd.

²²⁸ Öztürk ve diğerleri, **a.g.e.**, s. 301.

Kunter'in sınıflandırması kapsamında belirtiler (emare, iz)²²⁹ genel nitelikte temsili delillerdir ve tabii ve sun'i belirtiler olmak üzere iki gruba ayrılmaktadır²³⁰. Tabii belirtiler olayın bir parçası olan ve suçu işleyen iradesi dışında olayı tabii bir şekilde temsil eden delillerdir. Tabii belirtiler eşyaya ya da şahsa ait olabilir. Tabanca, bıçak gibi suçta kullanılan eşya, fren izi gibi suçun meydana getirdiği izler ya da sahte para gibi suçtan meydana gelen eşyalar eşyaya ilişkin tabii belirtilerin örneklerini oluşturmaktadır. Failin kan grubu, parmak izi gibi örnekler de şahsa ait tabii belirtilere aittir²³¹.

Ancak tabii belirtilerin somut olayı tespit edip etmediği iyi araştırılmalıdır. Zira bu tür deliller olaydan önce veya sonra meydana gelmiş olabilir. Bu sebeple bu tür delilleri somut olayı iyi bir şekilde temsil edip etmediği, değiştirilip değiştirilmediği iyi incelenmelidir. Bu tür incelemeler yapıp, belirtilerin sağlamlığına kanaat getirildiğinde, objektif özelliğe sahip olmaları sebebiyle diğer delillerle de desteklendiklerinde daha kuvvetli bir ispat gücüne sahip olurlar²³².

Sun'i belirtiler ise bir olayı tabii olarak değil sun'i olarak temsil eden insan yapısı işaretlerdir. Tabii belirtilerin meydana gelmesinde bir ispat amacı yoktur²³³. Tabii belirtiler failin iradesi dışında, onun iradesine rağmen meydana gelmektedir²³⁴. Sun'i belirtilerin meydana gelmesinde ise amaç zaten ispattır. Örneğin, biletlerin kullanıldığı gösterilmek için üzeri zımbalanmaktadır²³⁵.

d- Maddi delil-Bilimsel delil

Buraya kadar incelediğimiz belirti delillerine ilişkin klasik doktrinel açıklamaların yanında, teknoloji ve bilimin gelişmesi ile birlikte artık belirti delilleri maddi deliller ve bilimsel deliller kavramları ile birlikte de kullanılmaktadır.

²²⁹ Belirtiler doktrinde emare, iz ve maddi delil gibi farklı kavramlarla da adlandırılmaktadır. Bkz. Mustaf Kaygısız, **Kriminalistik Olay Yeri İnceleme: Suç Yeri ve Delil Güvenliği**, Ankara: Adalet Yayınevi, Ocak, 2010, s. 37 vd.

²³⁰ Kunter, **a.g.e.**, s. 630.

²³¹ Toroslu ve Feyzioğlu, **a.g.e.**, s. 196 vd.

²³² Aynı görüş için bkz. Toroslu/Feyzioğlu, s. 196 vd. Ayrıca bkz. Hakan Kızılarıslan, **Ceza Muhakemesi, Adli Tıp, Adli Bilimlerde Vücudun Muayenesi ve Örnek Alma, Doktrin ve Uygulama**, Ankara: Çetin Veb-Ofset A.Ş., Temmuz 2007, s. 283.

²³³ Kunter, **a.g.e.**, s. 654.

²³⁴ Kızılarıslan, **a.g.e.**, s. 283.

²³⁵ Kunter, **a.g.e.**, s. 654. Toroslu ve Feyzioğlu, **a.g.e.**, s. 197.

Özellikle çalışmamızın konusunu oluşturan dijital delillerin, delil türleri arasındaki yeri açısından bilimsel deliller büyük öneme sahiptir.

Maddi deliller, işlenen suçun yeniden canlandırılmasına, failin kimliğinin ve fail-mağdur-olay yeri arasındaki ilişkinin tespitine yarayacak, laboratuvarlarda incelendikten sonra soruşturma sırasında ya da mahkemede delil olarak kullanılabilir, maddi bir yapıya sahip, canlı ya da cansız herhangi bir nesne ya da ize denilmektedir²³⁶.

Bilimsel deliller ise belirli bir bilim dalının kural ve yöntemlerine göre elde edilen delillere denilmektedir. Örneğin DNA analizi ile elde edilen deliller bilimsel deliller olarak kabul edilmektedir. Ya da ceza muhakemesinde yer alan vücudun muayenesi ve örnek alma yöntemi ile elde edilen deliller bilimsel deliller olarak kabul edilmektedir. Bu deliller ancak ilgili oldukları olay açısından kesin delil oluştururlar ve diğer delillerle desteklenmeleri gerekmektedir. Bilimsel yöntemlerle elde edilen delillerde dahi hakimın kanaatindeki şüphe aydınlanmamışsa şüpheden sanık yararlanır ilkesinin uygulanması gerekmektedir²³⁷.

Hakim bu tür delilleri yargılama ve hüküm sırasında dikkate almak zorundadır ancak bu tür deliller her ne kadar bilimsel yöntemler kullanılarak elde edilmiş de olsalar objektif olamayabilirler. Bu sebeple bilimsel delillerin sıhhati mahkemece araştırılmalı, bu araştırma kapsamında bilimsel delillerin doğruluğu ve güvenilirliği ile mevcut olaya uygulanıp uygulanamayacağı incelenmelidir. Bu aşamaları değerlendirip bir kanaate varmak hakimın takdirindedir. Ancak objektifliği kabul edilen bir delilin de hakimi bağlaması gerekmektedir²³⁸.

ABD Federal Delil Kuralları (Federal Rules of Evidence) ve İngiltere Delil Kanunu (Evidence Act) çerçevesinde de bilimsel delillere değinilmektedir. Özellikle Anglo-Amerikan hukuk sistemine dahil olan bu ülkelerde mahkemeye sunulan bir delilin jüri önüne çıkartılabilmesi için hakimın incelemesinden geçmesi gerektiği için hangi tür bilimsel delillerin hangi şartları taşımaları halinde kabul edilebilir

²³⁶ Kaygısız, **a.g.e.**, s. 37.

²³⁷ Kızılarıslan, **a.g.e.**, s. 285.

²³⁸ **A.g.e.**, s. 285 vd.

olduğu yönünde doktrinde çeşitli tartışmalar yapılmış ve bu konuda bir takım kurallar benimsenmiştir²³⁹.

4- Dijital Deliller

a- Dijital delil kavramı

Amerika Birleşik Devletleri'nde faaliyet göstermekte olan Dijital Deliller Üzerine Bilimsel Çalışma Grubu (Scientific Working Group on Dijital Evidence) bünyesinde yapılan tanıma göre dijital deliller dijital formda depolanan ya da iletilen ispat gücüne sahip bilgiler olarak tanımlanmaktadır²⁴⁰.

Dijital deliller maddi delillerin²⁴¹ bir türüdür. Dijital deliller her ne kadar parmakizi, DNA örneği ve silah gibi diğer maddi delillere kıyasla nitelik olarak daha az somut olsalar dahi yine de maddi delil olarak kabul edilmektedirler. Bu özellikleri göz önüne alındığında; dijital deliller özel aletlerin ve tekniklerin kullanılarak toparlandığı ve analiz edildiği manyetik alanlar ve elektronik sinyallerden oluşmaktadır²⁴².

Teknolojinin gelişmesi ile dijital cihazlar günlük hayatın her alanına dahil olurken bu cihazlar aracılığıyla depolanan ya da iletilen veriler de delil olarak kabul edilerek pek çok soruşturma ve kovuşturmayla temel alınmaktadır. Amerika Birleşik Devletleri gibi pek çok ülkede mahkemeler dijital veriler gibi algılanması güç, soyut kavramların da delil olabileceğine karar vermişlerdir²⁴³.

²³⁹ Ahmad Mousa Hayajneh, Sami Hamdan AL-Rawashdeh, "Theoretical Approaches to Admitting Scientific Evidence in the Adversarial Legal System", **European Journal of Scientific Research**, Cilt 41, Sayı 2, 2010, ss. 182-193.

²⁴⁰ Mark M. Pollitt, "Digital Forensic", **Forensic Science and Law: Investigative Application in Criminal, Civil and Family Justice**, Derleyen Cyril H. Wecht, John T. Rago, Derleme Koordinatörü Benjamin E. Wecht, CRS Press, Aralık 2005, s. 495

²⁴¹ Maddi deliller deyimi yerine yabancı doktrinde "fiziksel deliller" deyiminin kullanıldığına sıkça rastlanmaktadır.

²⁴² Casey, **a.g.e.**, s. 4.

²⁴³ **A.g.e.**, s. 5.

b- Dijital delillerin özellikleri ve diğer delillerden farkları

Dijital deliller dünya üzerindeki tüm hukuk sistemlerinin henüz üzerinde çok gelişmiş sistemler ve kurallar geliştiremediği yeni bir alanı oluşturmaktadırlar. Diğer delillere kıyasla dijital deliller gözle görülemez, duyulamaz, tadılamaz ya da koklanamazlar. Ancak dijital ortama aktarılan verilerin oluşturduğu bu tür deliller özel bir takım programlar aracılığıyla anlaşılabilir. Dijital delillerin ancak özel bir takım incelemeler ve özel programlar aracılığıyla somutlaştırılması onları diğer maddi delillerden ayırmaktadır.

Dijital delillerin görüntülenmesinde birçok farklı cihaz da devreye girmektedir. Örneğin bir e-posta metni ekranda görüntülenebildiği gibi bir yazıcı vasıtasıyla da bu metnin basılmış hali edinilebilir. Ancak yazı aracılığıyla basılmış bir e-posta metni dijital belgenin kim tarafından, ne şekilde yazıldığına ilişkin sağlıklı bilgi vermeyebilir. Bu takdirde söz konusu e-posta metninin bulunduğu bilgisayar içinde incelenmesi halinde bu belgeyi destekleyen farklı verilere de ulaşılabilecektir. Bu durumu yine bir e-posta örneği üzerinden açıklayacak olursak, çıktısı alınmış bir e-postada bu metnin kimin e-posta adresinden, kime, hangi tarihte ve hangi saatte yazıldığında genellikle ulaşılabilmektedir. Ancak bu bilgilerin doğruluğu yine de sorgulanmalıdır. Zira e-postanın çıktısından bulunan bilgiler e-postanın ait olduğu zannedilen kişi dışında kişilerce de yazılmış olabilir.

Bu gibi haller de göz önüne alınarak dijital bilgilerin kullanılması sistemin bir bütün olarak incelenmesi sonucunda mümkün olmalıdır. Ancak bütün sistemin incelenmesi sonucunda dijital deliller doğrulanabilir ve sıhhatinden emin olunabilir. Dijital delillerin sistemin bütününün incelenmesi ve/veya bir kaynaktan teyit edilmesi (internet sağlayıcıları gibi) sonucunda kullanılabilir olması onları diğer delillerden ayıran bir başka özellik olmaktadır²⁴⁴.

Dijital delillerin özelliklerinden bir başkası ise aidiyetinin tespit edilmesinin oldukça güç olmasıdır. Hukuk sistemimizde yeni denebilecek kadar yakın geçmişte uygulanmaya başlanan elektronik imza yöntemi belgelerin kime ait olduğunu belirleyebilme yönünde kuvvetli bir kanaat oluşturmaktadır²⁴⁵. Ancak elektronik

²⁴⁴ Göksu, **a.g.e.**, s. 31.

²⁴⁵ Göksu, **a.g.e.**, s. 31. Hukukumuzda elektronik imza 2004 yılında çıkartılan 5070 sayılı Elektronik İmza Kanunu ile düzenlenmiştir. Elektronik imza bir kişinin biyometrik bilgilerini içeren, elektronik

imzaya olan güven ceza yargılamalarında yine de sorgulanmaktadır. Zira elektronik imzaya ilişkin şifreler çalınmış olabilir.

Dijital delilleri diğer delillerden ayıran bir diğer özellik ise diğer delillere kıyasla daha zor yok edilebilmeleridir. Diğer delillerin daha kolay yollarla imhaları mümkünken dijital deliller çok kolay yedeklenebilir yahut tamamen silinmeleri halinde üzerinde bulundukları sistemin özellikleri kullanılarak geri getirilebilir. Hatta bazı durumlarda dijital deliller sistem tarafından otomatik olarak yedeklenmiş de olabilir. Öte yandan dijital belgeler her zaman sil komutu ile silinmeyebilirler. Bu belgelerin tamamen silinmesi için ayrı yazılımların kullanılmasına ihtiyaç duyulabilir. Bu durumda dijital deliller diğer delillerden çok daha zor yok olmaktadır²⁴⁶.

Dijital deliller hassas özelliklere sahip olup, kolayca değiştirilebilir, zarar verilebilir veya bir kez doğru bir şekilde silinmeleri halinde tamamen yok edilebilirler²⁴⁷. Bu özellikleri sebebiyle söz konusu bu delillerin resmi makamlar aracılığıyla nasıl ele geçirileceği ve inceleneceği de başlı başına bir sorun olarak hukuk düzeninde kendini göstermektedir. İnceleme sırasında kullanılan yazılımlar ufak bir dikkatsizlik sonucunda dijital belge üzerinde değişime sebep olabilir. Zira birçok dijital sistem bulunmakta ve bu sistemlerle birlikte birçok dijital yazılım ve donanımlar da bulunmaktadır. Bir dijital sistem üzerinde bulunan bir dijital verinin incelemesi, başka bir dijital düzleme aktarılması veride çeşitli değişikliklere sebep olabilmektedir²⁴⁸.

Dijital deliller maddi delillere benzemektedir. Ancak dijital delilleri diğer maddi delillerden ayrıdan farklı özellikler de mevcuttur. Diğer maddi delillere

kalem ve dijital şifreleme gibi çeşitli farklı metotlarla oluşturulan bir kimlik bilgisidir. Elektronik imza retina taraması, parmakizi gibi kişiye özel tıbbi verilerle oluşturulabileceği gibi sadece ilgili kişinin bilebileceği şifreleme yollarıyla da kullanılabilir. Bir başka yöntem olarak elektronik imza kişinin bilgisayar ortamına aktardığı orjinal imzası ya da dijital bir kalem aracılığıyla doğrudan dijital bir cihaza attığı imzasının kullanılmasıyla da gerçekleşir (Bkz. Göksu, **a.g.e.**, s. 51 vd). 5070 sayılı Elektronik İmza Kanunu kapsamında getirilen tanımlara göre elektronik imza başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır. Yine aynı kanun çerçevesinde güvenli elektronik imza a) münhasıran imza sahibine bağlı olan, b) sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) Imzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan, elektronik imza olarak kabul edilmiştir. Bu kanun çerçevesinde güvenli elektronik imzanın elle atılan imza ile aynı sonuçları taşıyacağı hükme bağlanmıştır

²⁴⁶ Göksu, **a.g.e.**, s. 32.

²⁴⁷ Pollitt, **a.g.e.**, s. 495.

²⁴⁸ Göksu, **a.g.e.**, s. 33.

kıyasla (parmakizi, DNA incelemesi gibi) dijital deliller kopyalanabilir. Ayrıca orijinal veriye zarar gelmemesi için kopyalanarak incelenmesinde de fayda vardır. Kopyalanmış dijital veri tıpkı orijinali gibi incelenebilir. Doğru inceleme aletleri kullanıldığında dijital delil üzerinde oynama yapıp yapılmadığı rahatça ortaya çıkartılabilir. Tüm bunlara ek olarak yukarıda da belirttiğimiz gibi dijital delilleri yok etmek oldukça güçtür. Öyle ki, bazı durumlarda veriler kullanıcının haberi olmadan otomatik olarak yedeklenir.

Çalışmamızın bu bölümünü tamamlamadan önce dijital delillerin yok edilmesinin güçlüğüne ve yedeklenebilme özelliklerine yukarıda sıkça atıfta bulunduğumuz için bu konuyu uygulamadan bir örnekle açıklamak daha isabetli olacaktır. Amerika Birleşik Devletleri'nde görülmüş olan Amerika Birleşik Devletleri Oliver North'a karşı davasında ABD ordusunda görevli olan Albay Oliver North'un İran'a silah sattığı ve bu silahlardan elde edilen para ile Nikaragua'daki hükümete karşı ayaklanan gerillalara destek sağladığı ortaya çıkartılmıştır²⁴⁹. Bu iddia ilk önce bir Lübnan gazetesinde öne sürülmüştür. Bu dava kapsamında yapılan incelemelerde ortaya çıkartıldığı üzere Albay Oliver North birçok belgeyi yok etmeye çalışmış ve delil niteliği taşıyan e-postalarını silmiştir. Ancak IBM Profesyonel Ofis Sistemi (IBM Professional Office System- PROFS) kullanılarak gönderilen e-postalar kullanıcının haberi olmadan yedeklendikleri için dava esnasında bu verilere ulaşım sağlanabilmiştir ve davada iddia edilen deliller ortaya çıkartılmıştır²⁵⁰.

Tüm bu farklı özelliklerinden ötürü günümüzde gerek ulusal gerekse yabancı hukuk sistemlerinde yadsınamayacak kadar sıklıkla başvurulmuş ve mevcut olayları aydınlatılabilme güçlerinden ötürü delil olarak da nitelendirilebilen dijital delillerin ayrı bir inceleme konusu yapılması gerekliliği burada da kendini göstermektedir.

c- Dijital deliller kapsamında adli bilişim alanı

Dijital delillerin incelenmesi hukuk sistemini içine aldığı kadar elektronik ve bilişim gibi teknik konularda da uzmanlık gerektirdiği için daha ziyade adli bilişim

²⁴⁹ U.S. vs. Oliver North, No 89-3118. Oliver North davası 1986'da ortaya çıkan ve günümüzde İranganate, İran/Contra isimleriyle anılan bir siyasi skandal olarak kabul edilmektedir.

²⁵⁰ Casey, **a.g.e.**, s. 5.

dalı altında incelenmektedir. Adli bilişim sistemi altında ele alınan dijital verilerin geçmişini oldukça yakın zamanları işaret etmektedir. Başta bilgisayar olmak üzere birçok bilişim cihazına ulaşmanın kolay olmaya başlaması ile zamanla birlikte uzmanların aklına bu türden kişisel cihazların içerisinde şüphelenen suça ilişkin bir takım belgelerin saklanabileceği ihtimali gelmiştir. Böylece bilgisayarlar söz konusu adli vakıalar açısından önemli bir hale gelmiştir.

Adli bilişim alanı hem adli bilişim disiplinine ilişkin bilginin hem de bilgisayar ve bilim uzmanlığının bir arada bulunmasını gerektiren bir alandır. En genel tanım ile adli bilişim; bilimin hukuka uygulanması olarak kabul edilebilir²⁵¹. Bu kapsamda bir ceza soruşturması sırasında delili tanımlama, asıl haline geri döndürmeye, yeniden yapılandırmaya ve incelemeye yarayacak her türlü bilimsel ilke ve teknik adli bilişimin bir parçasını oluşturmaktadır²⁵².

Bilimsel ilkeler genel olarak delillerle ilgili şu alanlarda sıkça kullanılmaktadır:

- *Parmakizi ve DNA'nın tespit edilmesi, işleme tabi tutulması ve incelenmesi,*
- *Şüpheli bir belgenin kaynağının ve doğruluğunun ortaya çıkartılması ya da yanlış belgelerin bir suçun delili için incelenmesi,*
- *Bir bilgisayarın sabit disk sürücüsünden zarar görmüş ya da silinmiş belgelerin kurtarılması,*
- *Toplama esnasında hiçbir bilginin kaybolmadığını temin ederek bir dijital delilin birebir kopyasını yapmak,*
- *Ağlar (networks) yoluyla taşınmış bütünlüğünü ve doğruluğunu korumuş dijitalleşmiş verilerin toplanması,*
- *Dijital delilin değiştirilmediğini doğrulayan çözümleyici bir algoritma mesajı kullanılması,*
- *Dijital delili doğru olduğunu onaylamak ve delil zincirini korumak için dijital delili dijital olarak imzalamak,*
- *Bir dijital delil parçasının şahsına münhasır özelliklerini belirlemek.*²⁵³

Dijital deliller açısından adli bilişim ise potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz tekniklerinin kullanılmasıyla

²⁵¹ Casey, **a.g.e.**, s. 3.

²⁵² **A.g.e.**, s. 3.

²⁵³ **A.g.e.**, s. 3.

yapılan bir uygulama şeklinde tanımlanabilmektedir²⁵⁴. Çalışmamız kapsamında pek çok kez dile getirildiği üzere dijital deliller parmak izi veya DNA delili gibi çoğu kez il bakışta fark edilemeyen , gizli ve görünmeyen bir yapıya sahiptir. Dijital deliller hassastır ve kolayca değiştirilebilir. Bazı durumlarda zamanla sinilebilir bir özelliğe sahiptir. Bu tür farklı özellikleri sebebiyle dijital delilleri emniyet altına almak ve toplamak amacıyla yapılan hareketlerin bu delillere zarar vermemesi yüksek önem taşır. Dijital delillerle birlikte çalışmak yüksek özen ve dikkati gerektirdiği için bu alanda görevli kişilerin ayrı bir eğitime tabii tutulmaları gerekmektedir²⁵⁵. Dijital delillerin adli sürece dahil edilmeleri ise adli bilişim disiplinin temel meselelerinden birini oluşturmaktadır.

Ancak tarihsel sürece bakıldığında adli bilişim alanının ve dijital delillerin farklı özelliklerinin kabul edilmesi belli bir zamanı almıştır. Amerika Birleşik Devletleri'nde önceleri bilgisayar incelemeleri resmi kurallara bağlı olmadan *ad hoc* biçimde yapılmaya başlanmıştır. Ancak zamanla hem disiplinin müşterek kurallarının geliştirilmesine olan ihtiyacın artması hem de bu alanda yetiştirilecek eleman açığının meydana gelmesi nedeniyle dijital verilerin adli sebeplerle incelenmesine yönelik çeşitli oluşumlar baş göstermeye başlamıştır. Amerika Birleşik Devletleri'nde lokal düzeyde kurulan birkaç merkezin ardından 1991 yılında Uluslararası Bilgisayar İnceleme Uzmanları Kuruluşu (International Association of Computer Investigative Specialist- IACIS)²⁵⁶ açılmıştır. IACIS bu alanda faaliyet göstermeye başlayan dünyanın ilk kuruluşu olarak kabul edilmektedir.

Amerika Birleşik Devletleri'nde kurulan IACIS kurumundan önce 1990'ların sonuna kadar adli bilişim alanı ve bu alan kapsamında dijital delillerin incelenmesine yönelik organize bir düzenleme bulunmadığı için bu alanda faaliyet gösteren kişiler için de dijital delilleri incelemeye olanak sağlayacak olan çeşitli programlara ulaşmak büyük bir sorun olmaktaydı. Dijital delillerin incelenmesine yarayacak çeşitli programların bilgisayar programcıları tarafından oluşturulması ve bu alanda uzman kişilerin yetiştirilmesi ancak 2000'li yılları bulmuştur. Zira 2000'li

²⁵⁴ Leyla Keser Berber, Erdem Akyazılı, "Adli Bilişim", **Bilişim Teknolojisi Hukuku Gündemi 2004-2005**, İstanbul: Bilişim Teknolojisi Uygulama ve Araştırma Merkezi, Ocak 2006, s. 29

²⁵⁵ **A.g.e.**, s. 30.

²⁵⁶ IACIS adli bilişim alanında yetkili kişileri yetiştirmek ve bu kişilerin eğitimlerine sertifika vermek amacıyla kurulmuştur. Bu kuruluşun kuruluş amacı ve faaliyetleri hakkında detaylı bilgi için bkz. **IACIS**, <https://www.iacis.com/>, (Erişim 21.08.2012)

yıllara gelmeden önce bu alan bir bilgisayar programı geliştirmek için yeterli büyüklükte bir pazar olarak görülmemiştir. Yapılacak yatırımların beklenen geliri getirmeyeceği yönündeki kanaat 2000’li yıllarda piyasaya sürülen Expert Witness, Encase ve Forensic Tool Kit isimli çeşitli programlarla beraber yok olmaya başlamıştır²⁵⁷.

Dijital delillerin şahsına münhasır özellikleri ve bu özellikler sebebiyle diğer delillerden ayrı inceleme metotlarına tabi olmaları yönünde ortaya çıkan ihtiyaç sonucunda Amerika Birleşik Devletleri dışında İngiltere ve Avrupa Birliği’nde de çeşitli düzenlemelere gidilmiştir. Özellikle bu alanda faaliyet gösteren uzman kişi sayısının da artması ile birlikte adli bilişim (*computer forensic- digital forensic*) alanına yönelik bir takım standartların belirlenmesi de gerekmiştir. Bu standartların sadece bir uzmanın dijital delil üzerinde yaptığı incelemeyi bir diğerinin anlamasını sağlamanın yanı sıra aynı zamanda bir uzmanın mahkeme önünde tartışılacak ve bir ceza muhakemesine ışık tutacak olan dijital delil üzerinde nereye kadar bir inceleme yapabileceğini de belirleyecek nitelikte olması gerektiği yönünde bir kanaat oluşmuştur.

Bu ihtiyaç kapsamında İngiltere’deki Emniyet Amirleri Derneği (The Association of Chief Police Officers- ACPO) Bilgisayar Tabanlı Elektronik Deliller için En İyi Uygulama Rehberi (Good Practice Guide for Computer-Based Electronic Evidence) belgesini yayınlamıştır²⁵⁸. Ayrıca İngiltere 2012 yılının Mart ayında son olarak Dijital Deliller için en İyi Uygulama Rehberi belgesini de yayınlamıştır (ACPO Good Practice Guide for Digital Evidence)²⁵⁹. Bu belgede dijital delillerin ele geçirilmesinden değerlendirilmesine kadar geçen süreç içerisinde araştırmayı yapmakla görevlendirilmiş kişilerin riayet etmesi gereken kurallara ve bu delillerin özelliklerine yer verilmiştir. Öte yandan dijital delillerin ceza uyuşmazlıklarına ışık tutması ve aynı zamanda dijital yollarla işlenen suçları birçok ülkenin güvenliğini tehdit eden bir yapıya sahip olması sebebiyle G-8 Yüksek Teknolojili Suç Altkomitesi Bilgisayar Delilleri için Uluslararası Organizasyon’a (International Organization for Computer Evidence-IOCE) bu alanda uluslararası kuralların

²⁵⁷ Pollitt, **a.g.e.**, s. 497.

²⁵⁸ Association of Chief Police Officers, **Good Practice Guide for Computer-Based Electronic Evidence**, <http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf>, (Erişim tarihi Mart 2013).

²⁵⁹ Association of Chief Police Officers, **Good Practice Guide for Digital Evidence**, <http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf>, (Erişim tarihi Mart 2013).

benimsenmesi gerektiğini belirtmiş ve bu anlamda kuruluşu faaliyete davet etmiştir. IOCE, Avrupa Adli Bilimler Enstitüsü Ağı (European Network of Forensic Science Institutes- ENFSI), Dijital Delil üzerine Bilimsel Çalışma Grubu (The Scientific Working Group on Digital Evidence- SWGDE) ve topluluğun diğer çalışma grupları ile birlikte çalışarak bir takım ilkeler ve tanımlar benimsemiştir²⁶⁰.

Çalışmamızın bu bölümünde dile getirilen dijital delillerin adli bilişim disiplini çerçevesinde incelenen özellikleri ve bu özellikleri sebebiyle benimsenen ilkelere çalışmamızın son bölümü olan dijital delillerin doğrulanması başlıklı kısmında tekrar ve daha ayrıntılı bir biçimde değinilecektir. Zira bu alanda benimsenen çeşitli ilkeler çerçevesinde dijital deliller doğrulanmakta ve ceza muhakemesi kapsamında kabul edilerek kullanılabilmektedir.

d- Dijital delillerin delil türleri arasındaki yeri

Dijital deliller mahiyetleri gereği maddi delil olarak kabul edilmelidirler. Maddi deliller ve bilimsel deliller çeşitli yazarlarca belirtiler olarak incelenmişlerdir²⁶¹. Ancak dijital deliller, doğrulukları tespit edildiğinde, maddi delillerden, belirtilerden daha çok ispat gücüne sahiptir. Üstelik ileride değineceğimiz üzere dijital deliller üzerindeki incelemeler bir rapor halinde sunulmaktadır. Bu kapsamda dijital delilleri veri tespit eden belge niteliğinde belge delili olarak kabul etmek kanaatimizce dijital delillerin niteliğine uygun olacaktır. Böylece doktrinde belirtilen CMK 214 kapsamında delillerin okunması yönündeki gereklilik de yerinde getirilebilecektir²⁶². Öte yandan dijital delillerin belirti olarak kabul edilmesi görüşü kapsamında belirtmek gerekir ki belirtilerin sıhhati iyice araştırıldıktan sonra belirtiler de diğer deliller gibi değerlendirilebilmektedir²⁶³.

Yukarıda dijital delillerin özelliklerinde de değindiğimiz gibi dijital delillerin delil olarak değerlendirilmesi için içlerinde bulundukları dijital sistemin hepsinin incelenmesi gerekmektedir ve dijital delillerin değiştirilmesinin görece kolay olması

²⁶⁰ A.g.e., s. 496 vd.

²⁶¹ Centel ve Zafer, a.g.e., s. 201 vd.

²⁶² A.g.e., s. 244-245.

²⁶³ Aynı görüş için bkz. Toroslu ve Feyzioğlu, a.g.e., s. 196 vd; Kunter, a.g.e., s. 654 vd.

sebebiyle mutlaka uzmanlar tarafından doğrulanması gerekmektedir. Dijital delillerin adli bilişim prosedürüne aykırı olarak incelenmesi ve bu belgelerin doğrulanamaması halinde yine de hükme esas kılınması kanaatimizce açıkça isabetsiz olacaktır.

C- Türk Ceza Muhakemesinde Hukuka Aykırı Deliller

Çalışmamızın yukarıdaki bölümlerinde de belirttiğimiz üzere ceza muhakemesinin temel amacı maddi gerçekliğe ulaşabilmektir. Ancak ceza muhakemesinin bu amacı mutlak ve ne pahasına olursa olsun ulaşılması gereken bir amaç değildir. Ceza muhakemesinin temelini oluşturan maddi gerçeği ulaşma amacının sınırını delil yasakları, hukuka aykırı deliller çizer.

Ceza muhakemesi kapsamında hukuka aykırı deliller oldukça karmaşık bir konu olup söz konusu çalışmamız açısından da büyük bir öneme sahiptir. Zira dijital delillerin kendilerine özgü yapılarından kaynaklanan sorunlar bu konuda hukuka aykırı delillerle karşılaşma ihtimalini arttırmaktadır.

Çalışmamız kapsamında öncelikle hukuka aykırı delillere ilişkin genel bilgilere yer verilecek daha sonra hukuka aykırı delillerin nasıl değerlendirildiği meselesi incelenecek ve son olarak da Avrupa İnsan Hakları Sözleşmesi'nin bu konu hakkındaki tutumuna yer verilecektir.

1- Kavram ve Genel İlkeler

Hukuka aykırılık kavramı geniş bir kavramdır. Hukuk hakları anlamına gelir ve hukuk sadece kanunlarla güvence altına alınmış haklardan ibaret değildir²⁶⁴. Hukuka aykırı deliller sadece ulusal düzenlemelere aykırı olarak elde edilmiş deliller değil aynı zamanda uluslararası düzenlemelere aykırı olarak elde edilen delilleri de

²⁶⁴ Muharrem Özen, Mustafa Özen, “Ceza Muhakemesi Hukukunda Delil Yasakları”, **Prof. Duygun Yarsuvat’a Armağan, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, İstanbul: Pasifik Ofset, Cilt 9, Sayı 2, 2012, s. 301-329, s. 305.

kapsamaktadır²⁶⁵. Öte yandan hukuka aykırı deliller ulusal kanunlarda açıkça yasak olarak belirtilmiş kuralları ihlal ederek elde edilebileceği gibi kanunda yasaklama olmasa dahi ilgili kurallara aykırı biçimde de elde edilebilir²⁶⁶.

Delil yasakları; aydınlatma yükümlülüğünün yerine getirilmemesi (örneğin; kovuşturma makamlarının sanığa haklarını açıklamaması), yasak ifade ve sorgu yöntemlerinin kullanılması, ifade ve sorgu dışında söz konusu olabilecek delil yasaklarına başvurulması (örneğin; hukuka aykırı olarak yapılan vücut muayenesi), ve delil aracı yasakları (örneğin; tanıklıktan veya yeminden çekinme hakkı bulunanların hukuka aykırı bir şekilde tanık olarak dinlenmesi) olarak tasnif edilebilir²⁶⁷.

Bu kapsamda doktrinde tartışılmış olan delil yasakları ve hukuka aykırı deliller terimleri arasındaki farka değinmek gerekmektedir. Ünver ve Hakeri'nin de altını çizdiği üzere hukuka aykırı deliller ve yasak deliller aynı anlamda kullanılmamalıdır²⁶⁸. Zira delil ve ispat yasakları çok geniş bir alanı kapsayıp hukuka aykırı deliller bu alanın yalnızca bir parçasıdır²⁶⁹. Bu görüşe göre delil yasakları, hem hukuka aykırılık nedeniyle hem de başka nedenlerle elde ediliş değerlendiriliş veya başka alanda değerlendirilmesi/ kullanılması yasaklanmış delilleri ifade etmektedir²⁷⁰.

Öte yandan, Anayasa'da ve CMK'da delil yasaklarına ilişkin ifadelerde kullanılan terimler birbirini tutmamaktadır. 4709 sayılı Kanunun 15.maddesi ile Anayasa'nın 38. maddesinin 6. fıkrasına bir hüküm eklenmiştir ve bu haliyle Anayasa "*Kanuna aykırı elde edilmiş bulgular, delil olarak kabul edilmez*" ifadesini benimsemiştir. 5271 sayılı CMK'nun 217. maddesinin 2. fıkrası ise "*Yüklenen suç, hukuka uygun şekilde elde edilmiş her türlü delille ispat olunabilir*" ifadesini içermektedir.

²⁶⁵ Güçlü Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", **Türkiye Barolar Birliği Dergisi**, Ankara: Şen Matbaa, Temmuz-Ağustos 2012, Sayı 101, ss. 61-83, s. 63 vd.

²⁶⁶ A.g.e., s. 63.

²⁶⁷ Bahri Öztürk, "Ses ve/veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukundaki Yeri", **Prof. Dr. Seydullah Edis'e Armağan**, İzmir: Dokuz Eylül Üniversitesi, 2000, s. 219-233, s. 221 vd.

²⁶⁸ Ünver ve Hakeri (2. Cilt), a.g.e., s. 165.

²⁶⁹ A.g.e., s. 165.

²⁷⁰ A.g.e., s. 165.

Anayasa ve CMK’da kullanılan farkı ifadelerin sonuçları da farklı olmaktadır. Kanuna aykırılıktan bahsedildiği zaman var olan kanunlarda kullanılan ifadelere aykırı yapılan eylemler sonucu delil yasakları ile karşılaşılacaktır. Ancak hukuka uygunluktan bahsedildiği zaman evrensel hukuk kurallarına uygunluktan genel olarak insan haklarına uygunluktan bahsedilmektedir. Nitekim kanunların varlığı bir yerde her zaman ideal anlamda bir hukukun varlığına işaret etmez. Tarih bunun örneklerini pek çok defa görmüştür. Hala hatırlardan silinmeyen Nazi döneminde Almanya’da yaşanan pek çok şey için uygun kanunlar vardı ancak yaşananlar olması gereken hukuka uygun değildi. Bu temel felsefeden yola çıkılarak doktrinde Anayasanın ilgili hükmünün lafzi anlamda değil pozitif hukuk anlamında algılanması da savunulmuştur²⁷¹. Öte yandan bazı yazarlar tarafından lafzi anlamda kanuna aykırılıkların hepsinin delil yasakları kapsamında değerlendirilmesi eleştirilirken burada yasaklanan şey kapsamında korunan menfaat ile ihlal edilmesi halinde sonuç olarak ortaya çıkacak durum arasında bir menfaat dengesi yapılıp ona göre tercih yapılması gerektiği belirtilmiştir²⁷².

2- Hukuka Aykırı Delillerin Değerlendirilmesi

Hukuka aykırı delillere yönelik kavram tartışmalarından ziyade bu tarz delillerin nasıl değerlendirilecekleri tartışma konusudur. Bu noktada doktrinde farklı yaklaşımlar benimsenmiştir. Kesin kabul görüşüne göre eğer elde edilen delil söz konusu olayı açıklamaya faydalı ise nasıl elde edildiğine bakılmaksızın kabul edilir²⁷³. İkinci olarak kesin ret yaklaşımı kapsamında hukuka aykırı olan deliller kesinlikle hükme esas alınamaz²⁷⁴. Son olarak ise esnek yaklaşım kapsamında hukuka aykırı elde edilen deliller bazı durumlarda kullanılacak bazı durumlarda ise kullanılmayacaktır²⁷⁵.

Doktrinde her üç yaklaşımın da temsilcileri bulunmaktadır. Ancak dünyadaki hukuk sistemlerinde de söz konusu bu üç yaklaşım farklı ülkeler tarafından kabul edilmektedir. Türkiye ve İtalya kanuna aykırı elde edilen delillerin kesinlikle

²⁷¹ A.g.e., s. 303

²⁷² Öztürk ve diğerleri, a.g.e., s. 374-375.

²⁷³ Özen ve Özen, a.g.e., s. 304

²⁷⁴ A.g.e., s. 304

²⁷⁵ A.g.e., s. 304

geçersiz olduğunu kabul eden hukuk sistemleri arasındadır²⁷⁶. Anayasa’da dahi teminat altına alınan bu duruma ilişkin Yargıtay kararlarının da aynı isabette olmasını temenni eden Yarsuvat, doktrinde hukuka aykırılık ve kanuna aykırılık terimleri hakkındaki tartışmaları da ‘garip’ olarak nitelendirmektedir. Zira Yarsuvat hakların kanunlarla düzenlendiğini belirterek kanuna aykırılık teriminin konuyu berraklaştırdığını ileri sürmektedir²⁷⁷.

Bu görüş çerçevesinde Kiziroğlu, ayrıca bir temyiz nedeni olarak öngörülen hukuka aykırılık hakkında şu açıklamada bulunmaktadır: “...kanımızca hukuk düzeni, hukukun üstünlüğü korunmaktadır. Dolayısıyla delil olabilecek bir şey elde edilirken hukuka aykırılıkta bulunulmuş ise, artık hüküm üzerinde etkisinin olup olmadığının araştırmasına gitmeksizin, hüküm mutlak surette bozulmalıdır.”²⁷⁸

Nevzat Toroslu ise hukuka aykırı delillerin kesin olarak neden reddedilmeleri gerektiğini son derece sarıh bir dille ifade etmiştir. Toroslu’nun ifadeleri hukuka aykırı delillere ilişkin herhangi bir açık kapı bırakmayan bu görüşün felsefesini masaya yatırmaktadır. Toroslu’ya göre:

“Hukuka aykırı veya yasak deliller konusunda sorulması gereken ilk soru, nasıl bir Ceza Muhakemesi istediğimiz sorusudur. Ne pahasına olursa olsun bütün suçluları cezalandırmayı amaçlayan bir ceza muhakemesi mi, yoksa hukuki yollarla elde edilen delillerle suçlu bulunanları cezalandırmayı amaçlayan bir ceza muhakemesi mi istiyoruz? Bir başka deyişle de, eski mutlakiyetçi rejimlere özgü olan ve günümüzde de daha az mutlakiyetçi olmayan baskıcı rejimlerde benimsenen ve sanığı peşinen suçlu kabul eden, ceza muhakemesinin amacını sadece mahkumiyeti haklı gösterecek delilleri elde etmek olarak anlayan, bunun için de, işkence de dahil, her yolu meşru gören baskıcı bir ceza muhakemesi mi, yoksa özgürlükçü toplumlarda benimsenen ve suçlulukla mücadele konusunda çatışır gibi gözüken toplumsal menfaat ile bireysel menfaat arasında bir paralellik bulunduğunu kabul eden, böylece suçluların ortaya çıkarılmasını da

²⁷⁶ Duygun Yarsuvat, **Ceza Muhakemesi Hukukunda Kanuna Aykırı Elde Edilen Delillerin Geçerliliği**, <http://www.yarsuvat-law.com.tr/articles/article2.pdf>, Haziran 2009, s. 4-5

²⁷⁷ YARSUVAT s. 7

²⁷⁸ Serap Keskin Kiziroğlu, **Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık**, İstanbul: Alfa Basım Yayım Dağıtım, 1997, s. 176.

amaçlayan bir ceza muhakemesi mi istiyoruz?”²⁷⁹

Hukuka aykırı delilleri esnetilmiş olarak değerlendiren görüşlere değinmeden önce hukuka aykırı delilleri tamamen kabul eden sistemlere değinmekte fayda vardır. Doktrinde dile getirilen bir konu olmamakla birlikte otoriter rejimler, insan haklarından ve adil yargılanmadan ziyade suçlunun en ağır şekilde cezalandırılmasını ön planda tutan rejimler kapsamında hangi yolla elde edildiği önemsenmeksizin her türlü delil muhakeme kapsamında değerlendirilmektedir.

Doktrinde tartışılan bir diğer görüş ise esnek yaklaşım görüşüdür. Bu görüşün temelinde hukuka aykırılık anlayışını yorumlamak yatmaktadır. Esasen hukuka aykırı deliller insan haklarına aykırı sonuçlar ortaya çıkardıkları için yasaklanırlar. Hukuka aykırılık, haklara aykırılıktır ancak somut olay açısından herhangi bir hak kaybı yoksa hukuka aykırılıktan söz edilemez. Bu ifadesi ile esnek yaklaşım görüşü hukuka aykırılık ve kanuna aykırılık kavramlarını kesin olarak birbirinden ayırmaktadır²⁸⁰.

Hukuka aykırılığın ölçüsünün temel alındığı bu görüşte hak ihlalinin niteliği önem taşımaktadır²⁸¹. Haklar mutlak ve nisbi olarak ayrılmakta ve delil yasakları bu ayrıma göre şekillenmektedir. Nisbi haklar kamu yararı kapsamında hakkın niteliksel üstünlüğü ve sayısal üstünlüğü ölçütlerine göre değerlendirilir. Nisbi hukuka aykırılıkta hakkın topluma verdiği zarar ile delillerin toplanması için uygulanan yöntemlerin topluma verdiği zarar arasında bir değerlendirme yapılacaktır²⁸².

Bu görüş kapsamında delilin kanuna aykırı bir yöntemle elde edilmiş olduğu belirlenirse, bu delili hüküm verirken kullanıp kullanmamak mahkemenin takdirindedir²⁸³. Zira verilecek karar sanığın adil yargılanma hakkını ihlal etmiyorsa kanuna aykırı olan delil hükümde kullanılabilir, ancak kanunda delilin kullanılmasını tamamen yasaklayan bir norm varsa bu norma riayet edilmelidir²⁸⁴. Hukuka aykırı delillerin merkezine oturtulan adil yargılanma hakkı ve sanığın ihlal edilen hakları incelenecektir. Devlet yargıladığı sanığa temel bütün haklarını sağlamakla mükellef olduğu için, Kunter, Yenisey ve Nuhoğlu'na göre i) dürüst yargılanma hakkı

²⁷⁹ Nevzat Toroslu, “Hukuka Aykırı Deliller Sorunu”, **Prof. Dr. Hamide Topçuoğlu’na Armağan**, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayın No: 498, 1995, ss. 55-58, s. 55.

²⁸⁰ Öztürk ve diğerleri, **a.g.e.**, s. 370-374.

²⁸¹ Özen ve Özen, **a.g.e.**, s. 305.

²⁸² **A.g.e.**, s. 305.

²⁸³ Kunter, Yenisey ve Nuhoğlu, **a.g.e.**, s. 1422.

²⁸⁴ **A.g.e.**, s. 1422.

kapsamına giren temel sanık hakları sağlanmadan elde edilen veya ii) yetki sınırı aşarak veya iii) kanunun önceden elde edilmesini yasaklamış olduğu halde elde edilen deliller “kanuna aykırı yöntemle elde edilen delil” olarak kabul edilir²⁸⁵.

Hukuka aykırı delillerin yasaklanması ile temelde korunmaya çalışılan menfaatin ne olduğunu belirlemeyi amaçlayan ve böyle bir menfaat dengesi öngören bu görüşte, sıkça Amerikan Mahkemesi kararlarına atıflar da yapılmaktadır. Amerikan hukukunda 1914 yılında *Weeks v. United States* kararında hukuka aykırı deliller (*exclusionary rule*) teorisi geliştirilmiştir. Anglo-Amerikan hukukunda polisin ceza muhakemesinde etkin rol almasıyla bağlantılı olarak, hukuka aykırı delillerin değerlendirme dışında bırakılmasının sebebi bireyleri polisin yırtıcı davranışlarına karşı korumak olarak tanımlanmaktadır²⁸⁶. Amerikan Hukukunda bu teori çeşitli yargı kararları ile gelişmiştir ve Anayasa tarafından garanti altına alınan sanık haklarına aykırılıklar halinde delillerin değerlendirilmeyeceği anlayışı oluşmuştur. Ancak Amerikan Yüksek Mahkemesi çeşitli kararlarında bu teorinin mutlak olmadığını ve her bir olayı kendi bünyesinde değerlendirerek ihlal edilen sanık hakkının niteliği belirlenmeye çalışılmıştır. Amerikan hukukunda delillere ilişkin bilinen kararlardan biri olan *Duncan v. Louisiana* (1968) kararında yine çeşitli içtihatlarla belirlenen sanığın temel haklarından sayılan hakların ihlal edilmesi halinde kanuna aykırı yöntemle elde edilen deliller söz konusu olur ve bunların hüküm verilirken kullanılıp kullanılmaması konusunda mahkeme takdir yetkisine sahiptir²⁸⁷.

Önceden belirlenmiş kurallardansa her bir örneği kendi içerisinde değerlendiren Amerikan hukukunda ve genel olarak Anglo-Amerikan hukuk sisteminde hukuka aykırı delillerle ilgili “zehirli ağacın meyvesi” teorisi geliştirilmiştir. bu kapsamda bir delilin hukuka aykırılığı tespit edildiğinde ve bu delilin kullanılmamasına karar verildiğinde bu delilden etkilenecek ortaya çıkartılan diğer delillerin de hukuka aykırı sayılacağı kararlaştırılmıştır (hukuka aykırı delillerin uzak etkisi). Bu teori Silverthorne *Lumber Co., Inc. v. United States* (1920) kararı ile doktrinde yerini almıştır.

Hukuka aykırı delillerin değerlendirilmesi hususunda örnek alınan bir diğer

²⁸⁵ A.g.e., s. 1424.

²⁸⁶ Guido Calabresi, “The Exclusionary Rule”, *Harvard Journal of Law and Policy*, Cilt 26, Sayı 1, 2003, ss. 111-118, s. 111.

²⁸⁷ Kunter, Yenisey ve Nuhoğlu, a.g.e., s. 1424

sistem de Alman hukukudur. Hakların nisbi ve mutlak olarak ayrılması hususunda Alman hukuku doktrinine sıkça atıfta bulunulmaktadır²⁸⁸. Ancak Alman hukukunda delil elde etme ve değerlendirme yasağına ilişkin genel bir hüküm bulunmadığı için her somut olayda uygulanabilecek bir asli ölçütten kaçınılmaktadır²⁸⁹. Alman hukukunda somut olayın koşulları, karşı karşıya gelen hukuksal değerler, delilin ispat yönü ve ilişkin olduğu husus gibi konularda her somut olay ayrı ayrı değerlendirilir ve hukuka aykırılık inkar edilmese de bu nitelikteki bir delilin bazen delil değerlendirme yasağı alanı dışına çıkarılarak o vakıda uygulanmasına göz yumulmakta veya bu durum özellikle istenmektedir²⁹⁰.

Yargıtay kararları kapsamında hukuka aykırı delillerin nasıl ele alındığını tartışmadan önce esnetilmiş görüşe ilişkin bazı hususları belirtmek isabetli olacaktır. Esnetilmiş görüşün temelinde hukuka aykırılık teorisinin son derece katı uygulanması sebebiyle ortaya çıkabilecek hukuki çıkmazları azaltmak vardır. Ancak hukuka uygunluk ve hukuka aykırılık arasında her zaman son derece keskin ayrımlar bulunmaz ve böyle muğlak durumlarda hukuka aykırılığı yok saymak hukuki süreçlerdeki tıkanmaları ortadan kaldırsa da zamanla derin problemlere sebep olabilmektedir. Bu görüş kapsamında hangi ölçütle hukuka aykırılığın mutlak ya da nisbi kabul edileceği yeterli ölçüde açıklanmamaktadır; yalnızca bazı hukuka aykırılıkların sonuca etkisi olmadığı önceden kabul edilmektedir²⁹¹.

Bu duruma ilişkin eleştirilerimiz şu şekilde somutlaştırılabilir. Öğretide herhangi bir hakkın ihlal edilmediği her türlü basit şekli aykırılıkların da mutlak bozma sebebi sayılması eleştirilmiş, gündüz yapılması gereken aramanın gece yapılması halinde ve bundan başka hiçbir hukuka aykırılık yoksa, burada hangi hakkın ihlal edildiği örneklenerek tartışılmıştır²⁹². Nihayetinde bir soruşturma kapsamında aramaya başvurulacaksa söz konusu yer o soruşturma kapsamında aranacaktır. Ancak arama ve elkoyma bir koruma tedbiri olarak CMK'da ayrıntılı olarak düzenlenmiştir. Bu düzenlemelerin ve usule ilişkin kuralların mevcudiyetinin bizatihi sebebi zaten sanık haklarını korumaktır. Bu tarz usuller olmadan dünyanın birçok ülkesinde aramalar gerçekleştirilmektedir ve elde edilmek istenen deliller elde edilmektedir ancak hukuk devletlerinde insan haklarına riayet etmek amacıyla bir

²⁸⁸ Öztürk ve diğerleri, **a.g.e.**, s. 370-374.

²⁸⁹ Ünver ve Hakeri (2. Cilt), **a.g.e.**, s. 183.

²⁹⁰ **A.g.e.**, s. 183.

²⁹¹ **A.g.e.**, s. 183.

²⁹² Öztürk ve diğerleri, **a.g.e.**, s. 374.

takım usuller getirilmiş ve sanık hakları ile devlet görevlilerinin yetkileri arasında bir denge kurulmaya çalışılmıştır. CMK'nın 118. maddesi açıkça konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılmaz demektir. Bu kuralın amacı kolluk görevlilerine gece vakti iş çıkartmamak değil, gece vakti şüpheli veya sanığı böyle bir travmayla karşı karşıya bırakmamak ona da kendi haklarını arayabileceği, başına gelenleri algılayabileceği bir alan yaratabilmektir. Bu örnek üzerinden düşüncelerimizi somutlaştıracak olursak gece yapılmaması gereken bir arama gece yapıldığı için hukuka aykırıdır çünkü o kişi o anda müdafisine ulaşamamış olabilir, o anda gece vakti ne yaşadığını dahi algılayamamış olabilir, ailesi oluşan bu durumdan zarar görebilir ve bunu sadece “basit şekli” bir sebepten hukuka uygun kabul etmek hukuki süreçlerdeki tıkanıklıkları gidermek ve suç ve suçluyla mücadele etmek adına hukuk eliyle topluma zarar verilmesine sebep olabilir.

Kanaatimizce doktrinde tartışılan karşılaştırmalı hukuk teorileri Türk Ceza Muhakemesi kapsamında hukuka aykırı deliller sorununu çözememektedir. Zira Türk Ceza Muhakemesi kapsamında temel alınan kanunların ve Anayasanın lafzı buna izin vermemektedir. CMK çerçevesinde hukuka uygunluktan bahsedilmiş, bir üst norm olan Anayasa kapsamında ise kanuna uygunluktan bahsedilmiştir. Bu sebeple kanunların kullandıkları dil itibarıyla kanunlarda belirtilen usullere aykırılıklar ve haklar teorisi çerçevesinde hukuka aykırılıklar sonucu elde edilen bulgular delil olarak değerlendirilemez. Aksine yapılacak bir yorum ceza muhakemesi kapsamında genişletici yorum olur ve söz konusu bu duruma ilişkin kanunlarda bir boşluk olmadığı gibi aynı zamanda da insan haklarına ilişkin sınırlayıcı hükümlerde genişletici yorum kabul edilemez.

3- Yargıtay Kararları Kapsamında Hukuka Aykırı Deliller

Yargıtay kararları kapsamında hukuka aykırı deliller farklı şekillerde yorumlanmıştır. Yargıtay daha önceki tarihli kararlarında hukuka aykırı delillerin hükme esas teşkil edemeyeceği ve mutlak suretle değerlendirme dışında bırakılacağı istikrarlı olarak görülmektedir. Yargıtay gerek CMUK (madde 254/2) gerekse CMK

(madde 217/2) kapsamında hukuka aykırı olarak elde edilen delillerin hükme esas alınamayacağı yönünde kararlar vermiştir²⁹³.

Yargıtay'ın yerleşik bu görüşü "hint keneviri" kararı olarak anılan 29.11.2005 gün ve E. 2005/7-144, K. 2005/150 sayılı Ceza Genel Kurulu kararında açıkça tüm hususlarıyla şu şekilde belirtilmiştir.

"Ceza yargılaması hukukumuzda delillerle ilgili geçerli ilke, "delil serbestisi" prensibidir. Bu nedenle, ceza yargılaması hukukunda, medeni yargılama hukukundan farklı olarak, her şey delil olarak kabul edilebilir. Öte yandan, 1412 sayılı Ceza Muhakemeleri Usulü Kanununun 254. maddesinin birinci fıkrasında; "Mahkeme irat ve ikame edilen delilleri, duruşmadan ve tahkikattan edineceği kanaate göre takdir eder." denilmekle, yargılama sürecinde sunulan ve toplanan kanıtlardan çıkarım yapılması yargıçların takdirine bırakılmıştır. Ancak hem "delil serbestisi" hem de "delillerin yargıçların kanaatine göre takdir edilmesi" ilkelerinin belli sınırları bulunmaktadır. Bunlardan biri de, mahkemenin, ancak hukukun izin verdiği yöntemlerle elde edilen delilleri dikkate alabilecek olmasıdır. Başka bir deyişle, hukuk düzeninin yasakladığı yöntemlerle toplanan deliller mahkemece dikkate alınamazlar. Temel hak ve hürriyetlere yasadışı müdahale suretiyle elde edilen delillerin davalarda hükme esas alınmasının hukuka aykırı sayılması ise, çağdaş hukuk sistemlerinin bazılarında içtihadi ilkeler, kimilerinde de pozitif hukuk normları sayesinde mümkün olabilmektedir.

Hemen belirtmek gerekir ki, 1412 sayılı Ceza Muhakemeleri Usulü Kanunu ile getirilen yargılama sisteminde eskiden bu yana pozitif hukuk normu olarak bazı delil yasakları da mevcuttur. Tanıklıktan ve yeminden çekinme hakkını kullanmış bulunanların önceden verdikleri ifadelerin duruşmada okunamayacağı (CMUK md. 47 vd., 245), dolayısıyla bu açıklamaların yapılmamış varsayılması gerektiği ve kararda bunlara dayanılamayacağı yolundaki ilke bunlardan biridir. Yine bu sistemde, sanığın iyi haline ilişkin belgelerin duruşmada okunması kabul edilmemiştir. (CMUK md. 249/1) Ancak bu münferit hükümlere karşın,

²⁹³ Yargıtay 8. CD E. 2008/334, K. 2009/15739, T. 14.12.2009, www.kazanci.com, (Erişim 22 Mart 2013)

1992 yılına kadar delil yasakları konusu anılan Yasada genel bir ilke biçiminde düzenlenmemiştir. Konuyu düzenleyen açık bir pozitif hukuk normu mevcut olmadığından, bu tarihten önceki süreçte mahkemeler, içtihadi ilkeler geliştirmişlerdir. Örneğin; Askeri Yargıtay 2. Dairesi 26.04.1973 tarihli bir kararında ".....kanuna, ahlaka ve genel adaba aykırı surette toplanan delilleri, hakim, telakki etmekten kaçınmak zorundadır" görüşüne yer vermiştir.

Ancak, 1412 sayılı Ceza Muhakemeleri Usulü Kanununda 18.11.1992 gün ve 3842 sayılı Yasa ile değişiklik yapılarak Yasaya iki önemli hüküm eklenmiştir. Bunlardan ilki, Yasanın 135/a maddesidir. Yasanın 135. maddesinde ifade alma ve sorguya çekmenin yöntemi düzenlenmiş olup, 135/a maddesinde ise, ifade ve açıklamaların özgür iradeye dayanması gerektiği belirtildikten sonra, bunu engelleyici nitelikte kötü davranma, işkence, zorla ilaç verme, yorma, aldatma, bedensel cebir ve şiddette bulunma, bazı araçlar uygulama gibi iradeyi bozan bedeni veya ruhi müdahalelerin yapılamayacağı, yasaya aykırı menfaat vaat edilemeyeceği belirtilerek, bu ve benzeri uygulamalar yasak sorgu yöntemleri olarak sayılmış, ayrıca "bu yasak yöntemlerle elde edilen ifadelerin rıza olsa dahi delil olarak değerlendirilemeyeceği" hükme bağlanmıştır. Konumuzu ilgilendiren asıl değişiklik ise CMUK.nun [254.](#) maddesine eklenen ikinci fıkradaki; "soruşturma ve kovuşturma organlarının hukuka aykırı şekilde elde ettikleri deliller hükme esas alınmaz" emredici kuralıdır. Delil yasakları ile ilgili genel ve kapsayıcı nitelikteki bu prensip uyarınca, hükme esas alınması mümkün bulunmayan deliller, "hukuka aykırı biçimde elde edilen deliller"dir. Nitekim, Ceza Genel Kurulunun 8.4.2003 gün ve 30-98 sayılı kararında; suç örgütü ile ilgili soruşturmada telefon konuşmalarının hakim kararı olmaksızın dinlendiği ve kayda alındığına işaret edilmek suretiyle, "....1412 sayılı CMUK.nun [254.](#) maddesinin açık hükmü uyarınca, hukuka uygun olarak elde edildiği saptanamayan bu ses kayıtlarının kanıt olarak hükme esas alınamayacağı" belirtilmiştir.

Öte yandan, Yerel Mahkeme hükmünden sonra 1 Haziran 2005 tarihinde yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanununun [148.](#)

maddesinde de ifade alma ve sorgudaki yasak usuller örneksene yoluyla ve sayılanlarla sınırlı olmayacak biçimde gösterilmiş, ayrıca önceki yasal düzenlemeye benzer biçimde, "yasak usullerle elde edilen ifadelerin rıza ile verilmiş olsa dahi delil olarak değerlendirilemeyeceği" hükme bağlanmıştır. Keza 217. maddenin ikinci fıkrasında, "yüklenen suçun, hukuka uygun olarak elde edilmiş her türlü delille ispat edilebileceği" belirtilmiştir. Madde metninden de açıkça anlaşılacağı üzere, hukuka uygun olarak elde edilmeyen deliller, yeni ceza yargılama sistemimizde de ispat aracı olarak kabul edilmemiştir. Kaldı ki, 230. maddenin birinci fıkrası uyarınca, mahkûmiyet hükmünün gerekçesinde, delillerin tartışılması ve değerlendirilmesi, hükme esas alınan ve reddedilen delillerin belirtilmesi; bu kapsamda dosya içerisinde bulunan ve hukuka aykırı yöntemlerle elde edilen delillerin ayrıca ve açıkça gösterilmesi de zorunludur.

"Yasadışılıktan" daha geniş bir içeriğe sahip olan "hukuka aykırılık kavramı" ise, gerek pozitif hukuk metinlerine gerekse kişilerin temel hak ve hürriyetlerine ilişkin evrensel hukuk ilkelerine aykırılık olarak anlaşılmalıdır. Bu kavram, Anayasa Mahkememizin 22.06.2001 gün ve 2-2 sayılı kararında da benzer biçimde tanımlanmıştır.

Sözü edilen kararda: "Hukuka aykırılık en başta milli hukuk sistemimiz içinde yürürlükteki tüm hukuk kurallarına aykırılık anlamına gelir. Bu çerçevede içinde, anayasaya, usulüne uygun olarak kabul edilmiş uluslararası sözleşmelere, kanunlara, kanun hükmünde kararnamelere, tüzüklere, yönetmeliklere, içtihadı birleştirme kararlarına ve teamül hukukuna aykırı uygulamaların tümü hukuka aykırılık kavramı içinde yer alır.

Bunun dışında, hukuk sistemimiz, hukukun genel ilkeleri adı verilen ve uygar dünyanın tüm medeni ülkelerinde uygulanan kuralları da hukuk kuralı olarak kabul etmektedir. Hukukun genel ilkelerinin neler olduğu konusunda bir belirsizlik olsa da, hukukun genel ilkelerinin hukuki bağlayıcılığı bulunduğu gerek uygulamada gerekse doktrinde tartışmasız olarak kabul edilmektedir. Anayasa Mahkememiz de birçok kararında,

hukukun genel ilkelerinin varlığını kabul etmenin hukuk devletinin gereklerinden biri olduğunu ve bu ilkelerin yasakoyucu tarafından dahi yok edilemeyeceğini hükme bağlamıştır (örneğin bkz. E. 1985/31. K. 1986/1, KT. 17.3.1986, Anayasa Mahkemesi Kararlar Dergisi, S. 22. s. 115). Anayasa Mahkemesi'nin bu görüşleri çerçevesinde hukukun genel ilkeleri, yasalardan, hatta Anayasa'nın değiştirilebilir hükümlerinden de üstün bir konuma getirilmiştir." denilmektedir.

Açıklanan pozitif hukuk normları ve uygulamayı yansıtan yargısal kararlar karşısında belirtmek gerekir ki; "hukuka aykırı biçimde" elde edilen deliller, Türk Ceza Yargılaması Hukuku sisteminde dikkate alınamaz. Bu bakımdan, sanığın konutunda hukuka aykırı olarak gerçekleştirilen arama işleminde elde edilen maddi delil ile buna ilişkin düzenlenen ekspertiz raporlarının Yerel Mahkemece hükme esas alınması isabetsiz bulunmuştur.

Esasen somut olayda; aramanın hukuka aykırı olduğu ve sonucunda elde edilen delilin hükme esas alınamayacağı hususunda Yargıtay Özel Dairesi ile Yargıtay C.Başsavcılığı arasında bir görüş farklılığı bulunmamaktadır. Çözümü gereken uyuşmazlık, hukuka aykırı aramada elde edilen maddi delil dışındaki diğer delillerin, bu bağlamda hakkındaki ihbar ile sanığın mevcut ikrarının somut olayda mahkumiyet için yeterli olup olmadığı hususunda toplanmaktadır.”²⁹⁴

Ancak son dönemde Yargıtay’ın yerleşmiş olan bu içtihadından saptığı ve nisbi ve mutlak hukuka aykırılık görüşüne kararlarında yer verdiği gözlemlenmektedir. Ceza Genel Kurulu’nun 13.03.2012 tarih, E. 2011/8-278 ve K. 2012/96 sayılı kararına göre:

“...uyuşmazlığa konu olayda, aramaya ondört kolluk görevlisi ile sanığın katıldığı, bununla birlikte Yasanın arama sırasında bulunmasını istediği diğer kişilerin katılmadığı, bunun da şeklen hukuka aykırı olduğu ve 5271 sayılı CYY’nin 217. maddesinin 2. fıkrasında; "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir"

²⁹⁴ Yargıtay Ceza Genel Kurulu, 29.11.2005 tarih E. 2005/7-144, K. 2005/150, www.kazanci.com, (Erişim 20 Nisan 2014)

şeklindeki hüküm uyarınca, arama sonucu elde edilen delilin hukuka uygun biçimde elde edilen delil niteliğinde bulunmadığı ileri sürülebilir ise de; usulüne göre alınmış bir arama kararı bulunan somut olayda, bu karara ve kararın infazı sırasında yapılan işlemlere yönelik bir itiraz vaki olmadığı gibi, arama işlemine ve arama yapılırken bir takım haklarının ihlal edildiğine yönelik olarak sanıktan gelen herhangi bir yakınma da bulunmamaktadır.

Bu nedenle, sırf arama sırasında şekle ilişkin bir koşulun ihlal edilmesine dayanılarak aramanın hukuka aykırı sayılmayacağı ve ele geçirilen delillerin "hukuka aykırı biçimde elde edilmiş delil" olarak nitelenemeyeceğinin kabulü gerekmektedir.

Öğretide de; Prof. Bahri Öztürk, Doç. Dr. Mustafa Ruhan Erdem ve Doç. Dr. Veli Özer Özbek tarafından hazırlanan Uygulamalı Ceza Muhakemesi isimli eserde bu konudan bahsedilirken, ikili bir ayırım yapılarak, bu tasnifte; hak ihlalinin niteliği üzerinde durulup, bir hukuk devletinde bazı hakların mutlak, diğer bazı hakların ise nisbi koruma altında bulundurulduğu belirtildikten sonra; buna bağlı olarak "mutlak delil yasakları" ve "nisbi delil yasakları" kavramlarının ortaya çıktığı ifade edilmiştir. Buna göre mutlak delil yasakları;

- 1- Sanığın kendisini suçlandırıcı beyanda bulunmaya zorlaması,*
- 2- Bir kimsenin yakınlarını suçlandırıcı beyanda bulunmaya zorlanması,*
- 3- Sanığa kendisi ile ilk temasa geçen yetkili tarafından bazı haklarının hatırlatılmaması, (susma hakkı, müdafî tayini isteme hakkı gibi)*
- 4- Hayatın gizli alanına (özel hayatta değil) yapılan müdahaleler,*

Olarak sayılmış, bunların dışında kalan durumlarda ise hakim tarafından oranlılık (ölçülülük) ilkesi göz önünde tutularak "kamu yararı" bakımından bir değerlendirme yapılması gerekliliğinden bahsedilmiştir.

Bu bağlamda; illiyet bağı, etkileme gücü ve hak ihlali kriterlerine yer vermeden yapılan bir değerlendirmenin; "herhangi bir hakkın ihlal edilmediği her türlü basit şekli aykırılıkların da mutlak bozma sebebi

sayılmasını" gerektireceği için, böyle bir yaklaşımın ceza yargılamasında hakkaniyete aykırı sonuçların doğmasına, adalet ve eşitlik ilkelerinin zedelenmesine yol açabilecek son derece ağır sonuçları da birlikte getireceği kuşkusuzdur.

Her şekle aykırılığın aynı zamanda bir hak ihlaline de yol açacağı şeklindeki bir kabul isabetli olmayacağından, olayımızda olduğu gibi "Cumhuriyet savcısı, iki ihtiyar heyeti üyesi veya iki komşu" bulunmadan yapılan bir aramada, CYY'nin 119. maddesine şekli bir aykırılık söz konusu ise de, herhangi bir hakkın ihlal edildiği söylenemeyecektir.

Usulüne göre alınmış arama kararına istinaden, herhangi bir hak ihlaline neden olunmadan yapılan arama sonunda ele geçen delillerin, sadece arama sırasında bulunması gereken kişilerin orada bulundurulmaması suretiyle şekle aykırı hareket edildiğinden bahisle "hukuka aykırı olarak elde edilmiş delil" sayılmaları ve mahkumiyet hükmüne dayanak teşkil edememeleri kabul edilemez."²⁹⁵

Yargıtay son dönemde verdiği kararlarda içtihat değişikliğine giderek hakların mutlak ve nisbi olarak ayrılması kapsamında mutlak ve nisbi hukuka aykırılık görüşünü benimsediğini açıkça belirtmiştir. Yargıtay bu kararlarıyla bazı hukuka aykırılıkların varlığı tespit etmekle birlikte bunları önemsiz, basit ve şekli olarak kabul ederek bu nitelikteki delillerin kullanılabileceğini belirtmektedir.

Çalışmamız kapsamında daha önce ifade ettiğimiz üzere, Yargıtay'ın bu görüşü bir yorumdur. Ancak bizim hukukumuz ve uygulamada olan hukuki metinlerimiz henüz bu yoruma elverişli değildir. Yargıtay'ın verdiği bu kararların şu an yürürlükte olan kanunlar açısından bir temeli bulunmamaktadır²⁹⁶.

4- AİHM Kararları Kapsamında Hukuka Aykırı Deliller

AİHM kararları kapsamında hukuka aykırı deliller ayrıca değerlendirilmemiştir. Zira mahkeme AİHS kapsamında ele alınan hakları ele alır ve

²⁹⁵ Yargıtay Ceza Genel Kurulu, 13.03.2012 tarih, E. 2011/8-278 K. 2012/96, www.kazanci.com, (Erişim 20 Nisan 2014)

²⁹⁶ Ünver ve Hakeri, **a.g.e.**, s.174-175.

sözleşme kapsamında hukuka aykırı delillerle alakalı bir madde bulunmamaktadır. Mahkeme ulusal mahkemeye sunulan delilleri değerlendirmemektedir ve yine Mahkeme muhtelif kararlarında kanıtın kabul edilip edilmemesinin iç hukuk kurallarına göre, toplanan delillerin değerlendirilmesinin de ilke olarak ulusal mahkemelere ait olduğunu belirtmiştir²⁹⁷.

Ancak Mahkeme hukuka aykırı delillere ilişkin tespitlerini Sözleşmenin 6. maddesinde yer alan adil yargılanma hakkı çerçevesinde değerlendirmektedir. Mahkeme değerlendirmesini yalnızca adil yargılanma hakkı kapsamında yapar. Zira *Khan-İngiltere* kararında özel hayatın gizliliğinin (AİHS 8. Madde) ihlal edilmesi suretiyle elde edilen delillerin, adil yargılanma hakkının (AİHS 6. Madde) zedelenmemesi şartıyla kullanılabileceği kararlaştırılmıştır. Bu kararda Mahkeme, 8. madde açısından, suç tarihinde gizli dinleme cihazlarının kullanılmasını düzenleyen İçişleri Bakanlığının rehber kurallarının ulaşılabilir olmaması nedeniyle müdahalenin kanunla öngörülmüş olmadığına ve 8. maddenin ihlal edildiğine karar vermiştir²⁹⁸. Ancak 6. madde açısından kararda belirtildiği üzere başvuru doğrudan hukuka aykırı delillere değinmemiş fakat üç hususun yerel mahkeme tarafından yerine getirilmiş olması gerektiğinin altını çizmiştir. Bu hususlar; başvuru delilinin kabul edilebilirliğini etkili biçimde sorgulayabileceği bir usulün bulunmuş olması, mahkemenin ihlalin niteliğine dikkat etmiş olması ve mahkumiyetin tamamen sözleşmeyi ihlal eden bir delile dayandırılmamış olmasıdır. Ancak Mahkeme, gizlice kaydedilmiş materyallerin başvuru delilinde kullanılması, 6. madde kapsamındaki adillik kavramını ihlal etmediğini kararlaştırmıştır²⁹⁹.

Mahkeme hukuka aykırı olarak elde edilmiş bir bulgunun tek başına sözleşmenin 6. maddesine aykırılık oluşturmayacağını, ancak somut olaya göre aykırılık oluşturabileceğini kabul etmektedir³⁰⁰. Mahkemenin bu tutumu *Schenk* kararında açıkça gözlemlenebilir. Sözleşme kapsamında delillerin geçerliliğine ve kabul edilebilirliğine ilişkin herhangi bir düzenleme bulunmamasına karşın Mahkeme yalnızca ceza muhakemesinin ilgiliye karşı bir bütün olarak adil olup

²⁹⁷ Ali Rıza Çınar, “Hukuka Aykırı Kanıtlar”, **Türkiye Barolar Birliği Dergisi**, Sayı 55, 2004, <http://tbbdergisi.barobirlik.org.tr/m2004-55-83>, (Erişim 20 Nisan 2014), ss. 35-64, s. 47.

²⁹⁸ Mualla Buket Soygüt Arslan, “Avrupa İnsan Hakları Mahkemesi’nin Mialhe/Fransa Kararı”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, İstanbul Yıl: 8, Sayı 16, Güz 2009 s. 159-171, s. 166

²⁹⁹ *Khan/İngiltere*, 35394/97, 12 Mayıs 2000.

³⁰⁰ Çınar, **a.g.e.**, s. 47.

olmadığının denetimini yapmak zorundadır³⁰¹. Mahkeme *Schenk* kararında, özel bir kişi tarafından hukuka aykırı olarak alınmış telefon kayıtlarının delil olarak kullanılmasının, muhakeme sürecinin tümü incelendiğinde, adil yargılanma hakkını zedelediğine kanaat getirmiştir³⁰². Mahkeme, başvurucuya muhakeme sürecinde delillerin sağlamlığını tartışma olanağı verilmesi ve muhakeme kapsamında kanaate varış sürecinde birçok delilin dikkate alındığını belirterek ihlal olmadığına karar vermiştir³⁰³.

III-Ceza Yargılamasında Dijital Delillerin Hazırlanması ve Sunulması

Dijital delillerin delil olarak yargılamada kullanılabilmesi için belirli usuller çerçevesinde ele geçirilmesi ve belirli incelemeleri geçirdikten sonra mahkemeye sunulması gerekmektedir. Bu süreç adli bilişim disiplininin belirlediği usuller çerçevesinde gerçekleşmektedir. Çalışmamızın bu kısmında kriminolojik açıdan dijital delillerin incelemeye alınmaları, incelenmeleri, analiz edilmeleri ve raporlanarak sunulmaları konu edilecektir. Başka bir ifade ile çalışmamızın bu bölümü dijital delillerin kriminolojik sürecini inceleyecektir. Bu süreci aşama aşama açıklamaya geçmeden önce burada dijital delilleri kimin toplamaya yetkili olduğu konusunda yapılan tartışmalara değinmekte fayda vardır.

Dijital verilerin hukuki anlamda delil olarak kullanılabilmesi 1990'lı yıllarda gündeme geldiği için özellikle geçtiğimiz bu dönem açısından dijital delillerin kim tarafından inceleneceği akla gelen ilk sorulardan olmaktadır. Tıpkı dijital deliller gibi maddi delillerin (fiziksel deliller) bir türü olan DNA veya parmakizi incelemeleri alanında uzman kişilere ulaşmak günümüzde zor olmazken; dijital delillerin derin bilişim bilgisi isteyen incelemelerini üstlenecek kişilere ulaşmak bu sürecin ilk başında kolay olmamıştır³⁰⁴. Ancak dijital sistemlerin insan hayatındaki yerinin artması ile birlikte bu alanda yetişmiş uzman sayısı da artmıştır.

³⁰¹ Serap Keskin Kızıroğlu, AİHM'de Hukuka Aykırı Deliller ve AİHM Schenk Örneği, **18. Hukuk İhtisas Semineri, Özel Hayatın Korunması**, İstanbul: Emniyet Genel Müdürlüğü/Basımevi, Yayın No 7, 18-19-20 Ekim 2002, ss. 104-106, s.105

³⁰² A.g.e., s. 105

³⁰³ A.g.e., s. 105.

³⁰⁴ Casey, a.g.e., s. 6.

Günümüzde dijital sistemlerden delil elde edilmesi kolluk ve savcılık makamlarının işlerinin ayrılmaz bir parçası haline gelmiştir. Bu nedenle bu alanda sorumlu her kişinin dijital delillerin hassas yapısını, bu konuya hakim olan ilkeleri, bu delillerin toplanmasını ve muhafazasına ilişkin yöntemleri bilmesi zorunludur³⁰⁵. Günümüzde dijital delillerin tespit edilmesi, toplanması, incelenmesi, muhafaza altına alınması ve nakil edilmesi işlemlerinden adli kolluk görevlileri ve adli bilişim uzmanları sorumludur³⁰⁶. Ancak dijital sistemlerin karmaşıklığı sebebiyle bazı durumlarda işletmeler, iletişim servis sağlayıcıları ve bilgisayar uzmanları da bu tür verilerin incelenerek maddi gerçeğin ortaya çıkartılması için birincil sorumlularla beraber çalışma yürütmektedir³⁰⁷.

Bu kapsamda dijital deliller öncelikle elde edilmeli, ardından incelemeye tabii tutulmalı, yapılan bilişim incelemesinden sonra bu veriler analiz edilmeli başka bir deyişle değerlendirilmelidirler. Son aşama olarak yapılan bu değerlendirmelere ilişkin bir rapor düzenlenmeli ve bu rapor mahkemeye sunulmalıdır.

A- Dijital Delillerin İncelemeye Hazırlanması

Dijital delillerin elde edilmesi dijital verilerin delil olarak değerlendirilmesi sürecinin ilk basamağıdır. Dijital delillerin incelenme aşamaları doktrinde soğan benzetmesiyle görselleştirilmektedir. Bu benzetmeye göre soğanın en dışındaki kabuk fiziki araçlardır. Kabuğun altına doğru katmanlar sırasıyla işletim sistemi, dosya sistemi, dosya ve içerik analizi olarak sıralanmaktadır³⁰⁸.

Bu benzetme özellikle dijital verilerin durağan (statik) hali için yapılmaktadır. Bir disket üzerine kaydedilmiş dijital veri dijital verinin statik halinin en somut örneğini oluşturmaktadır. İşletim sistemi kullanılarak disket üzerindeki veriye ulaşılır. İşletim sistemi içerisinde bulunan dosya sistemi uygulamaların oluşturduğu dosyaları depolar ve düzenler. Bu sistem içerisinde dijital verinin yer aldığı dosyaya ulaşılır ve içerik analizi yapılabilir. Bu süreçlerin her biri kendine has zorluklar içermektedir. Verinin içerik analizine gelene kadar her aşamada ayıklanması

³⁰⁵ Berber, **a.g.e.**, s. 43.

³⁰⁶ **A.g.e.**, s. 43.

³⁰⁷ Casey, **a.g.e.**, s. 7.

³⁰⁸ Pollit, **a.g.e.**, s. 499.

gereken diğer veriler bilişim uzmanının işini zorlaştırmaktadır. Zira binlerce veriyle dolu bu dijital sistemler içerinden inceleme yaparken önemli verilerin gözden kaçırılmaması gerekmektedir³⁰⁹. Öte yandan adli bilişim incelemelerinin uzun sürmesi davaların sonuçlanması açısından olumsuzluklara sebep olduğu için, her verinin incelenmesi iş yükünü artırırken veriler arasında tercih yapılması adli süreçleri bambaşka sonuçlandırabilecek önemli hatalara yol açmaktadır. Bu sebeple yabancı doktrinde dijital verilerin ele geçirilmesinden delil olarak kullanılmasına kadar geçen inceleme sürecine ilişkin yeniliklere ihtiyaç olduğu öne sürülmektedir³¹⁰.

Dijital verinin incelenmesi bu şekilde gelişirken söz konusu inceleme aşamalarından ilkinin verinin elde edilmesi oluşturur. Bu ilk evrede önemli olan adli bilişim incelemesine tabii olacak delilin hukuki ve bilimsel değerini koruyacak şekilde toplanmasıdır. Bu genellikle verinin kayıtlı olduğu dijital alete el konulması yada birebir kopyasının alınması yoluyla olmaktadır. Kopyalama işlemi genellikle verinin görüntüsünün alınması (image) ya da veri akışı kopyasının (bit-stream copy) alınması ile olmaktadır. Veri akışı kopyasının alınması tüm sistem üzerinde gizlenen bilgilere ulaşılmasını sağladığı gerekçesiyle daha sağlıklıdır. Verinin internet veya iletişim ağları üzerinde ele geçirilmesi için ise veri akışının bir kısmı ya da tamamı toplanır. Toplanan bu veriler daha sonra sırasına dizilerek bir bütün oluşturulur³¹¹.

Pollitt'in görüşüne göre, arama kararı kapsamında dijital verilerin bulunduğu cihazlara el konulacağı zaman aramayı yapacak yetkili kişilerin verinin orijinal haline el konulmasına gerek olup olmadığını belirlemeleri önem arz eder. Zira bazı durumlarda bu araçlara el koymak gereksiz, uygunsuz veya özel iletişim hallerinde olduğu gibi izin alınamaz olabilir. Pollitt, delillere el konulmasını devlet ile tarafların menfaatleri arasında önemli bir denge unsuru olarak görmektedir³¹².

Pollitt'in bu düşüncesi yabancı doktrinlerde oldukça önemli bir nokta olarak gündeme getirilmektedir. Tahkik amacıyla gelen görevlilerin tüm cihazlara el koyması oldukça kolay bir yöntem olmakla beraber çok zarar verici de olabilir. Bir işyerinde yapılan aramayı ele alacak olursak, o işyeri açısından elzem olan cihazlara

³⁰⁹ A.g.e., s. 498 vd.

³¹⁰ Eoghan Casey, Monique Ferraro, Lam Nguyen, "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence", *Journal of Forensic Sciences*, Cilt 54, Sayı 6, November 2009, s. 1353.

³¹¹ Pollitt, a.g.e., s. 500.

³¹² A.g.e., s. 500.

el konulması söz konusu iş yerinin faaliyet gösteremeyeceği anlamına gelmektedir. Bu sebeple her el koyma gerekçeli, uygun ve orantılı olmalıdır. El konulacak verilerin orantılılığı konusundaki hassasiyet kendini İngiltere'nin bu konudaki kılavuz metni olan ACPO'nun Dijital Deliller için En İyi Uygulama Rehberi'nde göstermektedir³¹³. ACPO bu uygulama belgesinin 4.3. bölümünde el konulacak cihazları da ayrıştırarak temelde el koyma işlemi gerçekleştirilmeden el konulacak cihazın aranan delili içerdiği konusunda emin olunması prensibini getirmiştir³¹⁴.

B- Dijital Delillerin İncelenmesi

Ele geçirilen dijital delillerin incelenmesi aşamasında her ülkenin kendi hukuku çerçevesinde getirildiği bir takım yaklaşımlar mevcuttur. Ancak maalesef şu an ülkemiz hukuk sisteminde dijital delillerin nasıl inceleneceği yönünde üzerinde uzlaşma sağlanmış herhangi bir meslek kuralları bütünü bulunmadığı için bu alana dair açıklamalarımızı yabancı hukuk sistemlerinde soruşturmada görevli polis kuvvetlerinin veya adli bilişim uzmanlarının yayınlamış oldukları kurallar çerçevesinde incelemek durumunda kalacağız.

Bu aşamada ilk yapılması gereken incelemeyi gerçekleştirecek kişinin bir inceleme amacı saptamasıdır³¹⁵. ACPO'nun belirlediği uygulama rehberinin 5.2. bölümünde de belirtildiği üzere dijital aletlerin inceleme kapasitesine aşacak kadar çok veri depolama kabiliyetleri sebebiyle neyin araştırıldığı, temel odak noktasının ne olduğu stratejik olarak belirlenmelidir³¹⁶.

İnceleme amacının belirlenmesi ile birlikte bu amaca en uygun inceleme araçlarına karar verilmelidir. Bu aşamada öncelikle ön izleme (previewing) olarak bilinen bir işleme başvurularak hangi cihazın incelemesine öncelik verileceği saptanmalıdır. Ön izleme (previewing) bir ağa bağlanarak ya da ağlarlar tüm

³¹³ Association of Chief Police Officers, **Good Practice Guide for Digital Evidence**, <http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf>, (Erişim tarihi Mart 2013). Rehber kapsamında İngiltere'deki rehber metne sıkça atıf yapılmaktadır. Çalışmamız kapsamında dijital deliller açısından çıkarılmasını önerdiğimiz Yönetmelik için de yine bu rehber metin örnek alınmıştır. Metnin orijinali ve ilgili kısımların tercümesi için Ekler bölümüne bakınız.

³¹⁴ Angus Marshall, **Digital Forensics: Digital Evidence in Criminal Investigation**, West Sussex: Wiley-Blackwell Print, 2008, s. 21 vd.

³¹⁵ Pollitt, s. 500.

³¹⁶ Association of Chief Police Officers, **Good Practice Guide for Digital Evidence**, <http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf>, (Erişim tarihi Mart 2013).

bağlantılar kopartılarak yapılabilir. Ağlarla tüm bağlantılar kopartılarak yapıldığında verilere ağlar üzerinden gelecek zarar önlenmiş olmaktadır. Bu uygulamanın en büyük sıkıntısı ise fiziksel olarak depolanan veriye ulaşabilmek için cihazın kapatılması gerekliliğinin ortaya çıkabilmesidir. Zira her cihaz inceleme esansında kapatılamayabilir. Bu tür durumlarda ise dış ağlara bağlı (online) ön izleme önem kazanır³¹⁷.

Ön izlemenin (previewing) temel amacı, cihaza hukuki sebeplerle el konulmasını sağlayacak “olası nedene” yakın bir veriye ulaşmaktır. Bu kapsamda getirilen inceleme kurallarına ne kadar riayet edilirse edilsin ön izleme metodu ile incelenen verilerde değişikliğin olmadığını kanıtlamak oldukça güçtür ve istihbarat amacı dışında bu yöntemle elde edilen verilerin kullanılmasının güç olduğu belirtilmiştir³¹⁸. Kanaatimizce istihbarat amacıyla dahi sıhhatinden şüphe edilecek verilere dayanmak sakıncalı sonuçlar ortaya çıkarabileceği için bu konu üzerinde dikkatle inceleme yapılması gereken ayrı bir çalışma alanına girmektedir.

Dijital delillerin incelenmesinde bir diğer yöntem olarak görüntü alınması (imaging) incelenebilir. Dijital verilerle çalışırken her zaman bir kopyası üzerinden işlem yapmak daha sağlam olarak görülmektedir. Bir dijital cihazın verileri kopyalanırken birebir bütün kopya alınabilmesi çok önemlidir. Zira böyle bir kopya ile kullanılmayan alanlar, silinmiş veriler ve zarar görmüş alanlara ulaşılabilecektir³¹⁹.

Bir diğer metot yedeklemektir (backups). Bu yöntemin en önemli özelliği yedekleme işlemi işlemin yapıldığı anda dijital cihazın bellek kopyasını sağlamaktadır. Başka bir deyişle bu yöntem ile yedeklemenin yapıldığı anda dijital cihazın anlık görüntüsü ele geçirilmektedir. Ancak bu burada unutulmaması gereken bir özellik de bu metot ile elde edilen her görüntü kısmi olarak elde edilmektedir. Bu sebeple saklanmış verilere erişmek için iyi bir yöntem olmadığına dikkat çekilmelidir³²⁰.

Bahsedilen bu tür metotlar aracılığıyla yapılan incelemelerde ilk başta belirlenen inceleme amacı kapsamında bazı tekniklerle silinmiş verilere ulaşmak için veri kurtarma (data recovery), inceleme kapsamından muaf tutulmuş veriler için

³¹⁷ Marshall, **a.g.e.**, s. 46.

³¹⁸ **A.g.e.**, s. 46.

³¹⁹ **A.g.e.**, s. 47 vd.

³²⁰ **A.g.e.**, s.48.

veri azaltımı (data reduction) ve verilerin içeriklerine ulaşmak için içerik araştırması (content search) gibi yöntemlerden de yararlanılabilir³²¹.

Dijital verilerin incelenmesinde en önemli aşamalardan bir tanesi ise herhangi bir usulle görüntüsü (image) elde edilmiş olan verinin ve incelenmiş olan cihazın tıpkı bir olay yeri gibi davranılarak korumaya alınması gerekliliğidir. Değişimi engelleyici metotlar (write-blocking) incelemeye tabii tutulan araçların bir daha değiştirilememesini sağlayabilir. Bu aşamada incelemeyi gerçekleştiren kişinin de verilerde herhangi bir değiştirme veya tahribat yapmadığından emin olmak gerekmektedir. Bu tür güvenlik önemleri elde edilen verilerin delil değerini doğrudan ilgilendirdiği gibi yanı zamanda incelemeyi yapan kişiye de birden çok defa yapılan işlemi kontrol ederek hata sonucu oluşabilecek yanlışlıklardan kendini korumasını sağlar³²².

Dijital delillerin incelenmesi aşamasının son safhasını ve belki de en önemli olan kısmını bu delillerin korunması oluşturur. Dijital deliller hukuka uygun bir şekilde korunmalıdırlar ki mahkemede hakim önüne çıkartılabilsinler. Koruma teknikleri de tıpkı inceleme tekniklerinde olduğu gibi değişiklik göstermektedir. Bunun için güvenli bir depolama bölgesinin bulunması, yeterli yedekleme işlemlerinin yapılması ve mutlaka verinin orijinal halde olduğunun kanıtlanması gerekir³²³. Dijital verilerin hash değerlerinin alınmasının önemi kendini bu noktada da göstermektedir³²⁴.

C- Dijital Delillerin Analiz Edilmesi

Dijital delillerin incelenmesi ve analiz edilmesi süreçleri esasen birbirine çok yakın süreçlerdir. Şöyle ki, yukarıda açıklandığı üzere çeşitli bilişim metotları kullanılarak incelenen verilerin bu kısmında analiz edilmesi gerekir. Analiz işlemi somut soruşturma konusunda incelenen verilerin değerlendirilmesi aşaması olarak

³²¹ Pollitt, **a.g.e.**, s. 501.

³²² Marshall, **a.g.e.**, s.48.

³²³ Stuart Cameron, **Digital Evidence**, FBI Law Enforcement Bulletin, Ağustos, 2011, s. 15.

³²⁴ Çalışmamızın yukarıdaki bölümlerinde de değindiğimiz üzere hasd değeri alınmış dijital veriler üzerinde değiştirme yapıp yapılmadığı kolayca anlaşılır. Zira incelemenin başında alınan hash değeri ile sonunda alınan hash değerinin birbirini tutumaması inceleme sırasında dijital delilin orjinallik özelliğini kaybettiğini göstermektedir.

tanımlanabilir. Bu iki safha birbirinden ayrılamaz olarak düşünülse de dijital deliller açısından en önemli kısım analiz kısmıdır. Zira bu kısımda ele geçirilen veriler incelendikten sonra şu üç soruya cevap verip vermedikleri araştırılmalıdır:

- Bu veriler davaya ilişkin vakıaları kanıtlıyor mu?
- Elde edilen bu veriler şimdiye kadar bilinenleri doğrulamakta mı?
- Bu bir delil midir yoksa delil başlangıcı değerinde midir? ³²⁵

Bu sorulara verilecek cevaplar doğrultusunda soruşturma kapsamında ele geçirilen dijital veriler değerlendirilecek, delil olarak sunulup sunulmayacaklarına karar verilecektir. Dijital delillerin analiz edilmesi aşamasında ilişkin İngiltere Polis Teşkilatının yayınlamış olduğu Dijital Deliller için En İyi Uygulama Rehber Kitap 5.10. bölümünde yer alan Dijital Verilerin Yorumlanması başlığına da değinmekte yarar vardır. Bizim çalışmamızda dijital delillerin analiz edilmesi başlığı altında incelediğimiz dijital verilerin somut soruşturma konusu açısından değerinin tespit edileceği analiz aşaması bu rehber kitapta incelenirken ele geçirilen dijital verilen nasıl yorumlanması gerektiğinden de bahsedilmiştir.

Rehberde açıklandığı üzere dijital verilerin delil olarak analiz edilmesinde bu işlemi yapmakla görevli olan kişinin bilgi ve tecrübesinin önemi büyüktür. Zira rehberde verilen örnekte olduğu üzere bir bilgisayarda ele geçirilen müstehcen çocuk resimleri kendiliğinden kişinin bu resimlerin sahibi olduğu anlamına gelmez. Bu resimlerin beklenen doğrultuda delil oluşturabilmesi için kişinin bu resimlerin varlığından haberdar olması gerekir. Aynı şekilde delillerin kökenini belirlemek de araştırmayı yapacak olan uzmana düşmektedir. Dijital ortamda bulunan verilerin öylesine orada bulundukları değil, soruşturma konusu olayla ilgili oldukları ve suç atfında bulunan kişiye ait olduklarını belirlemek bu araştırmayı yapacak olan bilişim uzmanına aittir. İngiltere Polisi'nin yayınladığı rehber kitapta delillerin kökeninin belirlenmesi meselesi bir DNA örneği ile açıklanmaktadır. Şöyle ki, olay yeri incelemesinde bir şişe üzerinde sanığın parmak izlerinin bulunması bu suçun sanık tarafından incelendiği anlamına gelmemektedir. Zira o şişe oraya başka birileri tarafından da konulmuş olabilir. Dolayısıyla aynı bu örnekte bahsedildiği üzere

³²⁵ Pollitt, **a.g.e.**, s. 501.

gerektiği takdirde delil olarak kabul edilebilecek oluşumların kökenlerini ve aidiyetlerini belirlemek de bu analizi yapacak olan bilişim uzmanına düşmektedir.³²⁶

D-Dijital Delillere İlişkin Düzenlenen Raporların Sunulması ve Delillerin İbrası

Dijital delillerin mahkemeye sunulması üzerlerinde yapılan incelemeden sonra hazırlanacak bir rapor yahut mahkemenin inceleyebileceği şekle getirilmeleri ile gerçekleşir. Bu aşamada da uzman bir kişinin teknik bilgi ve deneyiminden yararlanılmaktadır³²⁷.

Yukarıda ele aldığımız usullerde incelenen dijital deliller incelemenin içeriğini açıklayan ve bulguları belirten bir yazılı rapor formunda yahut yine bir elektronik belge formunda mahkemeye teslim edilir. Hazırlanan raporlar açısından en önemli nokta bu raporların söz konusu teknik bilgiye hakim olmayan kimseler tarafından da kolayca anlaşılır nitelikte olması gerekliliğidir³²⁸.

Tıpkı normal keşiflerde olduğu gibi dijital verilerin elde edildiği keşiflerde de temel amaç her zaman için söz konusu davayı açıklığa kavuşturacak belgelerin belirlenmesidir. Belirlenen bu belgeler incelemeye tabii tutularak ilgili verilere ilişkin bir rapor hazırlanır ve inceleme sona erdirilir. Bu süreçle ilişkin tüm notlar muhafaza edilmelidir. Zira araştırmayı yapan uzmanın gerektiğinde inceleme prosedürüne ilişkin beyan vermesi gerekebilir. Leyla Keser Berber'in ve Erdem Akyazılı'nın değindiği gibi dijital verilerin incelenmesi sürecinde verilerin keşfinde delillerin bütünlüğünü ve kalıcılığını sağlamak oldukça önemlidir³²⁹.

Özellikle Anglo-Amerikan hukukunda dijital delillerin incelenmesine ilişkin raporlar bu incelemeyi bizzat yapan uzman kişilerde mahkemeye sunulmaktadır. Bu kişilerin hazırladıkları raporla birlikte beyanları da mahkeme huzurunda dinlenilir. Bu beyan bir çeşit bilirkişi görüşü gibi kabul görür ve bu tür hukuk sistemleri

³²⁶ Association of Chief Police Officers, **Good Practice Guide for Computer-Based Electronic Evidence**, <http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf>, (Erişim tarihi Mart 2013).

³²⁷ Göksu, **a.g.e.**, s. 67.

³²⁸ Pollitt, **a.g.e.**, p. 502.

³²⁹ Berber ve Akyazılı, **a.g.e.**, s. 30.

içerisinde tanık beyanında daha itibar edilen bir tür beyanı oluşturur. Amerika Birleşik Devletleri Federal Delil Kurallarına göre uzman görüşünü bildirecek kişinin alanındaki yeterliliği incelenir ve uygun görüldüğü takdirde uzmanın söz konusu fiziki delil ile ilgili mevcut vakıyı tespit etmeye yarayacak sonuçlara varmasına izin verilir. Uzman tarafından mahkemeye sunulan inceleme raporu ve uzmanın kendi beyanları da çapraz sorgu yöntemi ile sorgulanmaya tabii kılınır³³⁰. Ancak bizim hukukumuzda benzer düzenlemeler olmayıp sadece bilirkişi kurumu vardır. Dijital delillere ilişkin incelemeler ve hazırlıklar hakimnin gerekli gördüğü hallerde bilirkişilik kurumuna başvurması ile gerçekleşir³³¹.

Dijital delilin incelemesini yapan ve bu konuda bir rapor hazırlayan uzman kişinin en büyük sorumluluğu yazdığı raporun objektifliğini sağlamaktır. Bu doğrultuda uzmanın temel görevi mahkeme heyetini yönlendirmek değil, onları bilmedikleri bir alanda aydınlatmak olmalıdır³³². Zira bilimsel yöntemleri fiziksel delillere uygulanması sonucunda onlarca kişinin hayatlarını etkileyebilecek sonuçlar çıkabilmektedir. Bu sebeple uzmanları tarafsız bir görüş olarak sadece kendilerine incelenmek üzere teslim edilen dijital verileri usullerine uygun olarak inceleyip bilimsel konularla ilgili mahkemeyi aydınlatmakla görevlidirler.

Dijital delillerin incelenmesi sonucunda uzman kişilerin yazdıkları raporların haricinde bu delillerin mahkemeye nasıl sunulacağı ise ayrı bir tartışma konusudur. Bu husus başlıca başka problemleri de içerir. Dijital verilerin somut bir görünümü olmadığı için incelemeye tabii tutulan, içeriklerine ilişkin rapor düzenlenen bu verilerin mahkemeye sunumunun nasıl olacağı tartışmalı bir alandır. Bu tür delillerin mahkemeye sunulmasında iki temel ayırım gözetilebilir. Bir yol olarak dijital deliller bilgisayar çıktısı ile somut hale getirilerek mahkemeye sunulabilirler. Ancak bilgisayar çıktısı dijital verinin sureti niteliğindedir. Verinin orijinali değildir. Diğer bir yol olarak ise dijital delillerin dijital yöntemlerle mahkemede temsil edilmesidir. Bu noktada karşılaşılabilecek teknik aksaklıklar hususunda dikkatli davranmak gerekir. Zira mahkeme salonlarının yeterli teknik destekten yoksun olmasının yanı sıra bir de her türlü bilgisayar her türlü teknik donanımı çalıştırmaya elverişli değildir. Dijital delillerin dijital ortamlarda mahkemeye sunulması açısından dikkat edilmesi gereken bir diğer nokta ise orijinal hali sunulan verinin değişmemesine ve

³³⁰ Pollitt, **a.g.e.**, s. 502.

³³¹ Göksu, **a.g.e.**, s. 67.

³³² Pollitt, **a.g.e.**, s. 502.

tahrip olmamasına dikkat etmektir. Orijinal halde sunulan veriler doğruluğun tespiti için daha elverişlidir ancak orijinal veri her zaman zarar görmeye açıktır.

IV-Bilişim Yoluyla Elde Edilen Verilerin Delil Olarak Değerlendirilmesi

A-Ceza Muhakemesi Çerçevesinde Dijital Delillerin Kabul Edilebilirliği Meselesi

Ceza Muhakemesi Hukuku'nun temel amacı her zaman için gerçekliğe ulaşmaktır. Medeni muhakemeden farklı olarak ceza muhakemesi tarafların öne sürdüklerinden bağımsız olarak geçmişte ne olduğunu araştırır. Böylece “geçmişte ne olmuştu” sorusunda verilecek cevap doğrultusunda muhakeme sonuçlandırılır ve adalet yerine getirilmeye çalışılır. Bu kapsamda çalışmamızın önceki bölümlerinde de değindiğimiz üzere ceza muhakemesinde deliller medeni muhakemeden farklı değerlendirmelere tabii tutulurlar. Çalışmamızın vicdani kanaat sistemi ve delil serbesti ile ilgili kısmında değindiğimiz üzere, temel amaç maddi gerçekliğe ulaşmak olduğu için ceza muhakemesinde her şey delil olarak kabul edilmektedir.

Bu sebeple “delillerin kabul edilebilirliği” tartışması ceza muhakemesi açısından üzerinde tartışılacak bir husus olmamaktadır. Zira ceza muhakemesi hukukunda delillere ilişkin kesin sınırı delil yasakları oluşturmaktadır ve delil yasakları haricinde temel prensip her şeyin delil olabileceğidir³³³.

Ceza muhakemesi kapsamında delillerin kabul edilebilirliğinin sınırını hukuka aykırı delillerin oluşturduğunu belirtmekle birlikte delillerin kabul edilebilirliği meselesi esas itibariyle jüri ile yargılama yapan daha ziyade Anglo-Amerikan yargılamalarında tartışılan bir meseledir. Çalışmamızın devamında dijital delillerin doğrulanması sorunu ve değerlendirilmesi meselelerine değinip yabancı hukuk sistemlerinden örnekler vereceğimiz için bu kısımda özellikle yabancı hukuk sistemlerinde delillerin kabul edilebilirliği meselesini incelemekte fayda olacağı kanaatindeyiz.

³³³ Akyürek, **a.g.e.**, s. 61.

Delillerin kabulü Anglo-Amerikan hukuk sistemlerinde yapılan yargılamalarda en kapsamlı düzenlenmiş alanlardan biridir. Zira bu hukuk düzenlerinde yapılan yargılamalarda jürinin nihai karar üzerindeki etkisi çok büyük olduğu için gerçeğe aykırı veya davada kullanılamayacak delillerle jürinin etkilenmesi ve doğru düşünceden uzaklaşması önlenmeye çalışılmıştır. Göksu'nun elektronik delillerin hukuk yargılamalarında kullanılmasına ilişkin çalışmasında detaylı olarak belirttiği üzere Amerika Birleşik Devletleri Federal Delil Kuralları'nın (Federal Rules of Evidence, FDR) ilgililik (relevancy), önemli olma (materiality) (FRE Bölüm IV), doğrulama (authentication) (FRE Bölüm IX) ve “en uygun delil” (best evidence rule) (FRE Bölüm X) delillerin kabul edilebilirliğine yönelik oldukça ayrıntılı düzenlemeler getirmektedir³³⁴.

Özellikle Amerikan hukukuna göre delillerin kabul edilebilirliği hususunda ilgililik ve önemlilik kriterlerinin rolü büyüktür. Amerikan hukukunda ilgili delil (relevant evidence), iddia edilen husus veya vakıalarla ilgili yahut doğrudan onlarla bağlantısı olan ve bu husus veya vakıaları ispat edebilecek olan delillere denilmektedir. Önemli delil ise, davaya konu olayı esas olarak etkileyen delillere denilmektedir. Genel kabul edilebilirlik kuralına göre olay ile ilgili tüm deliller kabul edilebilirdir. Ancak bir delil, jüri üzerinde adil olmayan bir önyargı oluşturacaksa, o delilin ilavesi davaya konu olaydan başka yan konulara dikkat çekip ilgiyi dağıtacaksa, delil jüriyi yanlış yönlendirecekse, delil duruşmayı gereksiz yere uzatacaksa ve zaman kaybı yaratacaksa ve olayın taraflarından birisinin sunulan bir delil karşısında, bu delilin sunulacağını haklı gerekçelere dayanarak hiç tahmin etmemiş olmasından dolayı, haksızlığa ve zarara uğrayacak bir durumda bırakacaksa hakim deliller ilgili ve önemli de olsa onları kabul edilebilir bulmayacaktır.

Ancak bir delil;

- Jüri üzerinde adil olmayan bir önyargı oluşturacaksa,
- O delilin ilavesi davaya konu olaydan başka yan konulara dikkat çekip ilgiyi dağıtacaksa,
- Delil jüriyi yanlış yönlendirecekse,
- Delil duruşmayı gereksiz yere uzatacaksa ve zaman kaybı yaratacaksa
- Olayın taraflarından birisinin sunulan bir delil karşısında, bu delilin sunulacağını haklı gerekçelere dayanarak hiç tahmin etmemiş olmasından dolayı,

³³⁴ Göksu, **a.g.e.**, s. 105 vd.

haksızlığa ve zarara uğrayacak bir durumda kalacaksa, hakim deliller ilgili ve önemli de olsa onları kabul edilebilir bulmayabilecektir³³⁵.

Ancak delil teorileri hakkındaki hemen hemen her konuda olduğu gibi burada da bilimsel deliller hakkında çeşitli çekinceler belirtilmiştir. Bilimsel yollarla incelenen delillerin olayı ispat gücü çok yüksek olmasına karşın her zaman için ilgili ve kabul edilebilir bulunmaları doğru görülmemiştir. Bilimsel usullerle elde edilen delillerin de yukarıda açıklanan kabul edilebilirlik testlerine tabii tutulması gerektiği vurgulanmıştır³³⁶.

Amerikan hukukunda gündemde olan kabul edilebilirlik ve ilgililik tartışmaları İngiliz hukukunda da geçerlidir. İngiliz hukukundaki ifade şekli ile ancak dava konusu olay ile ilgili olan veriler delil olarak duruşmada temsil edilebilir³³⁷. Fakat bir delilin ilgili olması ile o delilin kabul edilebilir olması aynı şeyleri ifade etmez. İlgililik basit bir mantık yürütme kapsamında dava konusu uyumsuzluk ile ileri sürülen delil arasındaki bağıdır. Ancak kabul edilebilirlik hukuki bir tartıma konusu olup kabul edilebilirlik testi söz konusu delilin mevcut olay ile ilgili mantık bağı ve bu delilin duruşmada tartışılmasının faydalarını birleştiren bir değerlendirmeden ibarettir³³⁸.

İngiltere’de “bilirkişi tanıklığı” kategorisinde değerlendirilen dijital delillerin mahkemeye kabulünde hakim rolü büyük önem taşımaktadır. Yaptığı dijital incelemeyi açıklamak için mahkeme huzuruna çağırılan adli bilişim uzmanının açıkladığı bilimsel yaklaşımların somut olaya ne derece kanıt olabileceğine hakim karar vermektedir. Böylece adli bilişim uzmanının yaptığı bilimsel açıklamalar yargılamanın şekillenmesinde çok önemli bir rol oynamaktadır³³⁹.

Bir diğer önemli husus ise dijital delillerin tartışıldığı yargılamalarda yahut siber suçlara ilişkin yargılamalarda adli bilişim uzmanlarının yaptıkları incelemeleri aleni olarak inceleyebilmek için özel ekipmanlarla donatılmış mahkeme salonlarının gerekliliğidir. Zira uzmanlar tarafından incelenmiş ve yargılamanın geleceği için önem arz eden bu delillerin, delillerin aleniliği prensibi kapsamında herkes

³³⁵ John C. Klotter, **Criminal Evidence**, Cincinnati: Anderson Publishing Company, 1980, ss. 94-104.

³³⁶ **A.g.e.**, s. 104.

³³⁷ Adrian Zuckerman, **The Principle of Criminal Evidence**, Oxford: Oxford University Press, 1989, s.47 vd.

³³⁸ **A.g.e.**, s.51.

³³⁹ Ian Walden, **Computer Crimes and Digital Investigations**, Oxford: Oxford University Press, 2007, ss. 387-389.

tarafından anlaşılır bir şekilde tartışılması esastır. Bu elzem tartışmanın sıhhatli bir şekilde yapılabilmesi için mahkeme salonlarında gerekli teknolojik donanımların bulunması gerekmektedir³⁴⁰.

Bu bölümü sonlandırmadan önce yukarıda bahsettiğimiz hususları yinelemekte fayda vardır. Delillerin kabul edilebilirliği konusu Türk Ceza Muhakemesi açısından tartışılması gerekli olan bir konu değildir. Zira Türk Ceza Muhakemesi sisteminde delil serbestisi gereği her şey delil olabilecektir. Bizim hukuk sistemimizde sınırı delil yasakları çizmektedir. Ancak delillerin kabul edilebilirliği meselesi bu konuya özgü çeşitli hukuki testler getirilerek daha ziyade Anglo-Amerikan hukuk sistemlerinden tartışma konusu yapılmıştır. Çalışmamızda özellikle bu hususa değinip yabancı hukuk sistemlerinden örneklerle açıklamalar getirmemizdeki temel amaç ileride emsal olarak gösterilecek yabancı hukuk sistemlerine yönelik temel bilgileri incelemektir.

Ancak kendi hukuk sistemimiz açısından delillerin kabul edilebilirliği olmasa da CMK kapsamında düzenlenen Cumhuriyet Savcısının delilleri değerlendirme yetkisi bu açıdan karşılaştırılabilir bir düzenlemedir. CMK'nın 170. maddesinin 2. fıkrası uyarınca *“soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturunca; Cumhuriyet savcısı, bir iddianame düzenler.”* Cumhuriyet savcısı kamu davası açmakla görevlendirilmiş kişidir ve bu görevini de soruşturma evresi sonunda delilleri değerlendirerek, yeterli şüpheye ulaşıyorsa, iddianame düzenleyerek yerinde getirir. Belirttiğimiz üzere delillerin serbest değerlendirilmesini benimseyen hukuk sistemimizde bu kuralın sınırını delil yasakları çizmektedir. CMK 170 kapsamında, Cumhuriyet savcısı “delil” niteliği taşıyan ve hukuka uygun bulunan deliller bakımında kamu davası açılıp açılmamasına ilişkin yeterli şüpheyi tespit edecektir³⁴¹. Bu kapsamda öncelikle Cumhuriyet savcısı hukuka aykırı delil elde etmemekle yükümlüdür. Ayrıca hukuka aykırı olarak elde edilen delilleri de iddianame kapsamında değerlendirmemelidir. Netice itibarıyla hukuka aykırı delillere dayanarak hüküm oluşturulamayacağı üzere yine aynı şekilde hukuka aykırı delillere dayanarak iddianame

³⁴⁰ A.g.e., s. 388 vd.

³⁴¹ Hasan Tahsil Gökcan, “Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması”, **Ankara Barosu Dergisi**, Ankara, Ocak 2012, <http://www.ankarabarusu.org.tr/siteler/ankarabarusu/tekmakale/2012-1/2012-1-9.pdf> (Erişim 25 Nisan 2014), s. 199

hazırlanmamalıdır³⁴². Zira hakimin hükmünü dayandırabilmesi için delillerin ispat edecek nitelikte olması, hukuka uygun yollarla elde edilmiş olması, sağlam ve güvenilir olması ve müşterek olması gibi genel delil özelliklerini taşıması gerekmektedir³⁴³. Ceza Muhakemesi hukukumuzda Cumhuriyet savcısına bu anlamda dolaylı bir görev verildiği ve savcının iddianame düzenleyebilmek için delilleri önceden takdir edip hukuka uygunluk süzgecinden geçirdikten sonra iddianameyi düzenleyebileceğini kabul etmek isabetli bir tutum olacaktır³⁴⁴.

Dolayısıyla dijital deliller açısından Cumhuriyet savcısı öncelikle bu delillerin hukuka uygunluğunu incelemeli ve bu delillerin ne ölçüde ispata elverişli olduklarını tespit etmelidir. Dijital delillerin incelenmesi hususunda esas sorumlu kişi olan adli bilişim uzmanlarının ise bu konuda kısıtlı yetkileri olduğu kanaatindeyiz. Zira adli bilişim uzmanlarının görevleri elde edilen delilleri adli bilişim çerçevesinde incelemek ve bu incelemeyi bir rapor halinde sunmaktır. Ancak bu inceleme kapsamında herhangi bir hukuka aykırılığın olup olmadığının, delillin delil özelliğini ve ispat kuvvetini etkileyecek herhangi bir bulgunun olup olmadığının veya söz konusu delillerin suçun işlendiği hususunda yeterli şüphe oluşturup oluşturmadıklarının tespiti konusunda yetkili makam soruşturma esnasında Cumhuriyet savcılığı, kovuşturma esnasında ise mahkemedir.

B- Dijital Delillerin Doğrulanması ve Dijital Delillere İlişkin Hukuki Kurallar

Dijital delillerin doğrulanması konusu dijital delillere ilişkin en tartışmalı konulardan birini oluşturmaktadır. Zira dijital verilerin kendilerine özgü özellikleri ve kolay zarar görebilen, değiştirilebilen ve yok edilebilen yapıları sebebiyle doğrulanmaları son derece önemlidir. Dijital delillerin doğrulanamaması halinde delillin hukuka uygunluğu şüpheye düşebilecektir.

³⁴² **A.g.e.**, s. 199-200.

³⁴³ Ünver ve Hakeri (2. Cilt), **a.g.e.**, s. 105

³⁴⁴ Benzer bir yaklaşım için bkz. Fatih Birtok, “Cumhuriyet Savcısı’nın Delilleri ve Fiili Takdir Yetkisi”, **Prof. Dr. Nur Centel’e Armağan**, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 19, Sayı 2, İstanbul, 2013, s. 955 vd.

Dijital delillerin doğrulanmasına yönelik detaylı açıklamalara geçmeden önce “dijital delilleri doğrulanması” terimi ile ne kastedildiğini açıklamakta fayda vardır. Dijital delillerin doğrulanması delilin iddia edilen “şey” olup olmadığını ispat etmektir³⁴⁵. Doğrulama sadece dijital deliller bağlamında değil diğer deliller açısından da geçerli bir aşamayı oluşturur. Çağırılan bir tanığın iddia edilen kişi olup olmadığının tespiti, mahkemeye ibraz edilen bir fotoğraftaki kişilerin gerçekten iddia edilen kişiler olup olmaması ya da bir yazının bir kişiye ait olup olmadığının saptanması delillerin doğrulanması aşamasını oluşturur³⁴⁶.

Özellikle son yıllarda dijital delillere dayanarak sürdürülmekte olan birçok ceza yargılaması bulunmasına karşın maalesef henüz hukukumuzda, diğer bazı hukuk sistemlerine kıyasla, dijital delillerin doğruluğunu tayin etmeye ilişkin geliştirilmiş bir kurallar bütünü bulunmamaktadır. Türk Ceza Muhakemesi’nde dijital delillere ilişkin kurallar 134. madde kapsamında bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma başlığı altında toparlanmıştır. Çalışmamızın bu bölümünde öncelikle Türk Ceza Muhakemesinde dijital delillere ilişkin getirilen bilgisayar aramaları kapsamındaki düzenlemeler detaylı olarak incelenecektir. Ardından yabancı hukuk sistemlerinde bu husustaki düzenlemelerden örnekler ele alınacaktır ve son olarak bu konudaki uluslararası kurallardan bahsedilecektir.

1- Türk Ceza Muhakemesinde Dijital Deliller Kapsamında Bilgisayar Aramalarına İlişkin Kurallar

a- CMK 134. maddenin incelenmesi

Dijital delillerin muhakeme hukukuna etkisinin en detaylı örneklerini sergileyen İngiltere ve Amerika’ya kıyasla maalesef Türk hukuk sisteminde henüz bu konuda geliştirilmiş, yalnızca dijital verilerin delil değeri konusunda yol gösterecek bir kurallar bütünü bulunmamaktadır. Buna karşın tüm dünyada olduğu

³⁴⁵ Göksu, **a.g.e.**, s. 170.

³⁴⁶ Göksu, **a.g.e.**, s. 170.

gibi ülkemizde de yargısal süreçte dijital deliller sıkça karşımıza çıkmaya başlamıştır.

Dijital delillerin Türk Ceza Muhakemesi kapsamında ele alınmalarında CMK'nın "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma" başlıklı 134. maddesi büyük önem taşımaktadır. Ancak CMK dışında dijital deliller ve adli bilişim alanına ilişkin Adli ve Önleme Aramaları Yönetmeliği ve Suç Eşyası Yönetmeliği bu konuda incelenmesi gereken hukuki metinler arasında yer almaktadır.

21. 02. 2014 tarihli 6526 sayılı kanunun 11. maddesi ile değiştirilen CMK'nın 134. maddesinin son hali şu şekildedir:

Madde 134 - (1) *Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) 3. fıkra göre alınan bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(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 tarafından imza altına alınır.

Ceza Muhakemesi Kanunu'nda yer alan bu hüküm hangi şartlar altında bilgisayar incelemesine başvurulacağını belirttiği gibi aynı zamanda da bu incelemenin hangi kapsamda yapılacağına da değinmektedir.

134. maddenin ilk düzenlenme zamanındaki gerekçesine baktığımızda öncelikle ilk fıkra da vurgulanan “başka suretle delil elde etme” imkanının bulunmaması dikkati çekmektedir. Zira bu madde ile kanun koyucu bireye ait kişisel bilgiler üzerindeki hakkın kısıtlanmasını özel koşullara bağlamak istemiştir. Maddenin gerekçesinde açıklandığı üzere bilgisayar program ve kütüklerinde arama yapılması şu şartlara bağlanmıştır:

- 1. İki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve aygıta geçici olarak elkoyma yapılabilir.*
- 2. Bunun için, söz konusu işleme başvurulmasının zorunlu olması yani bunun bir "ultima ratio" çare oluşturması gereklidir.*
- 3. Bu husustaki kararın mutlaka hâkim tarafından ve gizli olarak verilmesi gerekir. Bu karar, soruşturma evresinde sulh ceza hâkimi tarafından gizli olarak verilecektir.*
- 4. Arama sonucu, suçla ilgili bilgi metin hâline getirilecektir.*
- 5. Bilgiler şifreye bağlanmış ise ve bu nedenle giriş yapılamıyorsa, çözümün yapılabilmesi için araç ve gereçlere, aygıta geçici olarak elkonulabilir. Çözümünden hemen sonra bilgisayardaki bilgilere zarar vermeden aygıtın ilgisine hemen geri verilmesi gerekir³⁴⁷.*

CMK'nın 134. maddesi kanunun konuyu düzenleyiş biçimine sadık kalınarak incelendiğinde şu sonuçlar ortaya çıkmaktadır. Öncelikle kanun, 134. maddenin ilk fıkrası ile bir suç soruşturmasının varlığını, somut delillere dayanan kuvvetli suç şüphesinin varlığını ve başka suretle delil elde edilemeyecek olmasını şart olarak aramış ve bilgisayar incelemelerinin Cumhuriyet Savcısının talebi ve hakimnin kararıyla yerine getirileceğini belirtmiştir.

Kanun bilgisayar aramalarını genel arama kurallarından ayırarak özel olarak

³⁴⁷ **CMK Madde Gerekçeleri**, www.ceza-bb.adalet.gov.tr/mevzuat/cmkmaddegerekce.doc, (Erişim Mayıs 2012).

düzenlemiştir. Bu konuda belirtmekte fayda vardır ki CMK'nın 134. maddesi bir elkoyma maddesi değil bir arama maddesidir³⁴⁸. Kanun bu madde ile verilerin örnek çıktılarının ve kopyalarının alınmasını öngörür, yani delil tespiti söz konusudur³⁴⁹.

Maddenin 1. fıkrası iki önemli şartı bünyesinde barındırır. 134. madde kapsamında bilgisayar aramasına başvurulabilmesi için somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde etme imkanının bulunmaması gerekir. Soruşturma aşamasında bu iki zor şartın bir arada aranması, kişisel verilerin de ihlal edilmesine sebep olabilen bilgisayar aramalarının başvurulacak en son tedbir olarak değerlendirilmesi için öngörülmüştür.

Uygulamadaki tartışmalı hususlar saklı kalmak üzere, yalnızca kanunun lafzı dikkate alınacak olursa kanun koyucu “başka suretle delil elde etme imkanının bulunmaması” halini ifade ederken suçun bilgisayarla işlenmiş olduğu durumlara işaret etmektedir. Zira bilgisayar aramasına başvurmak için başka suretle delil elde edebilme imkanının bulunmadığı tek durum suçun bilgisayar ile işlendiği durumlardır. Bu düzenlemenin amacı sınırlı olarak bilgisayar incelemesi yapılmasını sağlamak ve sadece bilgisayar ile işlenen suçlar bakımından bu tedbirin uygulama alanı bulmasını sağlamaktır. Bu kapsamda bilgisayarlarda arama yapılacak veriler de suçun konusunu oluşturan veriler olmalıdır.

Öte yandan maddenin başlığı ve ilk fıkrasında kullanılan ifadeler itibariyle 134. Madde kapsamında yapılacak bir arama yada el koyma işleminin sadece bilgisayarlar açısından mı geçerli olduğu da değinilmesi gereken bir husustur. Kanun lafzı itibariyle burada sadece bilgisayarlardan bahsetmiştir. Ancak günümüzce pek çok cihaz teknolojik olarak gelişmiş olması sebebiyle tıpkı bir bilgisayar gibi çalışmaktadır. Neticede çalışmamızın başlarında da belirttiğimiz gibi bir soruşturma kapsamında delil elde etmek için veriler incelemek gerekecektir ve bu veriler veri depolama özelliğine sahip olan her cihazda bulunabilir. Bu durum kanun kapsamında ele alınmamıştır. Gelişen teknoloji ile beraber yeni ihtiyaçlar doğuran uygulama bu anlamda CMK'nın 134. maddesi tarafından tam olarak

³⁴⁸ Yener Ünver, Hakan Hakeri, **Ceza Muhakemesi Hukuku 1. Cilt**, Ankara: Adalet Yayınevi, Mayıs 2013, s. 578.

³⁴⁹ **A.g.e.**, s. 578.

desteklenememektedir, mevzuat teknolojinin oldukça gerisinde kalmıştır³⁵⁰.

134. maddenin ikinci fıkrasında inceleme sırasında bilgisayar şifrelerinin çözülememesi sebebiyle verilere ulaşılamaması halinde bilgisayarlara el konulabileceğini öngörmektedir. Burada doğrudan bir el koyma zorunluluğu getirilmemiş işin gereği kapsamında el konulabileceğinin altı çizilmiştir. Ünver ve Hakeri bu noktada uygulamada karşılaşılan sorunlara değinerek önemli eleştiriler getirmişlerdir. Ünver ve Hakeri uygulamada bilgisayar aramaları sonucunda elkoymanın son derece pervasızca uygulandığını belirterek hukuki olarak kabul edilemeyecek gerekçelere dayanılarak menkul mala el koyar gibi davranmaktadırlar³⁵¹. Kanunun lafzı elkoymaya izin verebilecek bir düzenleme yapmıştı ve buradaki takdir yetkisi uygulama geniş bir şekilde kullanılmaktadır. Ancak uygulamada karşılaşılan bu sorun CMK'nın 134. maddesi ile koruma altına alınmaya çalışılan kişisel verilerin korunması amacını zedelemekte ve kanun maddesi amacından uzaklaşarak uygulanmaktadır.

134. maddenin ikinci fıkrasına yönelik bir diğer eleştiri de adli bilişim uzmanlarından gelmektedir. Berber'e göre adli bilişim kendi disipliner özelliklerinden dolayı bilgisayarlarda depolanan verilere ulaşmak için şifre gibi koruma yöntemleri kullanmamaktadır. Bu sebeple burada ifade edilen husus şifrelerin çözülememesi değil bilgisayar üzerindeki incelemelin uzun sürmesi olarak anlaşılmalıdır³⁵². Berber'in getirdiği haklı eleştiri kanun kapsamında kullanılan sözcüklerle ilgilidir. Bir adli bilişim incelemesinin sonucunda bilgisayar içerisindeki verilere er yada geç mutlaka ulaşıldığı düşünülürse 134. Maddenin 2. Fıkrası uyarınca şifre dolayısıyla bilgilere ulaşılamamasından değil, yalnızca bu incelemenin uzun sürmesinden bahsedilebilir. Ancak bu noktada belirtmekte fayda vardır ki kanun koyucunun bilgisayar incelemesinin uzun süreceği durumlara ilişkin elkoyma kararı verilebileceği yönünde bir düzenleme yapması temel insan haklarından biri olan özel hayatın dokunulmazlığı ve kişisel verilerin korunması ilkelerine taban tabana zıt sonuçlar doğurabilecektir.

³⁵⁰ Serap Keskin Kızıroğlu, Fulya Eroğlu, İlker Tepe, Hazırlık Kolokyumu Bölüm III Ceza Muhakemesi Türkiye Ulusal Grup Raporu, AIDP XIX. Dünya Kongresi, "Bilgi Toplumu ve Ceza Hukuku Hazırlık Kolokyumları", **Suç ve Ceza Ceza Hukuku Dergisi**, Ocak Şubat Mart 2013, Sayı 1, ss.75-100, s. 91.

³⁵¹ Ünver ve Hakeri (1. Cilt), **a.g.e.**, s. 580.

³⁵² Leyla Keser Berber, **Adli Bilişim, CMK 134 ve Düşündürdükleri**, <http://www.leylakeaser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html>, (Erişim Mayıs 2012)

134. maddenin ikinci fıkrasında belirtildiği üzere bilgisayarlarda bir şifre dolayısıyla bilgilere ulaşamaması halinde bilgisayarın tümüne el konulabilir. Şifrenin çözümü ve gerekli kopyaların alınmasından sonra bilgisayar gecikmeksizin iade edilir. Burada el koyma işlemine ilişkin yardımcı olacak iki ayrı kanuni düzenleme daha gündeme gelmektedir. Çalışmamızın bu bölümünün başında da belirttiğimiz gibi Suç Eşyası Yönetmeliği madde 9 ile Adli ve Önleme Aramaları Yönetmeliği madde 17, el koyma kararı kapsamında incelenecek kanuni düzenlemeleri oluşturmaktadır.

Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi, CMK 134. Maddede belirtilen hususları aynen tekrar etmektedir. Yönetmeliğin 17. maddesi yalnızca bütün verilerin yedeklenmesini düzenleyen 3. Fıkra ya bir cümle daha eklemiş ve bu işlemin bilgisayar ağları ve uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanabileceğini belirtmiştir. Ancak bir yönetmeliğin bir hakka ilişkin olarak kanunda öngörülenden daha geniş bir sınırlandırma getirmesi mümkün olamayacağından bu yönetmelik maddesinin uygulamasında kanunda öngörülen sınırların ötesine geçilmemesi gerekmektedir³⁵³. Suç Eşyası Yönetmeliği'nin 9. Maddesi ise bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşyaların bozulmalarını engelleyecek nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edileceğini belirtmiştir.

134. maddenin 3. fıkrası dijital deliller açısından son derece önemli bir düzenleme getirmektedir. Kanun bilgisayar ve bilgisayar kütüklerine elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklenmesinin yapılacağını belirtmiştir. Verilerin yedeklenmesi ve bundan sonra veriler üzerinde yapılacak incelemelerin yedeklenmiş suretleri üzerinde yapılması dijital delillerin dünyaca kabul edilen kurallarından biridir. Ancak Berber'e göre adli bilişimin özellikleri çerçevesinde yedekleme işleminin oldukça uzun sürmesi ve inceleme için bilgisayarların bulunduğu yere gelen görevlilerin kimi zaman yanlarında yeterli yazılımları taşımamaları sebebiyle el koyma anında yedekleme işleminin yapılması oldukça güç olmakta ve bilgisayarlar adli bilişim incelemesinin yapılacağı laboratuvarlara götürülmektedirler³⁵⁴. Berber'in getirmiş olduğu bu açıklama uygulamaya ilişkin sıkıntıları yansıtıyor olsa da kanaatimizce dijital delillerin güvenilirliğini sağlamak

³⁵³ Kızıroğlu, Eroğlu ve Tepe, **a.g.e.**, s. 94.

³⁵⁴ Berber (CMK 134), **a.g.e.**, (Erişim Mayıs 2012).

amacıyla olay yerinde yedekleme yapmak bir zorunluluk olarak algılanmalıdır. Yedekleme işlemlerinin uzun sürmesi mutlaka soruşturmanın süjesine rahatsızlık verecektir. Zira grup halinde polisler kişinin evinde/iş yerinde saatlerce incelemede bulunacaktır. Ancak kanaatimizce hukuki sürecin ilerleyen safhalarında güvenilirliği şüpheyeye düşen delillerle yargılanmaktansa en başta bu delillerin güvenilirliklerini sağlamaya yönelik adımlar atılmalıdır.

Maddenin 4. Fıkrasını eski haliyle ve yeni haliyle ayrı ayrı incelemek bilgisayar aramaları ile ilgili güncel sorunların kavranması açısından daha isabetli olacaktır. 6526 sayılı kanında bahsedilen değişiklikler olmadan önce maddenin 4. Fıkrasında yapılan yedeklemelerden talep halinde şüpheliye veya vekiline bir kopya verilebileceği belirtilmiştir. Şüpheli veya vekiline verilecek bu kopya talep şartına bağlanmıştır, polis re'sen yedeklemenin bir kopyasını vermek zorunda değildir. Ancak unutulmamalıdır ki şüpheli evinde veya işyerinde onlarca polis tarafından aramaya tabii tutulduğunda zaten bir şaşkınlık süreci geçirmektedir. Şüphelinin avukatı da bu talebi atlayabilir yahut şüphelinin avukatı bulunmayabilir. Üstelik burada söz konusu olan tarafların iddialarıyla bağlı oldukları bir özel hukuk süreci değil kamusal bir nitelik taşıyan ve sonuçlarının insan hayatı için çok daha ağır olabileceği bir ceza soruşturmasıdır³⁵⁵.

Ancak 6526 sayılı kanun ile yapılan değişiklikler kapsamında 4. Fıkra çerçevesinde artık 3. Fıkraya göre yapılan yedeklemelerden bir kopya da şüpheli veya vekiline verilerek bu husus tutanağa geçirilecektir. Kanaatimizce böyle bir durumda polise yedeklenen verilerden bir kopya verme yükümlülüğünün düzenlenmesi yerinde bir düzenleme olmuştur. Unutulmamalıdır ki dijital deliller hakkında polise getirilecek yükümlülükler kolluk kuvvetlerinin işini zorlaştıran külfetler olarak görülmemeli aksine polisin şeffaflığını arttıracak unsurlar olarak değerlendirilmelidir.

Son olarak 134. Maddenin 5. Fıkrasında belirtildiği üzere kopyalama işleminin yapılması için el koymaya gerek yoktur. Yetkililer verilerin hepsini ya da bir kısmını kopyalayıp kağıda yazdırıp ilgili tarafların imzası altında tutanağa kaydedebilirler. Berber bu hususta UYAP ağının adli makamlarda aktif olarak

³⁵⁵ Ünver ve Hakeri yedeklenen verilerin bir kopyasının şüpheliye verilmesine yönelik farklı bir eleştiri getirmektedir. Ünver ve Hakeri'ye göre bir hacker'a bu verilerin bir kopyasının verilmesi durumunda suçun işlenmesinin devam etmesinin söz konusu olabileceğini belirterek dikkatli olunması gerektiğinin altını çizmişlerdir. Bkz. Ünver ve Hakeri (1. Cilt), **A.g.e.**, s. 579.

kullanılmasını örnek göstererek dijital delillerin dijital ortamda da mahkemeye ibraz edilebileceğini belirtmektedir³⁵⁶. UYAP ağının tüm mahkemelerce kullanıldığı ve delillerin bu şekilde de aktarılabilmesi oldukça haklı ve çarpıcı bir noktadır. Ancak henüz dijital delillere ilişkin yeterli kurallara sahip olmamakla birlikte bu tür delillere ne kadar itibar edilebileceği hakkında uygulamada birçok sorunla karşılaşmaktadır. Bu sebeple ülkemizin sadece gelişmiş bölgelerini değil, tüm kesimlerini de dikkate alarak klasik delil görüşü çerçevesinde alınan kopyaların yazılı belge olarak ibraz edilmesinde kanaatimizce bir sıkıntı yoktur.

Son fıkraya ilişkin asıl altının çizilmesi gerek konu kopyalama işleminin yapılması için elkoymaya gerek görülmemesidir. Bu fıkra ile elkoymanın temel amaç olmadığı belirtilmiş ve verilerin tamamının veya bir kısmının elkoyma işlemi olmaksızın kopyasının alınabileceğine karar verilmiştir.

134. madde ile ilgili açıklamalara son vermeden önce belirtmekte fayda vardır ki kanun 134. maddenin uygulanma evresinin soruşturma olduğunu açıkça belirtmektedir. Kanun 134. maddenin 1. fıkrasında “bir suç dolayısıyla yapılan soruşturmada” diyerek söz konusu bu tedbire başvurmanın ancak soruşturmada söz konusu olabileceğini belirtmiştir. Bu şartlar altında kovuşturma evresinde bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine başvurulamayacaktır.

b- AİHM’nin bilgisayar aramalarına ilişkin kararları

CMK 134. madde kapsamında şüphelinin kullandığı yahut şüpheliye ait olan bilgisayarlar incelenebilir. Ancak eski tarihli 1412 sayılı Ceza Muhakemeleri Usulü Kanunu’nda bilgisayarlarda aramayı düzenleyen bir hüküm bulunmamakla birlikte aramaya ilişkin genel hükümler bu hususta da kullanılabilmekte idi. Ancak kanunun böyle bir hususu ayrı bir düzenlemeye tabii tutmasının amacı Avrupa İnsan Hakları Sözleşmesi’nin (AİHS) 8. maddesinde belirtilen “özel hayatın ve aile hayatının korunması” hakkının ihlal edilmesinin önlenmesidir.

Gelişen teknoloji ile birlikte bilgisayarlar sadece iş yerlerinde hesap amaçlı

³⁵⁶ Berber (CMK 134), **a.g.e.**, (Erişim Mayıs 2012).

kullanılan cihazlar olmaktan çıkmış hayatın her alanının bir parçası haline gelmişlerdir. Bu sebeple bilgisayarlar kişilerin özel notlarını ve kişisel bilgilerini içermektedirler. Öte yandan bazı durumlarda inceleme için bilgisayarlara elkonulması bilgisayar sahibinin işini ve hayatını olumsuz etkileyebilir. Özellikle avukatlık mesleği mensupları açısından bilgisayar incelemeleri AİHM tarafından hassasiyetle değerlendirilmiştir.

Craxi-İtalya kararında, İtalya Eski Başbakanı olan Craxi hakkında “temiz eller” operasyonu kapsamında bir soruşturma yürütülmüştür ve Craxi’nin evinde bulunan bilgisayarlardan elde edilmiş bir dosyaya el konulmuş ve sonra da mahkemeye sunulmuştur³⁵⁷. AİHM İtalya’nın 8. maddeyi ihlal ettiğine karar vermiş gerekçe olarak da elde edilen özel ve dava ile ilgili olmayan bilişim verisi ve telefon konuşmalarının duruşmada delil olarak okunması ve basına yayınlanması gösterilmiştir³⁵⁸.

Petri Sallinen ve Diğerleri- Finlandiya kararında, avukat bürosunda yapılan bir arama kapsamında AİHM öncelikle bilgisayarlarda arama yapılmasını ve elkonulmasını içerisinde e-postalar bulunduğu için özel hayatı ilgilendiren bir müdahale olarak kabul etmiştir³⁵⁹. Ardından bu müdahalenin hukuka uygun olup olmadığını tespit için iç hukukta var olan kurallar incelenmiştir. Ancak iç hukukta yer alan kuralların sözleşme standartlarına uygun olması gerektiği için, Mahkeme kanundaki tanımlamalarda “belirlilik kuralına” aykırılıklar olduğu ve Avrupa Konseyinin REC 200/21 Tavsiye Kararını dikkate alarak “avukat-müvekkil itimat ilişkisine” kanunda yer verilmediği ve yeterli yasal garantilerin olmadığını belirterek 8. maddenin ihlal edildiğine karar vermiştir³⁶⁰.

Bilgisayar incelemelerine ilişkin AİHM süre unsuru üzerinde durmuştur. *Smirnov-Rusya* kararında³⁶¹ Mahkeme bir avukatın bilgisayarının alınmasını ve uzun süre geri verilmemesini AİHS’ne aykırı olarak değerlendirmiştir. Mahkeme bu kararında bir avukatın uzun süre bilgisayarının geri verilmemesini mesleki gizliliğe tecavüz olarak değerlendirmiş ve bu durumun adaletin sağlanmasını olumsuz etkileyeceğinden sözleşmesinin 6. Maddesi ile korunan adil yargılanma hakkının da

³⁵⁷ Kunter, Yenisey ve Nuhoğlu, **a.g.e.**, s. 1111.

³⁵⁸ **A.g.e.**, s. 1111.

³⁵⁹ **A.g.e.**, s. 1113.

³⁶⁰ **A.g.e.**, s. 1113.

³⁶¹ Smirnov/ Rusya, 71362/01, 07.06.2007

zedelenebileceğinden bahsedilmiştir³⁶².

Bir diğer kararında ise AİHM yine avukat bürolarında yapılan incelemeleri işaret etmiştir. *GmbH-Avusturya* kararında³⁶³ Mahkeme avukat bürolarında yapılacak bilgisayar aramaları için gerekli şartlara değinmiştir. Mahkemeye göre özellikle hakim tarafından yerilen bir araştırma yapmak kararı ve yeterli suç şüphesinin bulunmasının altını çizmiştir³⁶⁴. Ayrıca yine bu araştırmanın avukatın bürosunda yapılıp kendisinin büroda bulunmaması durumunda araştırmanın bağımsız bir gözlemcinin nezinde yapılıp yapılmadığı avukatın susma hakkı kapsamında materyale el konulup konulmadığı Mahkemece belirleyici kriterler arasında sayılmıştır³⁶⁵. Elektronik olarak kaydedilen verilerle ilgili olarak keyfilik ve suiistimal eylemlerine ilişkin ulusal hukukta düzenlenmesi gereken koruma önlemlerinin AİHS madde 8/2 de getirilen temel hakkın kısıtlanabilmesi ölçülerine uygun olması gerektiği de belirtilen hususlar arasındadır³⁶⁶.

c- Bilgisayarlarda yapılan aramalar sonucu elde edilebilecek tesadüfi deliller

Çalışmamızın önceki kısımlarında da belirttiğimiz üzere bilgisayarlar gündelik hayatın ayrılmaz bir parçasını oluşturmaktadırlar ve kişiler hakkında şahsi birçok bilgiyi barındırırlar. Dolayısıyla bir suç soruşturması kapsamında yapılan bilgisayar araması sırasında başka bir suça ilişkin delillere ulaşmak mümkündür. Başka bir suç kapsamında soruşturma yürütülürken şüphelinin bilgisayarından çocuk pornosu görüntülerinin çıkması durumu bahsedilen tesadüfi delilleri açıklayıcı çarpıcı bir örnek oluşturabilir.

Tesadüfen elde edilen deliller daha ziyade doktrinde iletişimin denetlenmesini düzenleyen 135. madde kapsamında ele alınmıştır. Ancak tıpkı iletişimin denetlenmesi uygulamasında olduğu gibi bilgisayar aramalarında da tesadüfi delillere ulaşılabilir. Zira her iki koruma tedbiri de bireyin özel hayatına müdahale

³⁶² Ünver ve Hakeri (1. Cilt), **a.g.e.**, s. 579.

³⁶³ GmbH/ Avusturya, 74336/01, 16.10.2007.

³⁶⁴ Ünver ve Hakeri (1. Cilt), **a.g.e.**, s. 581.

³⁶⁵ **A.g.e.**, s. 581.

³⁶⁶ **A.g.e.**, s. 581.

etmektedir.

CMK'nın 138. maddesi tesadüfen ele geçirilen delilleri düzenler. Bu maddeye göre ;

(1) Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.

(2) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci Maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.

Kanun, bu düzenleme ile tesadüfi delilleri ikiye ayırmıştır. Eğer söz konusu tesadüfi delillere bir arama veya elkoyma tedbiri sırasında rastlanmışsa delil muhafaza altına alınıp derhal durum savcılığa bildirilecektir. Ancak söz konusu bu tesadüfi delil iletişimin denetlenmesi koruma tedbiri sırasında ortaya çıkarsa şüphelenilen suç ancak 135. maddede sayılan katalog suçlardan biri ise tesadüfen bulunan delil muhafaza altına alınarak Cumhuriyet savcılığına teslim edilecektir. Tesadüfen ele geçirilen bulgular katalogdaki suçlardan birine ait değilse derhal imha edilmelidirler.

Kanun iletişimin denetlenmesi koruma tedbirinin uygulanması gereken kuvvetli bir suç şüphesinin varlığını katalog suçlar belirleyerek somutlaştırmaya çalışmıştır. Ancak aynı durum bilgisayar incelemeleri için geçerli değildir. Her iki koruma tedbiri de özel hayatı korumayı amaçlıyor olsa da CMK 134 bu hususta çok yeterli kalamamaktadır. Ancak kanun lafzına sadık kalınarak yorumlanırsa, herhangi bir suç kataloğundan bahsetmeksizin, bilgisayar incelemeleri sırasında karşılaşılan tesadüfi delillerin muhafaza altına alınarak derhal Cumhuriyet Savcılığına ulaştırılması sonucuna ulaşılmaktadır.

d- CMK 134. madde kapsamında getirilen hukuki düzenlemeye aykırılık

Ceza Muhakemesi kapsamında değerlendirilen koruma tedbirleri içerisinde yer alan arama işleminin bilgisayarlar için özel düzenlemesi 134. maddede kendini göstermektedir. Çalışmamızın yukarıdaki bölümlerinde de belirttiğimiz üzere bilgisayarlar yalnızca bir kişinin işine ait belgeleri değil o kişinin tüm özel hayatına ilişkin bilgileri de içeriyor olabilirler ve kuralsızca gerçekleşen bilgisayar aramaları kişinin temel haklarından olan özel hayatın gizliliğini ihlal edebilir. Öte yandan bilgisayar aramalarında yönelik yapılan usulsüzlükler yalnızca insanların temel haklarını zedelemekle kalmayıp aynı zamanda da hukuki açıdan son derece hassas bir konu olan hukuka aykırı delillerin ortaya çıkmasına sebebiyet verecektir.

Çalışmamızın yukarıdaki bölümlerinde hukuka aykırı deliller kapsamında yer bulan tartışmalara değindiğimiz için bu bölüm dahilinde yalnızca 134. madde kapsamında karşılaşılabilecek hukuka aykırı deliller konusu tartışılacaktır.

CMK 134. madde bilgisayarlarda, bilgisayar kütüklerinde ve bilgisayar programlarında yapılan arama, kopyalama ve elkoyma işlemlerine ilişkin bir takım usul kuralları belirtmektedir. Madde hangi şartlar altında bilgisayar incelemesine başvurulabileceğini ve yine bu incelemenin nasıl yapılacağı konusundaki ana hatları çizmektedir.

134. madde arama üzerine getirilen bir özel normdur ve yalnızca bilgisayarlarda, bilgisayar kütüklerinde ve bilgisayar programlarında yapılacak arama, kopyalama ve elkoyma işlemini düzenler. Dolayısıyla, özel norm ve genel norm ilişkisi göz önünde bulundurularak, 116. maddeye göre yapılan bir aramada 134. maddenin izni yoksa bu arama kapsamında girilen yerdeki bilgisayarlar aranamayacaktır³⁶⁷.

Ceza muhakemesinde ispat sorunu kapsamında belirtilen delillerin temel özellikleri gereği deliller temsil edici olmalıdır. Delillerin temsil edici olabilmeleri için öncelikle güvenilir olmaları gerekir. Bir hukuk düzeninde güvenilir delil ancak hukuka uygun deliller açısından söz konusu olur. Bu kapsamda CMK 134 çerçevesinde belirtilen usullere riayet edilmeden elde edilen deliller delil olarak kabul edilmeyecek, delil yasakları gereğince yok hükmünde sayılacaktır.

³⁶⁷ Dülger, (2013), **a.g.e.**, s. 675

Öncelikle 134. madde kapsamında verilecek arama, kopyalama veya elkoyma kararı bir yargıç kararıdır. Cumhuriyet savcısının istemi üzerinde hakim kararı ile alınacak bir karardır. CMK 267. Madde uyarınca hakim kararlarına itiraz mümkündür. 6526 sayılı kanun kapsamında bazı koruma tedbirleri için karar alınacak makam olarak ağır ceza mahkemesi belirlenmiştir. Ancak 6526 sayılı kanun kapsamında 134. Maddede bu yönde bir değişiklik olmamıştır.

Öte yandan hukuk sistemimiz dahilinde dijital delillerin bütünlüğü ve güvenliğine ilişkin herhangi bir özel hüküm veya özel bir düzenleme bulunmamaktadır³⁶⁸. Bu tür deliller genel hükümlere tabidir ve bu durum gelişen teknoloji karşısında uygulanmanın sorun yaşamasına sebep olmakta, özellikle delil güvenliği açısından sorunlar yaratmaktadır³⁶⁹.

CMK 134. Maddede belirtilen usullere aykırılık kapsamında delil teorisi açısından hukuka aykırı deliller oluşacaktır. Çalışmamızın önceki bölümlerinde de belirttiğimiz üzere Türk Ceza Muhakemesi Hukukunda hukuka uygun yollarla elde edilmemiş olan bulgular, delil değildir³⁷⁰. Dolayısıyla şekle ilişkin usuli hataların basit hata olarak kabul edilmesi Anayasa'ya ve kanunlara aykırıdır³⁷¹.

Dijital delillerin güvenliği ve bütünlüğüne ilişkin bir ihlal yaşandığında ise Türk Ceza Kanunu (TCK) kapsamında düzenlenen bazı suçların oluşup oluşmadığı tartışılmalıdır. Somut olayın şartları kapsamında TCK 134. maddede düzenlenen özel hayatın gizliliğini ihlal, TCK 132. maddede düzenlenen haberleşmenin gizliliğini ihlal, TCK 243. madde kapsamında düzenlenen bilişim sistemine girme, yine TCK 244. Madde kapsamında düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçları söz konusu olabilecektir³⁷². Ayrıca dijital deliller güvenilirliği hakkında ortaya çıkacak sorunlar TCK 281. Maddesinde düzenlenen suç delillerini yok etmek, gizleme veya değiştirme suçu da oluşabilecektir³⁷³. Ancak delil güvenliğinin sağlanmasına ve denetlenmesi yönelik yeterli kurallar olmadığı için bu yönde bir suçun oluşup oluşmadığını tespit oldukça

³⁶⁸ Kızıroğlu, Eroğlu ve Tepe, **a.g.e.**, s. 91.

³⁶⁹ **A.g.e.**, s. 91.

³⁷⁰ Serap Keskin Kızıroğlu, Ceza Muhakemesi Hukukunda Delil ve İspat, **Güncel Hukuk**, Nisan 2014, ss. 25-27, s. 25.

³⁷¹ **A.g.e.**, s. 27.

³⁷² Kızıroğlu, Eroğlu, Tepe, **a.g.e.**, s. 91.

³⁷³ **A.g.e.**, s. 91.

zordur³⁷⁴.

2- Yabancı Hukuk Sistemlerinde Dijital Delillere İlişkin Kurallar

Amerika Birleşik Devletleri'nde yürürlükte olan Federal Delil Kuralları (Federal Rule of Evidence-FRE) genel olarak delillerin doğrulanması meselesini söz konusu delilin kabul edilebilmesi için gerekli bir aşama olarak düzenlenmektedir³⁷⁵. FRE delillerin doğrulanması konusunda dokuz farklı doğrulama metodu öngörmektedir. Böylece Amerikan yargılamasında delili öne süren taraf bu delilin doğruluğunu bu dokuz metoda dayanarak kanıtlamakta mükelleftir. Delili öne süren taraf FRE'de belirten metotlardan yalnızca biri veya birden fazlası ile bu yükümlülüğü yerine getirebilir, kanunda belirtilen sıralama bu anlamda sınırlı sayıda değildir³⁷⁶.

FRE kapsamında ele alınan doğrulama metotları çerçevesinde bir tanığın teşhis edilmesi, bir kişinin fiziki özelliklerinin tarif edilmesi, uzman incelemesi olmaksızın bir el yazısının tanınması gibi bir delilin ilk bakışta ispat etmek istenen “şey” olup olmadığını belirleyecek örnekler yer almaktadır. FRE kurallarına göre doğrulama delilin ispat kuvvetini etkilemez. Örneğin bir tanığın doğrulanması tanığın söylediklerinin de doğru olacağı anlamına gelmeyecektir.

Ancak FRE'nin getirdiği doğrulama kuralları dijital deliller konusunda yetersiz kalabilecek özelliktedir. Zira dijital delillerin doğrulanması teriminden anlamamız gereken basit ve yüzeysel bir doğrulamadan ziyade dijital delillerin herhangi bir değiştirmeye ya da zedelemeye uğramadıklarını saptamanın yanında kimi zaman mahkemenin akışını değiştirecek derecede önemli olan bu delillerin aidiyetini belirlemek olmalıdır.

İngiliz yargılamasında ise dijital delillerin ne tür işlemlere tabii tutulacağına ilişkin ACPO'nun yayınlamış olduğu Dijital Deliller için En İyi Uygulama

³⁷⁴ A.g.e., s. 91.

³⁷⁵ Steve Goode, “Admissibility of Electronic Evidence”, **The Review of Litigation**, Cilt 29, Sayı 1, Sonbahar 2009, ss.2-65, s. 8

³⁷⁶ Leah Voigt Romano, “VI. Electronic Evidence and the Federal Rules”, **Loyola Los Angeles Law Review**, Cilt 38, 2005, ss.1745 -1802.

Rehberinde belirtilen prensipler önem taşımaktadır. Bu rehberde dijital delillere ilişkin 4 temel prensip belirlenmiştir. Bu prensiplere göre;

- Hukuku uygulamaya yetkili kişiler daha sonra mahkemede aleyhlerinde iddialarda bulunulabilme tehlikesine dayanarak asla bir bilgisayardan veya depolama cihazından elde edilen veriyi değiştirmemelidir.
- İstisnai durumlarda, bir kişi bir bilgisayar ya da depolama cihazında bulunan orijinal veriye ulaşmayı gerekli gördüyse bu kimse mutlaka bu işlemi yapmaya yetkili biri olmalı ve yaptığı işlemin olası sonuçlarını ve olayla ilgisini açıklayacak kanıtlar sunabilmelidir.
- Bilgisayarla ilgili elektronik delillere uygulanan denetim yolu veya diğer süreçlerin tüm kayıtları oluşturulmalı ve korunmalıdır. Bağımsız bir üçüncü taraf bu süreçleri inceleyebilmeli ve aynı sonuca ulaşmalıdır.
- Soruşturmadan sorumlu olan kişi, hukuka ve bu prensiplere bağlı kalınacağına dair tamamen sorumludur³⁷⁷.

Bu prensipler İngiliz Emniyet Emirleri Derneğinin yayınlamış olduğu rehber kitapta vurgulandığı üzere kolluk görevlileri veya adli bilişim uzmanları gibi hukuku uygulamakla görevli kişilerin objektifliğini sağlamaya yöneliktir. Rehberin devamında ele geçirilen dijital cihazların çeşitliliğine göre elde edilen verilerin nasıl ve hangi teknik yollarla doğrulanabileceği üzerine teknik bilgiler de mevcuttur. İngiliz Emniyet Amirleri Derneği'nin yayınlamış olduğu bu rehberin hukuki bir bağlayıcılığı olmamakla birlikte artık İngiltere'deki uygulayıcılar tarafından tamamen kabul edilmiş ve riayet edilir prensipler haline gelmiştir³⁷⁸.

Fransız hukukunda ise dijital deliller hususunda daha ziyade delillerin serbest değerlendirilmesi ilkesine atıf yapılmaktadır. Fransız Ceza Muhakemesi Kanunu kapsamında madde 56'da dijital verilerin aranması, kopyalanması ve ele geçirilmesine ilişkin düzenlemeler mevcuttur. Fransız Ceza Muhakemesi Kanunu elkoyulan dijital verilerin envantere alınmasını ve şüphelinin önünde resmi mühürle mühürlenmesini hükmetmiş ve böylece güvenilirliğini sağlamayı amaçlamıştır. 56.

³⁷⁷ Association of Chief Police Officers, **Good Practice Guide for Computer-Based Electronic Evidence**, <http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf>, (Erişim tarihi Mart 2013).

³⁷⁸ Clifford May, "Computer-Based Evidence: The Identification and Recovery of Evidence in Electronic Format", **Computer Law & Security Report**, Cilt 16, Sayı 3, 2000, ss. 162-165, s. 163.

madde dijital verilere yalnızca gerçeğin ortaya çıkartılması amacıyla elkonulabileceğini belirtmektedir.

3- Dijital Delillere İlişkin Uluslararası Kurallar

Dijital deliller ve bu delillerin sıhhati hakkında uluslararası alanda da bir takım çalışmalar yapılmaktadır. Çalışmamızın yukarıdaki bölümlerinde de belirttiğimiz üzere IOCE (International Organization on Computer Evidence) bu çalışmaları yürüten kuruluşlardan birine örnektir. Bu organizasyon bir G8 Konferansı için bir takım standartlar önermiştir:

- Dijital delillere el konulduğunda, yapılacak işlemler delili değiştirmemelidir.
- Bir kişi için dijital delilin orijinal haline ulaşmak gerekli ise bu kişi mutlaka adli olarak yetki olmalıdır.
- Dijital delillere el koyulması, ulaşılması, depolanması ve aktarılmasına ilişkin tüm hareketler tamamen belgelenmeli, korunmalı ve incelemeye açık bulunmalıdır.
- Dijital delili elinde bulunduran kimse dijital delille ilgili yapılacak tüm işlemlerden sorumludur.
- Dijital delile el koyulması, ulaşılması, depolanması ve aktarılmasına dair sorumlu olan her görevli bu prensiplere uygun davranmakla mükelleftir³⁷⁹.

Söz konusu bu prensipler ACPO'nun yayınlamış olduğu prensiplerle büyük benzerlikler taşımaktadır. Bu metinde de temelde dikkat edilen mesele, dijital delilin incelemesini yapacak kişinin tüm sorumluluğu üstlendiği ve delile büyük özen göstermesi gerektiğidir. Dijital delillerin doğrulanabilmeleri ve güvenle hukuki süreçlere ışık tutabilmeleri için getirilmeye çalışılan tüm prensiplerde dijital delillerin tabii olduğu/olacağı süreçlerin hepsinin ayrıntılı olarak belgelenmesi gerektiği ve bu belgelerin de aleni olarak incelemeye açılması gerekliliğine vurgu yapılmaktadır³⁸⁰.

³⁷⁹ Peter Sommer, "Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness for Organizations", **Security Advisers and Lawyers, Information Assurance Advisory Council**, 3. Basım, Mart 2012, http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf, (Erişim Mayıs 2012), s. 43.

³⁸⁰ Belirtilen prensiplerin yanı sıra ISO tarafından geliştirilmiş olan bir takım standartlar da mevcuttur. Bu prensipler de diğerleri gibi dijital delillerin incelenme süreçlerine şeffaflık getirmek amacıyla

IOCE'nin belirtmiş olduğu bu standartlar 1999 yılında yapılan Uluslararası Yüksek Teknolojili Suçlar Konferansı'nda (International Hi-Tech Crime Conference) onaylanmıştır³⁸¹. Bu konferansın ardından 2001 yılında çıkartılan Avrupa Konseyi Siber Suçlar Sözleşmesi (Council of Europe Cyber Crime Convention), bir diğer adıyla Budapeşte Anlaşması dijital delillerle ilgili ilk bağlayıcı hukuki metin olma özelliğini taşımaktadır. Avrupa Konseyi bölgesel bir örgüt olmasına karşın bu sözleşme Konsey'e üye ülkelerin dışına ülkelere de destek görmüş ve kabul edilmiştir. Siber Suçlar Sözleşmesi bilgisayar ve teknolojik cihazların kullanımı ile işlenen suçlara ilişkin uluslararası bir mücadele anlayışı getirmektedir³⁸².

Siber Suçlar Sözleşmesiyle bağlantılı olarak Avrupa Konseyi 1995 yılında yayınladığı 95/13 sayılı tavsiye metni ve açıklayıcı genelgesi çerçevesinde dijital delillere dayanmaktadır. Tavsiye metnine göre; dijital delillerle ilgilenmek için delilin birliğini ve doğruluğunu temin eden ve yansıtan özel usul ve teknik metotların geliştirilmesi gerekmektedir. Belge delillerine ilişkin genel hukuki kurallar benzer olarak elektronik belgeler için de uygulanmalıdır. Açıklayıcı genelge ise saha ziyade elektronik belgelerin kağıt belgelerden farklı olduğuna dikkat çekmiş ve bu tür belgelerin okunabilmeleri için özel donanım ve yazılımların olması gerektiğine ve bu sebeple gözle fark etmenin mümkün olmayacağı tahriflerin mümkün olacağına dikkat çekmektedir³⁸³.

Dijital delillerin oldukça hassas yapıda olup çok çabuk değiştirilebilmeleri ve aidiyetlerinin (kimin tarafından oluşturulduklarının) saptanamaması gibi yargılama süreçlerinde kafalarda soru işareti doğurabilecek unsurların fazlalığı sebebiyle söz konusu bu delillerin incelenme usulleri ve doğrulanma sorununa dair bir takım kuralların getirilmesi elzemdir. Zira İngiltere'de ortaya çıkan ACPO prensipleri de öncelikle bu incelemelerden sorumlu kolluk görevlilerinin mesleki sorumluluklarını belirlemek amacıyla oluşturulmuştur. Bu tür kuralların varlığı ve daha da önemlisi

oluşturulmuştur. ISO'nun dijital delillere ilişkin prensipleri için bkz. **ISO Prensipleri**, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44381 ve ayrıca bkz. <http://www.iso27001security.com/html/27042.html>, (Erişim Mayıs 2012).

³⁸¹ Forensic Science Communications, **Digital Evidence: Standart and Principles**, <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>, (Erişim tarihi Mart 2013).

³⁸² Sommer, **a.g.e.**, s. 43vd.

³⁸³ Sommer, **a.g.e.**, s.44.

süreçlerin şeffaflığı sorumlu kişileri töhmet altında bırakmayacağı gibi yargılanan tarafların da güvenliğini temin edecektir.

C- Türk Ceza Muhakemesi Kapsamında Dijital Delillerin Değerlendirilmesi

1- Genel olarak

Dijital delillerin nasıl değerlendirileceği dijital delillerle ilgili en tartışmalı alanı oluşturmaktadır. Çalışmamızın başından beri vurguladığımız üzere dijital ürünler artık gündelik hayatın her alanına etki etmektedir. Böylesine hayatların içine dahil olmuş parçaları yok sayarak hukuki kararlar vermek çağın gerisinde kalmak olacaktır. Ancak sorun her zaman teknolojik gelişmelerden daha yavaş ilerleyen hukuk sistemlerinin dijital yollardan elde edilen delilleri nasıl kendi içlerine dahil edecekleri ve hukuki olarak nasıl değerlendirecekleridir.

Türk hukukunda dijital delillerin doğrulanmasına ilişkin kabul görmüş bir kurallar bütününe eksik olmasının yanı sıra dijital delillerin nasıl değerlendirileceğine yönelik de tutarlı bir bakış açısı bulmak zordur. Çalışmamızın bu bölümünde Türk Ceza Muhakemesi Hukukunda dijital delillerin değerlendirilmesi meselesi incelenecek olup öncelikle ceza muhakemesinden daha önce bu konuyu tartışmış olan hukuk muhakemesinin bakış açısı incelenecek ardından ceza muhakemesi kapsamında dijital delillerin değerlendirilmedi Yargıtay kararları ışığında incelenecektir.

2- Hukuk Muhakemesi Kapsamında dijital delillerin değerlendirilmesi

Türk Ceza Muhakemesi kapsamında dijital delillerin değerlendirilme sorununa değinmeden önce bu meselenin 6100 sayılı Hukuk Muhakemeleri Kanunu (HMK) kapsamında hukuk usulündeki çözümüne değinmekte fayda vardır. Elektronik imza kanununun uygulanmaya başlaması ile dijital belgeler üzerindeki tartışmalar HMK açısından bir nebze daha netleşmiştir.

HMK dijital delillerden bahsederken “elektronik” terimini kullanmayı tercih etmiştir. HMK’nın 199. maddesi elektronik verileri de içinde alarak belge kavramını düzenlemektedir. Maddeye göre: *“Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir.”*

HMK’nın 205. maddesi ise elektronik verilerin değerlendirilmesine ilişkin önemli bir hüküm içerir ve ikinci fıkrasında usulüne göre güvenli elektronik imza ile oluşturulan elektronik verileri senet hükmünde olarak kabul eder. Aynı kanun 210. maddesinde ise güvenli elektronik imzalı belgenin inkarını düzenleyerek güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulacağı hükmünü içerir.

HMK, CMK’ya kıyasla pek çok açıdan dijital verilere ilişkin önemli hükümleri barındırmaktadır. Ancak kanunda yer alan bu maddeler de bu konu üzerindeki tartışmaları tamamen sonuçlandırmamıştır. Zira dijital verilerin hemen her yerde insanın karşısına çıkması hukuki açıdan da meselenin çerçevesinin çizilmesini güçleştirmektedir. HMK güvenli elektronik imza ile oluşturulan verileri senet hükmünde kabul etmiştir. Ancak elektronik imza içermeyen dijital verilere ilişkin karışıklık hala devam etmektedir. Öte yandan yeni Ticaret Kanunu ile tüm şirketlere getirilen internet sitesi açma zorunluluğu kapsamında bu internet sitelerinden elde edilecek dijital verilerin delil değeri henüz kararlaştırılmamış hususlar arasındadır. Ancak çalışmamızın konusu Ceza Muhakemesi kapsamında dijital verilerin delil değeri olduğu için dijital verilerin HMK kapsamında nasıl ele alındığına kısaca değindikten sonra CMK kapsamındaki tartışmalara geri dönmek daha isabetli olacaktır.

3- Ceza Muhakemesi Kapsamında Dijital Delillerin Değerlendirilmesi

Türk Ceza Muhakemesi Hukuku kapsamında dijital deliller oldukça yeni bir tartışma konusunu oluşturmaktadır. Ancak dijital delillerden önce ses ve/veya görüntü tespit eden belgelerin delil olarak değerlendirilmesi meselesi ele alınmıştır.

Ses ve/veya görüntü tespit eden araçlardan elde edilen belgelerin de temel sorunu kolayca değiştirilebilir olmalarıdır. Ses ve/veya görüntü bantlarına ilişkin tartışmaların güncel olduğu dönemlerde bu tür belgelerin hükme esas alınmaması konusunda genel bir yaklaşım vardır³⁸⁴.

Usulüne uygun olarak muhafaza altına alınmış ve mahkemeye sunulmuş bulunan ses ve/veya görüntü bantların bir çeşit yazılı açıklama olarak kabul edildiği görülmektedir³⁸⁵. Yargıtay'ın ve Anayasa Mahkemesinin kararlarında ses ve/veya görüntü tespit eden kayıtların delil vasfının zayıf olduğunu belirten kararları bulunmaktadır. Yargıtay 9. CD.'sinin 5.10.1985 tarihli kararında “teyp bantlarının tek başına delil vasfını haiz olamayacağı” belirtilmiştir³⁸⁶. Yine Yargıtay görece daha yeni tarihli (22.2.2000) bir kararında “*teyp bantları, kaydedilen sözlerin kime ait olduğunun şüpheye yer bırakmayacak şekilde saptanmasının teknik olarak mümkün bulunmaması nedeniyle tek başlarına delil değeri taşımazlar*”³⁸⁷ ifadesiyle bu hususu açıkça belirtmiştir. Aynı kararın devamında ise “*Ancak, baştan beri ortaya konulan dosya kapsamında birlikte değerlendirildiğinde, söz konusu kayıttaki ifadelerin somut olayda diğer delillerle tam bir uyum içinde bulunması nedeniyle...*” ifadesini kullanarak bu tür belgelerin mutlaka diğer delillerle tespit edilmesi gerektiğini belirtmiştir.

Yargıtay'a ilişkin kararların yanı sıra aynı zamanda Anayasa Mahkemesi'nin de bu hususta verdiği kararlara ulaşmak mümkündür. Anayasa Mahkemesi 17-19.8.1971 tarihinde verdiği bir kararda, Cumhuriyet Senatosu üyesi bir siyasinin yasama dokunulmazlığının kaldırılmasına yönelik ses kaydı ile ilgili şu paragrafa yer vermiştir:

“Ses alma alanındaki ilerleme ve gelişmeler bugün o evrededir ki, bir sesin belirli bir kişiye ilişkin bulunduğunun hala parmak izlerinde olduğu gibi, kuşkusuzca ve kesinlikle saptanamamasına karşılık, birtakım montaj yollarıyla ve gerekirse ses taklit etmede usta kişilerin yardımlarından da yararlanarak bandlar istenildiği gibi doldurulabilmektedir. Bir toplantıda hazır bulunanlar, zamanında ve usulünce tutanaklarla saptanarak o toplantıya ilişkin bulunduğu ileri sürülen ses bantlarına böylece destek ve güç kazandırılmadıkça bant çevirilerine hukuk

³⁸⁴ Ayrıntılı bilgi için bkz Öztürk (Ses ve/veya Görüntü Kaydeden Araçlar), **a.g.e.**, s. 226.

³⁸⁵ **A.g.e.**, s. 226.

³⁸⁶ **A.g.e.**, s. 227.

³⁸⁷ Yargıtay 13. HD. E. 1999/9505, K. 2000/1439, www.kazanci.com, (Erişim tarihi Mart 2013)

yönünden tam bir güvenle bağlanıp dayanılamayacağı ortadadır.....Başka inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının ve gizli ajan raporlarının, bir yurttaşın yapılan ‘Türkiye Cumhuriyeti Anayasasını tağyir ve tedbile ve bu yasa ile kurulmuş Türkiye Büyük Millet Meclisi’ni iskata veya görevini yapmaktan men’e cebren teşebbüs gayesiyle gizlice ittifak kurmak’ gibi çok ağır bir isnada yasama dokunulmazlığının kaldırılması yönünden ciddilik kazandırılabilmesi bir hukuk devletinde düşünülemez”³⁸⁸.

Bu yargı kararlarından çıkarıldığı üzere usulüne uygun olarak muhafaza altına alınmış ve usulüne uygun bir şekilde mahkemeye delil olarak sunulmuş bulunan ses ve/veya görüntü bantları tek başlarına mahkumiyet kararı vermek için yeterli değildir, bunlar başka delillerle de desteklenmelidir³⁸⁹.

Ses ve/veya görüntü bantlarına yönelik bu çekinceler, yargı kararlarında da açıkça belirtildiği üzere, daha ziyade değiştirilebilmeleri üzerinedir. Bu tehlike bu tür belgeler üzerindeki güveni sarsmaktadır. Böylece ses ve/veya görüntü içeren bantlar bir olayla ilgili tek delil olarak bulunsalar bile mahkumiyet kararı için yeterli olmayacak başka delillerle destekleneceklerdir.

Çalışmamızın bu bölümünde ses ve/veya görüntü bantlarının Türk ceza muhakemesi kapsamında nasıl değerlendirildiğine geniş bir yer ayırmamızın sebebi çalışmamızın konusunu oluşturan dijital deliller konusuna en yakın örneğin ses ve/veya görüntü bantlarının oluşturmalarıdır. Henüz ceza hukuku kapsamında dijital deliller ile ilgili yeterli içtihadı bir gelişme olmamakla birlikte ses ve/veya görüntü kayıtlarına ilişkin yargı kararları ve akademik çalışmalar da çok daha eskiye dayanmaktadır.

Çalışmamızın da dikkatle altını çizdiği üzere günümüzdeki gelişmiş bilişim sistemleri artık ses ve/veya görüntü kayıtlarından çok daha karmaşık bir teknolojidir. Bu teknoloji içerisinde ele geçirilen deliller incelenerek pek çok mesele açıklığa kavuşturulabilecektir. Ancak hukuki anlamda buradaki asıl sorun bu incelemenin nasıl yapılacağı ve bu delillerin, tıpkı ses ve/veya görüntü kayıtlarında belirtilen çekincelerde olduğu gibi, değiştirilebilme ihtimalidir.

³⁸⁸ Öztürk (Ses ve/veya Görüntü Kaydeden Araçlar), **a.g.e.**, s. 227. Ayrıca bkz. Resmi Gazete, 15 Ocak 1972, s. 9.

³⁸⁹ **A.g.e.**, s. 232.

Bu doğrultuda dijital delillerle ilgili benzer çekinceler Yargıtay 11. Ceza Dairesi'nin bir kararında oldukça net ifade edilmiştir. E-posta yoluyla virüs gönderilerek bir şirketteki bilgisayarlara zarar verildiği iddiasıyla açılan davada dijital delillerin incelenmesi usulünde dikkat edilmesi gereken kurallara dikkat çeken emsal niteliğindeki bu kararda;

“- Virüs içeren bir e-posta veya e-postaların şikayetçinin bilgisayarlarına virüs bulaştırması sonucu doğacak zararın, şirketin gönderdiği e-postalar aracılığıyla başka adreslere virüs göndererek başka bilgisayarlara zarar vermesi ve kendi bilgisayarlarının sistem dosyalarını silerek çalışamaz duruma getirip iş ve zaman kaybına neden olması karşısında, virüslü veya virüssüz bir e-postayı gönderen bilgisayar bulmanın mümkün olduğunu,

- E-postayı gönderen bilgisayarın IP numarası, e-postayı gönderen sunucu bilgisayarın IP numarası, gönderici ve alıcı adreslerinin, e-posta almayı ve göndermeyi sağlayan e-postanın sunucu bilgisayarlarının tuttuğu günlük kayıtlarında saklandığını, servis sağlayıcı firmaların bir süre sonra bu kayıtların olduğu dosyaları silebildiğini, bu bilgilerin servis sağlayıcı firmalardan resmi yollarla istenilerek öğrenilebileceğini,

- E-posta sağlayıcı şirketin günlük (log) kayıtları mevcutsa gönderici e-posta adresini, e-postanın yazılıp yola çıkarıldığı ilk bilgisayarın IP numarasını ve IP numarasının sahibi servis sağlayıcı firmanın isminin bulanabileceğini, servis sağlayıcı firmadan da, günlük kayıtları mevcutsa verilen tarih ve saat için bu IP numarasının kullanıcısının öğrenilebileceğini,

- Şayet e-postanın yola çıkarıldığı sistemin IP numarası e-posta sağlayıcı şirketten öğrenilemezse ve e-postayı gönderen adres@yahoo.de olarak bulunursa Yahoo şirketinden; başka bir adres çıkarsa o e-posta adresini sağlayan servis sağlayıcıdan, bu adresi kullanan kişinin sistemde kayıtlı kimlik bilgileriyle, mevcutsa günlük kayıtlarından bu adres aracılığıyla e-posta gönderip almak için sisteme erişildiğindeki

tarih ve saatler ile erişilen IP numaralarının öğrenilebileceğini,

- Bu kullanıcı telefonla bağlanan bir ev kullanıcısı ise bağlanılan telefon numarasından kimliğinin kolaylıkla bulunabileceğini,

- Gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması ya da inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği,

- İncelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespiti yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değer (hash) belirlenmesi,

- Bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen IP adresinin bulunması (örneğin; şikayetçiye gelen e-postanın seçeneklerinden e-posta üst bilgisinin belirlenmesi ve bu üst bilginin uzman kişiler tarafından incelenmesi veya şikayetçiye gelen e-postanın göndericisinin ya da alıcısının e-posta sunucusunun sahibi şirkete belirtilen tarih ve saatte bahse konu e-postanın hangi IP adresinden gönderildiğinin sorulması,

- Daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin açık adres ve kimlik bilgilerinin talep edilmesi ve bulunan IP adresini kullanan

*abonenin sanıkla bağlantısının araştırılması gerektiği*³⁹⁰ hususları vurgulanmıştır.

Yargıtay'ın son dönemde medyada da tartışılan bu kararının ardından 9. Ceza Dairesinin 10 Eylül 2012'de verdiği başka bir karar dijital deliller hakkında dikkatleri çekmektedir. Yargıtay'ın 11. Ceza Dairesinin vermiş olduğu karar kapsamında dijital delillerin kendilerine özgü özellikleri sebebiyle ne derece dikkatle incelenmeleri gerektiği, bu dikkatli inceleme gözden kaçırılırsa hukuka aykırılık oluşacağı ve hukuka aykırı delillerin delil olarak kabul edilemeyecekleri belirtilen bu kararın satır aralarından anlaşılmaktadır. Ancak 9. Ceza Dairesi dijital delillere ilişkin verdiği kararla 11. Ceza Dairesinin dikkat çektiği hususlar üzerinde gereğince durmayarak açıkça dijital verileri delil olarak kabul ettiğini beyan etmiştir. Gerek incelemeye konu ilk derece mahkemesi kararında gerekse Yargıtay tarafından yapılan değerlendirmede bilgisayar verileri ile ilgisi olmayan suçun neredeyse günümüzde kalmadığını ve bilgisayar verilerinin özellikle örgütsel yapıdaki suçları aydınlatmakta kullanılabileceği belirtilmiştir. Yargıtay bu kararıyla dijital delillere dayanarak mahkumiyet hükmü kurmuş olan ilk derece mahkemesinin kararını onamakla birlikte aynı zamanda dijital verilerin delil olduğunu ve bu tür delillerin merkeze alınarak mahkumiyet hükmü kurulabileceğini de kabul etmiştir³⁹¹.

Yargıtay'ın yukarıda bahsettiğimiz söz konusu bu iki kararı incelendiğinde aslında kararların belirli bir tutarlılık göstermediği açıkça ortadadır. Özellikle ilk kararda dijital delillerin önemi belirtilirken bu delillerin kendilerine özgü yapıları sebebiyle tedbirli davranılması gerektiğinin altı çizilmiştir. Ancak belirtilen ikinci kararda ise doğrudan dijital delillerin birçok suç hakkında aydınlatıcı olabilme özelliğine vurgu yapılarak yine doğrudan mahkumiyete temel alınabilecek nitelikte deliller olarak kabul edilmesi gerektiği belirtilmiştir. Her iki kararda da dijital verilerin günümüz dünyasında en basit beşeri ilişkilerde dahi vazgeçilmez olduğu belirtilirken bir kararda bu vazgeçilmez verileri nasıl ve hangi usullerle değerlendirmek gerektiğinin altı çizilirken diğer kararda doğrudan aydınlatıcılık

³⁹⁰ “Dijital Delillere Yargıtay’dan İnce Ayar”, **Bilişim Hukuku Bülteni**, <http://www.bilisimhukuk.com/2010/01/dijital-delillere-yargitaydan-ince-ayar/>, 27 Ekim 2010, (Erişim 21 Mart 2013)

³⁹¹ Kadir Kökten, **Yargıtay’dan Balyoz Davasına Emsal Olacak Karar: Dijital Veri Delildir**, http://www.zaman.com.tr/gundem_yargitaydan-balyoz-davasina-emsal-olacak-karar-dijital-veri-delildir_2010157.html, 2 Kasım 2012, (Erişim tarihi Mart 2013).

özelliği üzerinde durularak bu tür kendilerine özgü özelliklere sahip delillerin nasıl inceleneceği ve nelere dikkat edileceği üzerinde durulmamıştır.

Sonuç itibariyle Yargıtay 11. Ceza Dairesi delillerin güvenilirliğinin altını çizirken 9. Ceza Dairesi dijital delillerin pek çok olay açısından aydınlatıcı olduğunun altını çizerek bu delillerin hukuki nitelikleri hakkında bir çıkarıma varmamıştır. Yargıtay'ın iki dairesi aynı mevzu hakkında iki farklı değerlendirme yaparak iki farklı sonuca ulaşmıştır. Temyiz Mahkemesinin her iki dairesinde de tartışılan dijital verilerin delil değerine göre verilen yargı kararları konusu, dijital deliller üzerinde hususi bir yönetmelik olmadığı için son derece önemlidir. Zira doktrinde sıkça tartışılan ancak tam olarak nasıl kabul edilecekleri net olarak kararlaştırılamamış dijital deliller hususunda Yargıtay'ın bu kararları gerek doktrine gerekse uygulamaya ışık tutacak öneme sahiptir. Ancak maalesef Yargıtay dairelerinden farklı zamanlarda çıkan ve mevcut karışıklığı daha da derinleştiren bu kararlar meseleyi aydınlatamamıştır.

Çalışmamızın bu bölümünde Yargıtay'ın temel görevlerinden bahsetmenin faydalı olacağı kanaatindeyiz. Bir hukuk devletinde kanunlar herkese eşit şekilde uygulanır. Bu durum Anayasa'nın 10. maddesi kapsamında kanun önünde eşitlik ilkesi ile teminat altına alınmıştır. Eşitlik ilkesinin bir görünümü kanunlar çerçevesinde herkese eşit davranmak olduğu gibi bir diğer görünümü ise aynı koşullar altında gerçekleşen durumların kanunlar çerçevesinde aynı sonuçları yaratması, bir başka deyişle kanunların uygulanmasında eşitliğin sağlanmasıdır. Kanunlar birincil olarak mahkemeler tarafından uygulanır. İlk derece mahkemelerinin kararları Yargıtay'ca incelenir, bu inceleme sırasında hem ilk derece mahkemesi kararlarının eksiklikleri gözden geçirilir hem de ülke çapında verilen kararın müşterek olabilmesine dikkat edilerek hukuk birliği, içtihat birliğini, sağlanmaya çalışılır. 2797 sayılı kanunla yetkileri ve usulleri belirlenen Yargıtay'ın bu görevleri ilgili kanunun ilk maddesinde belirtilmiştir. Yine aynı kanunun 45. maddesi içtihadı birleştirme usulünden bahseder. İçtihatların birleştirilmesi Yargıtay'ın dairelerinin verdikleri kararlar arasında bir uyumsuzluk olduğu durumlarda söz konusu olur. Yukarıda da belirtildiği gibi içtihat birliği ancak yüksek mahkeme kararları arasında bir ahenk söz konusu olduğunda mevcut olur, ki böylece

Yüksek Mahkeme kararlarının ahengi ilk derece mahkemesi kararlarına yansıyabilsin³⁹².

Yargıtay'ın ceza daireleri arasında içtihat uyuşmazlığı olduğu zaman Yargıtay Kanunu'nun 15. maddesinin 2. fıkrasının b bendine göre içtihatlar Ceza Genel Kurula iletilebilir. Ceza Daireleri arasındaki uyuşmazlıklar Ceza Genel Kurulunun görevine girecektir. Yargıtay Kanunu'nun 45. maddesinde ise bu işlemin usulü belirtilmektedir. Kanunun belirttiğine göre: “İçtihatların birleştirilmesini Birinci Başkan, doğrudan doğruya veya Yargıtay dairelerinin veya genel kurulların verdikleri karar sonucunda veya Yargıtay Cumhuriyet Başsavcısının bizzat yazı ile başvurması halinde, ilgili kuruldan ister. Bu istemlerin gerekçeli olması zorunludur.”

Kanunda belirtilen bu kişilerin talebi üzerine içtihatların birleştirileceği kararlaştırılmıştır. Ceza daireleri arasındaki bir uyuşmazlık halinde Ceza Genel Kurulu, Ceza Genel Kurulu kararlarının birbiriyle, Hukuk Genel Kuruluyla ya da diğer dairelerle uyumsuzluğu halinde ise Yargıtay Büyük Genel Kurulu içtihatların birleştirilmesinde görevli mercilerdir ve bu mercilerin verdikleri kararlarla ülke genelinde eşitlik ilkesi kapsamında hukuk birliği sağlanmış olur.

Yargıtay'ın içtihadı birleştirme görevi üzerinde verilmiş olan bu bilgiler dijital delillerin değerlendirilmesi sürecinde ülke çapında geçilen aşamaları daha iyi açıklamaktadır. Dijital delillerin henüz nasıl değerlendirilecekleri kesin değilken ve bu konuda Yasama henüz üzerine düşen görevi yerine getirmemişken Yargıtay'ın inisiyatif alarak bu konuda tüm ülke çapında akılları kurcalayan sorulara açıklık getirmesi önemli ve beklenen bir adım olarak değerlendirilmelidir.

Yargıtay son 10 yılda dijital delillerle ilgili birkaç karara imza atmıştır. Bu kararlar genelde dijital delillerin kabul edilebilirliği yönündedir. Genel yönelim dijital delillerin hükme esas teşkil edebileceği yönündedir. Ancak özellikle 11. Ceza Dairesi'nin verdiği karar bu noktada içtihat birliğinde uyumsuzluk yaratmaktadır.

Kanaatimizce Yargıtay, özellikle 9. Ceza Dairesi kararı ve 11. Ceza Dairesi kararlarının birbirleriyle bu denli zıt olmaları karşısında içtihadı birleştirme yoluna gitmeli idi. Zira Yargıtay'ın kararları dijital delillerin hükme esas alınabilmesi yönünde olsa da 11. Ceza Dairesi'nin vermiş olduğu bu karar emsal olmaya devam

³⁹² M. Kürşat Coşkun, “İçtihatların Birleştirilmesi”, **Ankara Barosu Dergisi**, <http://www.ankarabarusu.org.tr/Siteler/1944-2010/Dergiler/AnkaraBarosuDergisi/2001-1.pdf>, Ocak 2001, s. 94.

edecektir. Esasen burada önemli olan husus Yargıtay'ın dijital deliller gibi toplumsal olarak hassas ve tartışmalı bir konuda içtihadı birleştirme görevi ile dijital delillerin ceza muhakemesinde bulundukları yeri belirleyebilmesidir. Ancak Yargıtay kanaatimizce çelişkili kararlar vermiş olmakla birlikte dijital delillerin hükme esas alınması doğrultusunda verdiği kararlarda daha ziyade dijital verilerin somut olayları aydınlatma özelliği üzerinde durmuştur. Oysaki görevi hukuk birliğini sağlamak olan Yüksek Mahkeme bu hususta alacağı içtihadı birleştirme kararı ile gelecek dönemde çıkarılması elzem olan bir dijital deliller yönetmeliğine temel teşkil edecek ispat hukukuna ilişkin hayati hususları tartışmalı idi. Yargıtay'ın bu konuda aldığı farklı kararlar ve dijital delillere yönelik kullandığı beylik ifadeler kanaatimizce gelecek yıllara ışık tutamamaktadır.

Çalışmamızın bu kısmını tamamlamadan önce son aylarda sıkça tartışılan kararlardan birinde Yargıtay'ın altını çizdiği temel noktalara değinmekte fayda vardır. Yargıtay'ın 9 Ekim 2013 tarihli 2013/9119 Esas, 2013/12351 Karar sayılı kararında Yargıtay ceza muhakemesindeki delil serbestisi ilkesinden bahisle dijital delillerin de delil olarak kabul edilebileceklerini belirtmiştir. Daha önce verilen Yargıtay kararlarına atıflarda bulunularak Yargıtay'ın bu husustaki genel görüşü belirtilmiştir. Dijital delillerin değiştirilebilir olmalarının hükme esas alınamayacak olmalarına sebep olmadığını belirterek önceki içtihatlar örnek gösterilmiştir. Yargıtay delillerde sahtecilik iddiaları için ise bu iddiaların delillerin ele geçirilmesi aşamasından sonra olması gerektiğinin altını çizmiştir.

Yargıtay 10 Ekim 2013 tarihli kararında dijital delillerle ilgili önemli gibi görünen bilgileri içermesine rağmen aslında çalışmamızın başından beri ifade etmeye çalıştığımız dijital deliller konusundaki açığı kapatamamıştır. Yargıtay kamuoyunda tartışılan bir kararda dijital delillerle ilgili temel prensipleri tartışmamıştır. En kısa sürede belirlenmesi gereken dijital delillerle ilgili kurallara değinmemiştir. Sadece dijital delillerle ilgili genel geçer analizler yaparak dijital delillerin hükme esas teşkil edebileceğinden bahsetmiştir. Oysa burada altını çizmeye çalıştığımız husus dijital delillerin hükme esas teşkil edip edemeyecekleri değildir. Dijital delillerin hangi koşullar altında delil olarak kabul edilebilir oldukları ve dijital delillerin hukuki kararlarda şaibe yaratmadan nasıl kullanılabilecekleri üzerinde derin bir analiz yapılarak daha sonra bu delillerin hükme esas alınıp alınamayacağı tartışılmalı idi.

Sonuç olarak gerek Yargıtay'ın belirttiğimiz kararları gerekse ilk derece mahkemelerinin son dönemde aldığı kararlar çerçevesinde Türk Ceza Muhakemesinde dijital delillerin tek başlarına mahkumiyete temel alınacak kuvvette deliller olduğunu kabul eden görüşün hakimiyeti dikkati çekmektedir. Dijital delillerin dünya üzerinde farklı yargılama usullerince de artık kuvvetli deliller olarak kabul edildikleri gerçeği ortadadır. Ancak dijital deliller hakkındaki en önemli tartışma ne derece kuvvetli oldukları değil ne derece güvenilebilir oldukları yönündedir. Çalışmamızın yukarıdaki bölümlerinde de belirttiğimiz üzere kimi hukuk sistemlerinde öncelikle bu güveni sağlamak ve çok daha önemlisi, öncelikle dijital delillerle ilk aşamada muhatap olacak polis memurlarının meslek itibarını korumak için detaylı kurallar oluşturulmuştur. Bu aşamada Türk Ceza Muhakemesi'ndeki temel sıkıntı; dijital delillere yönelik bir takım kurallar geliştirilmeden doğrudan mahkumiyet gibi sonucu insan hakları açısından ağır olabilecek cezalara temel sayılmalarıdır. Üstelik uygulamada sıkça karşılaşıldığı üzere, CMK 134. maddesinde belirtilen yedekleme işlemi, incelemenin yedekleme üzerinden yapılması, ele geçirilen dijital verinin el koyma anından hash değerinin alınarak güvenliğinin sağlanması ve şüpheliye yapılan işlemde bir kopya verilmesi gibi dijital deliller açısından hayati öneme sahip aşamaların kimi zaman gereğince yerine getirilmemesi, muhakeme sırasından hukuka aykırılık iddialarına sebebiyet vermektedir.

V- Dijital Delillerin Değerlendirilmesi Konusunda Alınması Gereken Önlemler

Çalışmamız kapsamında belirttiğimiz üzere dijital delillerle ilgili Türk Ceza Muhakemesi hukukunda birçok sorun söz konusudur. Her şeyden önce bu tür verilerin delil değerinin ne olduğu hususunda ortak bir kanaat mevcut değildir. Henüz dijital delillerin delil olup olmadıkları dahi tartışılmaktadır. Dijital deliller aracılığıyla oluşturulan inceleme raporları muhakeme aşamasında kullanılmaktadır. Ancak henüz bu tür delillerin hangi delil türü dahilinde kabul edilecekleri kesin olarak belirlenmemiştir.

Teorik tartışmaları bir kenara bırakacak olursak, bu tür delillerin bütünlüğünün ve doğruluğunun sağlanacağı bir sistem henüz mevcut değildir. Söyle

ifade etmek gerekirse, dijital veriler üzerinde uygulanan birçok teknik sistem mevcuttur ve istenirse belli bir aşamaya kadar dijital veriler üzerinde yapılan değişiklikler olduğu gibi tespit edilebilir. Ancak hukuk sistemlerini ve vicdanları rahatsız eden, bu tespit aşamasına ilişkin kontrolün zayıf olmasıdır. Kişilerin bilgisayarlarının aranması kapsamında kopyalama işlemi bazen günler sürebilmekte ve kolluk kuvvetleri bilgisayarlara elkoyarak kopyalama işlemini kendi merkezlerinde yapabilmektedirler. Ancak şüphelinin yanlarında bulunmadığı o işlem sırasında akıllarda sorular oluşmakta ve bu delillere ne kadar güvenilebileceği tekrar sorgulanmaktadır.

Uygulamadan örneklere bakıldığında Yargıtay'ın verdiği kararlarda bir tutarlılık görülmemektedir. Yargıtay bir takım içtihatlarında dijital deliller konusunda uygulamayı temkinli olmaya davet ederken son dönem içtihatlarında bu tür verilerin çok sık kullanıldığını ve bu yüzden ispat gücünün yüksek olduğunu belirtmektedir. Türkiye’de yargı birliğini sağlamakla ve içtihadi bir ahenk yaratmakla mükellef, dolaylı da olsa doktrine yön veren Yargıtay, maalesef dijital delillerin değerlendirilmesine dair esasa ilişkin sorunları belirleyememiştir. Öte yandan hukuka aykırı deliller konusunda benimsemekte olduğu yeni görüş ile Yargıtay'ın usule aykırılıkları basit aykırılıklar olarak görmesi dijital deliller açısından oldukça şaibeli kararlara mahal vermektedir.

Belirtilen tüm bu sorunların çözümü bu verileri delil olarak kabul etmemek değildir. Fakat bu verilerin ancak ve ancak belirli koşullar çerçevesinde hukuka uygun delil olabileceği de unutulmamalıdır. İşte şu an hukuk sistemimizin yaşadığı bu hususa dair en büyük sorun, bu “belirli koşulların” ne olacağının bilinmemesi ve gerek uygulamanın gerekse doktrinin aslında kesin olarak uzlaşmamış ve bilinmeyen “belirli koşullar” üzerinden çıkarımlarda bulunmasıdır.

Bu şartlar altında en azından dijital deliller konusunda yaşanan sorunları hafifletebilmek için şu aşamada öncelikle bir dijital deliller yönetmeliğine ihtiyaç olduğu kesindir. Bu yönetmelik kapsamında yabancı hukuk sistemlerinde uygulanmakta olan rehberler dikkate alınabilir. Kanaatimizce özellikle hukuka aykırı deliller konusunda dikkatle incelenmekte olan Anglo-Amerikan hukuku yaklaşımı dijital deliller konusunda da takip edilmelidir. Böylece hukuka aykırılığı işlevsel olarak yorumladığı öne sürülen bu sistemin dijital deliller hususundaki temkinli

yaklaşımı kendi hukuk sistemimiz üzerinde bıraktığımız hasarı anlamamıza yardımcı olacaktır.

Hukuka aykırı deliller konusunda önceden belirlenmiş kurallar içermeyen ve her bir olayı kendi şartları çerçevesinde inceleyerek daha ziyade içtihatla ilerleyen Amerikan ve İngiliz hukuk sistemlerinde dijital deliller üzerine oluşturulan çalışma grupları uygulamacıları temkinli olmaya çağırmaktadır. Bu konuda ACPO'da belirlenen prensipler dikkate alınmalıdır. İngiliz Polisinin belirlediği bu prensipler kapsamında belirlenen hususlar şunlardır:

İlke 1: Kolluk kuvvetleri, bu teşkilatlar içinde çalışan şahıslar veya onların görevlileri/temsilcilerinin dahil olduğu hiçbir eylem, sonraki süreçlerde mahkemede kullanılabilecek herhangi bir veriyi değiştirmemelidir.

İlke 2: Bir şahsın orijinal veriye erişimi gerekli bulduğu koşullarda, o şahıs bu konuda yetkili (çevirmenin notu: ehil) olmalı ve aynı zamanda, eylemlerinin uygunluğunu ve etkilerini açıklayan kanıt sunabilmelidir.

İlke 3: Dijital delil üzerinde uygulanan her türlü işlemin sonradan takip edilmesini sağlayacak denetim geçmişi ve diğer kayıtlar yaratılmalı ve korunmalıdır.

İlke 4: Soruşturmayı yürüten şahıs, hukuka ve bu ilkelere bağlı kalınmasını sağlamada tam sorumluluğa sahiptir.

ACPO bu ilkeleri ortaya koyarak birlikte ortaya çıkartılan delilin doğruluğunu ve bütünlüğünü göstermek yükümlülüğü savcılığa vermiştir³⁹³.

Amerika Birleşik Devletleri'nde ise bir delilin kabul edilebilir olması için alakalı, temel, yeterli ve ispat gücünün önyargılı her etkiden daha fazla olması gerektiğinin altı çizilmektedir³⁹⁴. Amerika Birleşik Devletleri'nde dijital delillerin bilimsel geçerlilikleri yönünde herhangi bir test olmamasına rağmen 1993 yılında görülmüş bir dava alan Daubert kararında³⁹⁵ mahkeme şu hususların dikkate alınmasının önemini belirtmiştir.

³⁹³ Bkz, ACPO 2.2.2: Böylelikle belgelere dayanan delil doktrini açıklanabilir: üretilen kanıtın kolluk kuvvetlerince elde edildiği ana kıyasla daha fazla ya da daha eksik olmadığını mahkemeye göstermek savcılık makamının sorumluluğu altındadır.

³⁹⁴ Daniel J. Ryan ve Gal Shpantzer, **Legal Aspects of Digital Forensics**, <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf> (Erişim Nisan 2014), s. 2.

³⁹⁵ Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

- Bilim uzmanı tarafından uygulanan teori ve tekniklerin test edilip edilmediği,
- Bu teknik ve teorilerin yayınlanmış olup olmamaları ya da hakem gözetiminden geçip geçmemeleri,
- Uzman tarafından uygulanan tekniğin bilinen bir hata oranı olup olmadığı,
- Bu tekniklerin uygulamalarının standartlarla yönetiliyor olup olmamaları,
- Uzman tarafından uygulanan teori ve tekniklerin genel kabul görüp görmediği incelenecektir.

Temel kriterleri saptamanın güç olduğunu kabul eden Amerikan hukuku Federal Delil Kuralları ve mahkeme içtihatlarıyla bu konu üzerinde bazı ilkeler geliştirmeye çalışmaktadır.

Dünyadaki diğer hukuk sistemlerinde ele alınan bu kriterler kapsamında Türk hukukunda da bu nevi bir yönlendirme metnine ihtiyaç olduğu açıkça ortadadır. Kanaatimizce en kısa zamanda bu açık kapatılmalı ve dünyadaki diğer emsallerinde olduğu gibi bizde de yapılması gerekli olan bu rehber metinde dijital delillerin ispat kuvvetinden ziyade doğrulanması ve bütünlüğünün nasıl sağlanabileceğinin altı çizilmelidir. Zira Anayasa ve kanunlarda belirtildiği üzere hukuka uygunluğunda şüphe olan bulgular delil olarak kabul edilemez ve bu bulguların ispat kuvvetinden söz edilemez.

SONUÇ

Teknolojinin gelişmesi ile dijital cihazlar günlük hayatın hemen her aşamasında sıkça kullanılır hale gelmiştir. Bu yaygın kullanım hukuki uyumsuzlukların çözümünde de kendini göstermektedir. Günümüzde dijital cihazlardan elde edilen dijital veriler hukuki ve cezai sorunların aydınlatılmasında delil niteliğinde kullanılmaktadır.

Dijital verilerin delil olarak değerlendirilip değerlendirilmemesi konusunda hala doktrinde bir görüş birliği bulunmamakla birlikte bu nevi verileri tamamen yok saymak da çağın gerisinde kalınmasına sebep olacaktır. Ancak hukuk sisteminin bu tür verileri sıhhatli bir şekilde kullanabilmesi için bu verilerin ele geçirilmesi, incelenmesi ve sunulmasına ilişkin sıkı kurallara ihtiyaç duyulmaktadır. Zira aksi takdirde ceza muhakemesi açısından bu verilerden elde edilen delillerin hükme başlı başına esas alınması hakkaniyete aykırı sonuçlar doğuracak ve kamu vicdanının yaralayarak hukuk sistemine olan güveni zedeleyecektir.

Gelinen teknolojik standartlarda belki de önümüzdeki yıllarda dijital delillerin ceza muhakemesine entegrasyonu tıpkı parmakizi tespitlerindeki gibi muhakeme kurallarını tekrar düşündürücü büyük etkilere sebep olacaktır. Ancak bu aşamaya henüz gelinmemiş olmakla birlikte bu tür verilerin şu anki teknolojiye var olan hassas özellikleri dikkate alınarak mahkumiyete temel teşkil etmemeleri özellikle bizim gibi hukukun üstünlüğü sorunu yaşayan ülkelerde büyük önem taşımaktadır. Bu konuda üstlenilecek asıl sorumluluk pek tabii dijital verilerin incelenmesi hususunda getirilecek detaylı bir kurallar bütünü oluşturabilmek ve bu kuralların denetimini sağlayabilmektir. Ancak bu şeffaflık sağlanıp vicdanlar rahatlatılıncaya kadar kanaatimiz dijital delillerin tek başlarına mahkumiyet kararlarına temel oluşturmamaları; başka delillerle desteklenmek suretiyle yargılamaların sonuçlandırılmasıdır.

KAYNAKÇA

Akıncı Hatice, A. Emre Alıç, Cüneyd Er, “Türk Ceza Kanunu ve Bilişim Suçları”, **İnternet ve Hukuk**, Derleyen Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004.

Akyürek Güçlü, “Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu”, **Türkiye Barolar Birliği Dergisi**, Ankara: Şen Matbaa, Temmuz-Ağustos 2012, Sayı 101, ss. 61-83.

Arslan Mualla Buket Soygüt, “Avrupa İnsan Hakları Mahkemesi’nin Mialhe/Fransa Kararı”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, İstanbul Yıl: 8, Sayı 16, Güz 2009 s. 159-171.

Ashcroft John, Deborah J. Daniels, Sarah V. Hart, “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”, **U.S. Department of Justice, Office of Justice Programs**, National Institute of Justice, Nisan 2004.

Association of Chief Police Officers, **Good Practice Guide for Computer-Based Electronic Evidence**, <http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf>, (Erişim tarihi Mart 2013).

Association of Chief Police Officers, **Good Practice Guide for Digital Evidence**, <http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf>, (Erişim tarihi Mart 2013).

Balı Yunus, **Hash Değerinin Aynı Olmadığı Durumlar**, <http://www.dijitaldeliller.com/hash.html>, (Erişim Mayıs 2012)

Balı Yunus, **IP Numarası Tespiti**, http://www.dijitaldeliller.com/ip_tespiti.html, (Erişim tarihi Mayıs 1012)

Berber Leyla Keser, **Adli Bilişim, CMK 134 ve Düşündürdükleri**, <http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html>, (Erişim Mayıs 2012)

Berber Leyla Keser, Erdem Akyazılı, “Adli Bilişim”, **Bilişim Teknolojisi Hukuku Gündemi 2004-2005**, İstanbul: Bilişim Teknolojisi Uygulama ve Araştırma Merkezi, Ocak 2006.

Berber Leyla Keser , **Adli Bilişim (Computer Forensic)**, Ankara: Yetkin Yayınları, 2004.

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı, <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>, (Erişim Mart 2013).

Birtek Fatih, “Cumhuriyet Savcısı’nın Delilleri ve Fiili Takdir Yetkisi”, **Prof. Dr. Nur Centel’e Armağan**, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 19, Sayı 2, İstanbul, 2013.

Buckland Michael, "What is a 'document'?" **Journal of the American Society for Information Science**, Cilt 48, Sayı 9, Eylül 1997, ss. 804-809, <http://people.ischool.berkeley.edu/~buckland/digdoc.html>, (Erişim Mart 2013).

Calabresi Guido, "The Exclusionary Rule", **Harvard Journal of Law and Policy**, Cilt 26, Sayı 1, 2003, ss. 111-118.

Cameron Stuart, **Digital Evidence**, FBI Law Enforcement Bulletin, Ağustos, 2011.

Campbell-Kelly Martin , "Origin of Computing", **Scientific American**, Eylül 2009, Cilt 301, Sayı 3.

Carey Peter , **Data Protection A Practical Guide to UK and EU Law**, New York: Oxford University Press, 2009.

Casey Eoghan, **Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet**, London: Academic Press, 2004.

Casey Eoghan, Monique Ferraro, Lam Nguyen, "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence", **Journal of Forensic Sciences**, Cilt 54, Sayı 6, November 2009.

Central Processing Unit, <http://letisialinares.blogspot.com/2010/10/central-processing-unit-cpu.html>, (Erişim tarihi Mart 2013).

Çetin Erol ve İsmail Malkoç, **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara: Adalet Yayınevi, Mart 1995.

Çınar Ali Rıza, "Hukuka Aykırı Kanıtlar", **Türkiye Barolar Birliği Dergisi**, Sayı 55, 2004, <http://tbbdergisi.barobirlik.org.tr/m2004-55-83>, (Erişim 20 Nisan 2014), ss. 35-64.

Computer Forensics World, <http://www.computerforensicsworld.com/> , (Erişim Mart 2013)

Coşkun M. Kürşat, "İçtihatların Birleştirilmesi", **Ankara Barosu Dergisi**, <http://www.ankarabarusu.org.tr/Siteler/1944-2010/Dergiler/AnkaraBarosuDergisi/2001-1.pdf>, Ocak 2001.

Council of Europe, **Convention on Cybercrime**, <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> , (Erişim Mart 2013)

"Dijital Delillere Yargıtay'dan İnce Ayar", **Bilişim Hukuku Bülteni**, <http://www.bilisimhukuk.com/2010/01/dijital-delillere-yargitaydan-ince-ayar/>, 27 Ekim 2010, (Erişim 21 Mart 2013).

Dülger Murat Volkan , **Bilişim Suçları**, Ankara: Seçkin Yayıncılık, Kasım 2004.

Dülger Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, Ankara:Seçkin Yayıncılık, Kasım 2013.

Erem Faruk, **Diyalektik Açidan Ceza Yargılaması Hukuku**, Ankara: Işın Yayıncılık, 1986.

Erman Sahir , **Sahtekarlık Cürümleri**, İstanbul: Sulhi Garan Matbaası, 1970.

Ersoy Yüksel , “Genel Hukuki Korum Çerçevesinde Bilgisayar Suçları”, **Prof. Dr. Yılmaz Günel’a Armağan**, Ankara: Ankara Üniversitesi S.B.F. Dergisi, Cilt.49, No. 3-4, Haziran-Aralık 1994, s, 153 vd.

Feyzioğlu Metin, **Ceza Muhakemesinde Vicdani Kanaat**, Ankara: Yetkin Yayınları, 2002.

Forensic Science Communicatons, **Digital Evidence: Standart and Principles**, <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>, (Erişim tarihi Mart 2013).

Gökcan Hasan Tahsil, “Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması”, **Ankara Barosu Dergisi**, Ankara, Ocak 2012, <http://www.ankarabarusu.org.tr/siteler/ankarabarusu/tekmakale/2012-1/2012-1-9.pdf> (Erişim 25 Nisan 2014).

Göksu Mustafa , **Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde)**, Ankara: Adalet Yayınevi, Nisan 2011.

Goode Steve, “Admissibility of Electronic Evidence”, **The Review of Litigation**, Cilt 29, Sayı 1, Sonbahar 2009, ss.2-65.

Gündel Ahmet , **İçtihatlı-Açıklamalı Zimmet, Sahtecilik, Hırsızlık, Gasp, Dolandırıcılık, Emniyeti Suistimal Suçları**, Ankara: Seçkin Yayıncılık, Eylül 2002.

Hafıza Kartı Nedir?, <http://bilgipaylas.com/hafiza-karti-nedir.html>, (Erişim Mayıs 2012).

Hafızoğulları Zeki, Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar**, Ankara: Us-A Yayıncılık, Ağustos 2012.

Hayajneh Ahmad Mousa , Sami Hamdan AL-Rawashdeh, “Theorotical Approaches to Admitting Scientific Evidence in the Adversarial Legal System”, **European Journal of Scientific Research**, Cilt 41, Sayı 2, 2010.

Helvacıoğlu Aslı Deniz, “Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümlerin İncelenmesi”, **İnternet ve Hukuk**, Derleyen Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004.

IACIS, <https://www.iacis.com/>, (Erişim 21.08.2012)

Internet Crime Forum Paper, **Reform of the Computer Misuse Act 1990 (June 2003)**, <http://www.internetcrimeforum.org.uk>, (Erişim Mart 2013).

ISO**Prensipleri,**

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44381 ve ayrıca bkz. <http://www.iso27001security.com/html/27042.html>, (Erişim Mayıs 2012).

Karagülmez Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara: Seçkin Yayıncılık, Mayıs 2005.

Kaya-Türkiye Kararı, http://www.tohav.org/aihm/kaya_turkiye.pdf (Erişim tarihi Mayıs 2012)

Kaygısız Mustafa, **Kriminalistik Olay Yeri İnceleme: Suç Yeri ve Delil Güvenliği**, Ankara: Adalet Yayınevi, Ocak, 2010.

Ketizmen Muammer , **Türk Ceza Hukukunda Bilişim Suçları**, Ankara: Adalet Yayınevi, Ocak 2008.

Kişisel Verilerin Korunması Kanun Tasarısı ve madde gerekçeleri, <http://www.tbmm.gov.tr/d23/1/1-0576.pdf> , (Erişim Mart 2013).

Kızıroğlu Serap Keskin, Ceza Muhakemesi Hukukunda Delil ve İspat, **Güncel Hukuk**, Nisan 2014, ss. 25-27.

Kızıroğlu Serap Keskin, **Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık**, İstanbul: Alfa Basım Yayım Dağıtım, 1997.

Kızıroğlu Serap Keskin, “AİHM’de Hukuka Aykırı Deliller ve AİHM Schenk Örneği”, **18. Hukuk İhtisas Semineri, Özel Hayatın Korunması**, İstanbul: Emniyet Genel Müdürlüğü/Basımevi, Yayın No 7, 18-19-20 Ekim 2002, ss. 104-106.

Kızıroğlu Serap Keskin, Fulya Eroğlu, İlker Tepe, Hazırlık Kolokyumu Bölüm III Ceza Muhakemesi Türkiye Ulusal Grup Raporu, AIDP XIX. Dünya Kongresi, “Bilgi Toplumu ve Ceza Hukuku Hazırlık Kolokyumları”, **Suç ve Ceza Ceza Hukuku Dergisi**, Ocak Şubat Mart 2013, Sayı 1, ss.75-100.

Kızıllarslan Hakan, **Ceza Muhakemesi, Adli Tıp, Adli Bilimlerde Vücudun Muayenesi ve Örnek Alma, Doktrin ve Uygulama**, Ankara: Çetin Veb-Ofset A.Ş., Temmuz 2007.

Klotter John C., **Criminal Evidence**, Cincinnati: Anderson Publishing Company, 1980.

Kökten Kadir, **Yargıtay’dan Balyoz Davasına Emsal Olacak Karar: Dijital Veri Delildir**, http://www.zaman.com.tr/gundem_yargitaydan-balyoz-davasina-emsal-olacak-karar-dijital-veri-delildir_2010157.html, 2 Kasım 2012, (Erişim tarihi Mart 2013).

Kunter Nurullah, **Ceza Muhakemesi Hukuku**, İstanbul: Yaylacık Matbaası, 1989.

Kunter Nurullah, Feridun Yenisey, Ayşe Nuhoglu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, İstanbul: Beta Basım Yayım Dağıtım A.Ş., Ekim 2010.

Kurt Levent , **Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara: Seçkin Yayınevi, 2005.

Mahoney Michael S. , “The History of Computing in the History of Technology”, **Annals of History of Computing**, Cilt 10, Sayı 2, 1998, s. 113 vd.

Malkoç İsmail, **Açıklamalı İctihatlı Türk Ceza Kanunu**, Ankara: Turhan Kitabevi, 2001, s. 1256.

Malkoç İsmail, **Açıklamalı Yeni Türk Ceza Kanunu Özel Hükümler (170-345), II. Cilt**, Ankara: Malkoç Kitabevi, 2006.

Marshall Angus, **Digital Forensics: Digital Evidence in Criminal Investigation**, West Sussex: Wiley-Blackwell Print, 2008.

May Clifford, “Computer-Based Evidence: The Identification and Recovery of Evidence in Electronic Format”, **Computer Law & Security Report**, Cilt 16, Sayı 3, 2000, ss. 162-165.

Nur Centel, Hamide Zafer, **Ceza Muhakemesi Hukuku**, İstanbul: Beta Basım Yayım Dağıtım A.Ş., Ekim 2012.

Online Etymology Dictionary, <http://www.etymonline.com/> , (Erişim Mart 2013).

Özbek Veli Özer, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayınları, Ekim 2013.

Özdilek Ali Osman, **Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku**, İstanbul: Vedat Yayıncılık, Eylül 2006.

Özen Muharrem, Mustafa Özen, “Ceza Muhakemesi Hukukunda Delil Yasakları”, **Prof. Duygun Yarsuvat’a Armağan, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, İstanbul: Pasifik Ofset, Cilt 9, Sayı 2, 2012, s. 301-329.

Öztürk Bahri ve Mustafa Ruhan Erdem, **Uygulamalı Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayıncılık, Kasım 2008.

Öztürk Bahri, “Ses ve/veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukundaki Yeri”, **Prof. Dr. Seydullah Edis’e Armağan**, İzmir: Dokuz Eylül Üniversitesi, 2000, s. 219-233.

Öztürk Bahri, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin Saygılar, Esra Alan, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Ankara: Seçkin Yayıncılık, Ekim 2010.

Pollitt Mark M., “Digital Forensic”, **Forensic Science and Law: Investigative Application in Criminal, Civil and Family Justice**, Derleyen Cyril H. Wecht, John T. Rago, Derleme Koordinatörü Benjamin E. Wecht, CRS Press, Aralık 2005.

Romano Leah Voigt, “VI. Electronic Evidence and the Federal Rules”, **Loyola Los Angeles Law Review**, Cilt 38, 2005, ss.1745 -1802.

Ryan Daniel J., Gal Shpantzer, **Legal Aspects of Digital Forensics**, <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf> (Erişim Nisan 2014).

Sieber Ulrich, **Legal Aspects of Computer Related Crimes**, <http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf>, Ocak 1998, (Erişim tarihi Mart 2013)

Sommer Peter, “Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness for Organizations”, **Security Advisers and Lawyers, Information Assurance Advisory Council**, 3. Basım, Mart 2012, http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf , (Erişim Mayıs 2012).

Stephan Ileana, “Cybercrime”, **Curentul Juridic**, http://revcurentjur.ro/arhiva/attachments_201103/recjurid113_13F.pdf, (Erişim tarihi Mayıs 2012) ss. 115-120.

Taş-Türkiye Kararı, www.inhak-bb.adalet.gov.tr/aihm/karar/tas.doc (Erişim tarihi Mayıs 2012)

Taşkın Şaban Cankat, **Bilişim Suçları**, İstanbul: Beta Yayıncılık, Kasım 2008.

TCP/IP Protokolü, <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html> (Erişim Mayıs 2012)

Tezcan Durmuş ve Mustafa Ruhan Erdem, **Teorik ve Pratik Ceza Hukuku**, İzmir: Şafak Matbaacılık, 2002.

Tezcan Durmuş, Mustafa Ruhan Erdem, Oğuz Sancaktar, **Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye’nin İnsan Hakları Sorunu**, Ankara: Seçkin Yayıncılık, 2002.

Topaloğlu Mustafa, **Bilişim Hukuku**, Adana: Karahan Kitabevi, Mayıs 2005.

Toroslu Nevzat , **Ceza Hukuku Özel Kısım**, Ankara: Savaş Yayınları, Ekim 2008.

Toroslu Nevzat, “Hukuka Aykırı Deliller Sorunu”, **Prof. Dr. Hamide Topçuoğlu’na Armağan**, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayın No: 498, 1995, ss. 55-58.

Toroslu Nevzat, Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, Ankara: Savaş Yayınları, Eylül 2009.

Tosun Öztekin, **Türk Suç Muhakemesi Dersleri**, I. Cilt, İstanbul: İstanbul

Üniversitesi Yayınları, 1981.

Turhan Faruk, “Avrupa İnsan Hakları Mahkemesi (AİHM) Kararları ışığında Kişi Özgürlüğü ve Türkiye, Gözaltında Kayıplar, Hakim Önüne Çıkarma ve Gözaltı Süreleri”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Haziran-Aralık 2000, Cilt: IV, Sayı 1-2, s. 204-258, http://www.hukuk.gazi.edu.tr/editor/dergi/4_10.pdf (Erişim tarihi Mayıs 2012)

Turhan Faruk, **Ceza Muhakemesi Hukuku**, Ankara: Asil Yayınevi, 2006.

Türk Ceza Kanunu Gerekçesi, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim Mart 2013).

Türk Dil Kurumu, **Güncel Sözlük**, <http://www.tdk.org.tr>, (Erişim Mart 2013).

Ünver Yener, Hakan Hakeri, **Ceza Muhakemesi Hukuku 1. Cilt**, Ankara: Adalet Yayınevi, Mayıs 2013.

Ünver Yener, Hakan Hakeri, **Ceza Muhakemesi Hukuku 2. Cilt**, Ankara: Adalet Yayınevi, Mayıs 2013.

USB Bellekler, http://www.arage24.com/index.php?option=com_content&view=article&id=215:usd&catid=5:ueruen&Itemid=13, (Erişim tarihi Mayıs 2013)

Walden Ian , “Harmonizing Computer Crime Laws in Europe”, **European Journal of Crime, European Journal of Crime, Criminal Law and Criminal Justice**, Cilt 12, Sayı 4, 2004, ss.321–336.

Walden Ian, **Computer Crimes and Digital Investigations**, Oxford: Oxford University Press, 2007, ss. 387-389.

Webopedia Online IT Dictionary, <http://www.webopedia.com/TERM/S/software.html> , (Erişim Mart 2013).

Yarsuvat Duygun, **Ceza Muhakemesi Hukukunda Kanuna Aykırı Elde Edilen Delillerin Geçerliliği**, <http://www.yarsuvat-law.com.tr/articles/article2.pdf>, Haziran 2009.

Yazıcıoğlu Yılmaz , “Bilişim Suçları”, **Hukuki Perspektifler Dergisi**, Sayı 2, Sonbahar 2004, ss.142-146.

Yenidünya Caner ve Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, Nisan 2003.

Zuckerman Adrian, **The Principle of Criminal Evidence**, Oxford: Oxford University Press, 1989.

EKLER

Dijital Deliller İçin En İyi Uygulama Rehberi (İlgili Bölümlerin Tercümesi)

1. KISIM 1: REHBERİN UYGULANMASI

1.1. Bu rehberin ilkeleri okunurken ve uygulanırken, aksi belirtilmediği müddetçe, polis servisine yapılan her türlü atıfta, İskoçya Suç ve Narkotik Uygulama (SCDEA) ve Kuzey İrlanda Polis Servisi'ni de kapsamaktadır.

1.2. Bu rehber temel olarak dijital kanıtlarla ilgilenmekte olan Birleşik Krallık kolluk kuvvetleri için hazırlanmıştır. Bu kolluk kuvvetleri şunları içerebilir:

- Dijital delinin kurtarılması sebebiyle arama mahallindeki malzemeleri koruma, ele geçirme ve bu malzemelerin arama mahallinden taşınmasını sağlama, ve de suçun araştırılması için gerekli olan dijital bilgiyi saptamaya dahil olan şahıslar;
- Dijital delilin saptanması, sunulması ve saklanması süreçlerini planlayan ve yöneten soruşturmacılar;
- Ele geçirilen dijital delili kurtaran ve yeniden ortaya çıkartan (çevirmenin notu: çoğaltan) ve de bu işlevi yerine getirme ve mahkeme önünde faaliyetleri hakkında bilgi verebilme konusunda gerekli eğitimi olan şahıslar. Uygun eğitimi almamış ve ilkelere bağlı kalamayacak durumda olan şahıslar bu faaliyeti yerine getirmemelidir;
- Dijital delillerin kurtarılması, saptanması ve yorumlanmasında yardımcı olmaları istenebilecek şahısların seçilmesi ve yönetiminde görevli olan şahıslar.

1.3. Bu rehberin bir önceki versiyonunun yayımlanmasından bu yana, Adli Tıp Düzenleme Kurumu, Birleşik Krallık genelinde benimsenecek olan yeni taslak adli tıp Etik ve Uygulama Kuralları'nı yayımlamıştır. Adli bilişim alanında çalışan tüm uygulamacılar bu kurallarla bağlıdır.

2 – KISIM 2: DİJİTAL DELİLİN İLKELERİ

2.1. İLKELER

2.1.1. İlke 1: Kolluk kuvvetleri, bu teşkilatlar içinde çalışan şahıslar veya onların görevlileri/temsilcilerinin dahil olduğu hiçbir eylem, sonraki süreçlerde mahkemede kullanılabilecek herhangi bir veriyi değiştirmemelidir.

2.1.2. İlke 2: Bir şahsın orijinal veriye erişimi gerekli bulunduğu koşullarda, o şahıs bu konuda yetkili (çevirmenin notu: ehil) olmalı ve aynı zamanda, eylemlerinin uygunluğunu ve etkilerini açıklayan kanıt sunabilmelidir.

2.1.3. İlke 3: Dijital delil üzerinde uygulanan her türlü işlemin sonradan takip edilmesini sağlayacak denetim geçmişi ve diğer kayıtlar yaratılmalı ve korunmalıdır.

2.1.4. İlke 4: Soruşturmayı yürüten şahıs, hukuka ve bu ilkelere bağlı kalınmasını sağlamada tam sorumluluğa sahiptir.

2.2. İLKELERİN AÇIKLANMASI

2.2.1. Tüm dijital deliller, belgelere dayanan delilleri içeren mevzuata ve kanunlara tâbidir.

2.2.2. Böylelikle belgelere dayanan delil doktrini açıklanabilir: üretilen kanıtın kolluk kuvvetlerince elde edildiği ana kıyasla daha fazla ya da daha eksik olmadığını mahkemeye göstermek savcılık makamının sorumluluğu altındadır.

2.2.3. Bilgisayarların işletim sistemlerinin elektronik hafızalardan veri silmesi, bu hafızalara veri eklemesi ya da hafızalardaki veriyi değiştirilmesi vakalarıyla sık sık karşılaşmaktadır. Bu, kullanıcının verinin değiştirildiğini fark etmesinden bağımsız olarak otomatik olarak gerçekleşebilir.

2.2.4. Dijital delil ilkelerine bağlı kalmak için, cihazın mümkün olan her yerde uygulanabilir, orantılı ve uygun bir görüntüsü alınmalıdır. Bu, orijinal verinin, İlke 3'ün gerektirdiği şekilde korunmasını, ve üçüncü bir şahıs tarafından yeniden incelenip aynı sonuca ulaşılmasını sağlayacaktır.

2.2.5. Bu, cihazın fiziksel/mantıksal bir görüntüsü olabileceği gibi, kısmi ya da seçili veri içeren mantıksal bir dosya görüntüsü de olabilir (bu görüntü bir seçim önceliği/triaj işleminin sonucunda elde edilebilir). Bu yöntem benimsenirse, soruşturmacılar, gerekli olan tüm delilleri elde etmeyi amaçlamak doğrultusunda kendi profesyonel muhakemelerini kullanmalıdır.

2.2.6. Yerel olarak değil de, uzaktan, muhtemelen erişilemeyecek olan bir lokasyonda depolanan verileri kapsayan durumlarda bir görüntü elde etmek mümkün olmayabilir. Bu akılda tutulmak suretiyle, dijital delili tekrar ele geçirmeye ehil olan ve sonrasında da mahkeme önünde delil olarak sunmaya kabil olan şahıslar bu erişimi sağlamalıdır. Başka bir hükümetin yargı alanı sınırlarında bulunan bir delil elde edilmişse, tatbik edilebilir kanunlara gerekli önem gösterilmelidir.

2.2.7. Mahkemede nesnelliğinin yanı sıra, süreklilik ve delillerin bütünlüğünü göstermek esastır. Ayrıca delilin nasıl kurtarıldığını kanıtlamak, delilin elde edildiği her bir aşamayı tek tek göstermek yoluyla, gereklidir. Delil, üçüncü bir şahsın aynı işlemi tekrar yerine

getirebilmesini ve mahkemeye sunulanlarla aynı sonuçlara ulaşmasını sağlayacak bir şekilde korunmalıdır.

2.2.8. Burada vurgulanmalıdır ki bu ilkelerin uygulanması, dijital delillerin orantısal bir yaklaşımla incelenmesine engel oluşturmamaktadır. Dijital soruşturmanın yürütülmesi hakkında karar verenler, mevcut istihbaratı ve soruşturma kaynaklarını hesaba katarak, soruşturmanın odağı ve kapsamı hususlarında sık sık değerlendirmelerde bulunmalıdırlar.

2.2.9 Bu dört ilkenin uygulanmasında aynı zamanda şunlar da göz önünde bulundurulmalıdır:

- Adli Tıp Düzenleme Kurumu’nun Etik ve Uygulama Kuralları
- Ulusal Polis Faaliyetlerini Geliştirme Kurulu’sunun (NPİA) Adli Tıp 21 programı uyarınca sağlanan adli bilişim süreci ilerlemelerinin rehberliği. Dijital delillerin toplanması, incelenmesi ve rapor edilmesinde görevli olan şahıslar da bu rehberliğe başvurmalıdır.

3. KISIM 3: PLAN

3.1. Bu aynı zamanda şunları da içerir:

- NPİA Adli Tıp 21 HTCU Bilgisayar İnceleme Süreci, 2011
- SCDEA HTCU rehberliği

3.2. Dijital cihazların çoğalması ve dijital iletişim kanallarındaki gelişmeler, dijital delilin, artık hemen hemen her suçun bir parçası olduğu ya da potansiyel olarak parçası olabileceği anlamına gelmektedir.

3.3. Dijital delil birden fazla farklı lokasyonda bulunabilir:

- Yerel olarak, bir son kullanıcı cihazında – genelde bir kullanıcının bilgisayarı, mobil/akıllı telefon, uydu navigasyon sistemi, USB depolama aygıtı, ya da dijital kamerada;
- Uzaktaki açık bir kaynakta – örneğin sosyal ağ kurma amaçlı internet siteleri, tartışma forumlar ya da haber gruplarında;
- Uzaktaki özel bir kaynakta – bir internet Hizmet Sağlayıcısının kullanıcı aktivitesi kayıtlarında (log), bir mobil telefon şirketinin müşteri faturası kayıtlarında , bir kullanıcının elektronik posta hesabında, ve giderek benzer bir şekilde, bir kullanıcının uzaktan dosya depolama biriminde;
- Nakil halinde – örneğin mobil telefon metin mesajları, sesli mesajlar, elektronik postalar, ya da internet sohbetlerinde.

3.4. Bir suça ilişkin delillerin yukarıda bahsedilen lokasyonların birden fazlasında bulunması ihtimali oldukça yaygındır. Ancak delillere ulaşmak bazı lokasyonlarda diğerlerine göre daha kolay olabilir; bu nedenle delillerin elde edilmesi aşamasında kaynak kullanımına özen gösterilmelidir.

3.5. Örneğin, eğer iki mobil telefon numarası arasında iletişim olduğu tespit edilirse, en iyi yöntem, mobil telefonların adli tıp incelemesi yerine, servis sağlayıcısından arama verilerini talep etmek olacaktır. Arama verileri, yüksek ihtimalle, bir telefonun arama kayıtlarından daha kapsamlı olacaktır. Ayrıca, arama tarih ve saatleri daha güvenilir olacaktır ki bu mobil telefonların arama kayıtları aracılığıyla her zaman elde edilemeyecek bir veridir.

3.6. Ayrıca, nakil halindeki delilleri elde etmeye çalışan soruşturmacılar, Soruşturma Yetkileri Yasası Yönetmeliği'nin gerekliliklerini göz önünde bulundurmalı ve yetkili makamlardan izin almalıdır.

3.7. Yukarıdaki maddeler tutularak, soruşturmacıların dijital delillerin varlığını tespit edecek gerekli stratejileri geliştirmeleri ve soruşturmaları boyunca delilleri korumaları ve değerlendirmeleri önemlidir.

3.8. Soruşturmacılar, herhangi bir adli bilişim sürecinin soruşturmanın geneline katabileceği faydalara her zaman gereken önemi vermelidir. Bir adli bilişim stratejisi düşünüldüğünde orantısallık göz önünde bulundurulmalıdır; çünkü adli bilişim soruşturması için gerekli olan kısıtlı kaynakların uygun bir şekilde kullanıldığını güvence altına almak hedeflenmelidir.

4. KISIM 4: ELDE ETME

4.1. Bu aynı zamanda şunları ifade eder:

- Görüntü Kaydının Kurtarılması ve Dijital CCTV v2.0 Sistemlerinden Çalışan Kopyaların Üretilmesi
- Network adli bilişimi ve hassas veri toplama – Ek A
- İnternet sitelerini, forumları, ve blogları içeren suçlar – Ek B

4.2. FİZİKSEL OLAY YERİ

4.2.1. Bir olay yerinin incelenmesi sırasında ele geçirilebilecek, her biri soruşturma için önemli veriler içerebilecek, çok sayıda farklı türde dijital medya ve son kullanıcı cihazları vardır. Veriyi korumak ve en iyi kanıta ulaşmak için, bu maddelerin uygun bir şekilde elde edilmesi ve bu maddelerin adli tıp tarafından incelenecek her bir diğer maddeye davranıldığı gibi özenle davranılması gerekmektedir. Bu kısmın amacı, şahıslara, maddeleri elde etmeye yönelik hareketlerinin doğruluğu hususunda yardımcı olmaktır.

4.3. ELDE ETMEYE YÖNELİK ORANTISALLIK HUSUSLARI

4.3.1. Elde etmeye yönelik orantısallık hususları şunlardır:

- Elde etmeden önce, bir maddenin kanıt taşıyabileceğini düşünün/değerlendirin. Örneğin, bu bir aile bilgisayar mı, yoksa bir şüpheliye ait bir bilgisayar mı?

- Maddenin nerede bulunduğuna dair detayların kaydedildiğinden emin olun; bu ilerleyen aşamalarda hangi maddelere öncelik verilmesi gerektiğini belirleyebilir.
- Suçun ne zaman işlendiğini düşünün/değerlendirin; CCTV kayıtlarını elde ederken, neyi elde etmeniz gerektiğini, kameralara ve tarih/saate göre, daraltın. Kanıtı kaydeden, daha iyi bir konuma yerleştirilmiş başka bir sistem olup olmadığını kontrol edin.
- Bir şüphelinin üzerinde bulunan mobil telefonlarla (muhtemelen o anda kullanım halinde olan) bir çekmecede bulunan mobil telefonları (o anda kullanımda olmayabilir) birbirinden ayırın; çünkü bunlar için farklı inceleme aşamaları gerekli olabilir.
- Ayrıca, delillerin online olarak ya da bir internet hizmeti sağlayıcısının sistemlerine kaydedilebileceğini ve son kullanıcı cihazlarının sadece hizmet sağlayıcısından delilleri isterken gerekli olabileceğini göz önünde bulundurun. Öyleyse, sadece güncel kullanımda olan cihazları (örneğin internete bağlı olanlar) ele geçirmek en iyi yöntemdir.

4.3.2. Dijital cihazlar ve iletişim araçları, sadece orada oldukları için ele geçirilmemelidir. Soruşturmayı yürüten şahsın eşyayı oradan götürebilmek için geçerli dayanaklara ihtiyacı vardır ve eşyayı götürmek için hukuka uygun sebepler olmalıdır. PACE Yasama Nizamnamesi'nin arama hükümleri İngiltere, Galler ve Kuzey İrlanda'da dijital cihazları ve iletişim araçlarını da eşit bir şekilde kapsar.

4.3.3. Avrupa İnsan Hakları Sözleşmesi'nin uygulanmasına da gereken önem gösterilmelidir.

4.4. DİJİTAL DELİLLERİ ELE GEÇİRMEK ÜZERE OLAY YERİNE GİTMEDEN ÖNCEKİ SAFHA

4.4.1 Dijital cihazları müsadere etmekten ya da olay yerinde verileri ele geçirmekten sorumlu şahıslar şu hususları temin etmelidir:

- Yeterli malzemeyi yanlarında bulundurdıklarını (detaylı bilgi için İlk Müdahale Ekibi Rehberi'ne bakınız).
- Delillerin potansiyel kaynaklarını ve nerede neyin gerekli olabileceğini göz önünde bulundurdıklarını

4.4.2 Bir soruşturma, kullanıcı tarafından çekilen görüntülerin incelenmesi ihtimalini içeriyorsa, kameraların ve dijital fotoğraf çekebilen diğer cihazların müsadere edilmesi hususu değerlendirilmelidir. Örneğin, bir şüphelinin çocukların uygunsuz fotoğraflarını çektiği düşünüldüğü vakalarda, dijital fotoğraf çekebilen cihazların müsadere edilmesi, sadece bu cihazların depoladıkları veriler için değil, bu cihazları dijital metaveri (EXIF verileri) incelemesi yoluyla önceden elde edilmiş uygunsuz fotoğraflarla bağlantılandırmak için de kullanışlıdır.

4.4.3. Gereken durumlarda, bir kuvvetin Adli Bilişim Birimi'nin uzman görüşü önceden istenmelidir. Soruşturma hakkında yeterince bilgilendirildikleri takdirde, Adli Bilişim

Birimleri aranan delilleri muhtemelen hangi cihazların taşıyabileceği hakkında gerekli bilgiyi verebilirler.

4.5. OLAY YERİNE GİDERKEN

4.5.1 İlke 3'e uymak için, dijital delillere yönelik olarak girişilen her türlü hareketin kaydı tutulmalıdır; bu kayıt işlemi, malzemenin yerinin fotoğraf ya da diagramlarını, mevcut tüm şahıslar tarafından verilen tüm bilgileri, ve olay yerindeki her türlü fiili içerebilir.

4.5.2 Parçaların (öğelerin, maddelerin, çevirenin notu) müsadere edilmesi ile ilgili olarak detaylı bilgi için İlk Müdahale Ekibi Rehberi'ne başvurunuz. Ancak, olay yerine iştirak eden şahıslar şuna büyük bir özen göstermelidir; hala çalışmakta olan sistemler dikkatle ele alınmalıdır, çünkü bu cihazlar üzerinde yapılacak yanlış bir işlem, dijital verilerin istenmeyen değişikliklere sebep olabilir. Bu sistemler üzerinde sadece eğitimli personel tarafından işlem yapılmalıdır. Ayrıca, bu tip durumlarda delil niteliğinde olabilecek hassas veriler kaybolabilir.

4.6. ONLINE DELİLLERİN ELE GEÇİRİLMESİ

4.6.1. Bazı soruşturmalarda, dijital delillerin ele geçirilmesi fiziksel değil online bir lokasyon üzerinden olabilir. Bu tip delillerin korunması hakkında detaylı bilgi, 'İnternet sitelerini, forumları ve blogları içeren suçlar'da ve 'Network adli bilişimi ve hassas veriler'de bulunabilir.

4.6.2. Online deliller, kabaca, kamuya açık (örneğin forumun kullanıcı adı ve şifre gerektirmediği durumlarda, forum yazıları) ve özel (örneğin Facebook hesabı bilgisi) olarak ikiye ayrılır. Her ikisini de elde etmek için olanak olabilir (forum yazısının resmini çekmek ve sonradan da forumun sahibinden yazıyı paylaşan kullanıcının hesap bilgilerini istemek gibi). Soruşturmacılar kamuoyu açık veriye ulaşırken, parmak izlerinin klavyenin üzerinde kalması da dahil olmak üzere, doğabilecek potansiyel sorunların farkında olmalıdır. Bu sorunlar, bir internet sitesinin sahibini, kolluk kuvvetleriyle işbirliği yapma yoluna itebilir.

4.6.3. İlke 3 uyarınca, delilleri ele geçirmek için yapılan tüm fiillerin kaydı tutulmalıdır.

5. KISIM 5: ANALİZ

5.1. Bu aynı zamanda şunları ifade eder:

- NPIA Adli Bilişim 21 HTCU Bilgisayar İnceleme Süreci, 2011
- Adli Tıp Düzenleme Kurumu Etik ve Uygulama Kuralları
- Dijital Görüntüleme Usulü v2.1

5.2. Bir arama sonucunda müsadere edilmiş cihazlar genellikle Adli Bilişim Birimi kuvvetlerine teslim edilecektir. Dijital cihazlarda depolanan verilerin hacmi ve

karmaşıklığı sebebiyle, soruşturmacıların incelemesi için bir cihaz üzerinde bulunan tüm verilerin elde edilmesi ne mümkündür ne de arzu edilir. Bunun yerine, soruşturmanın sadece gerekli ve ilgili verilerin incelenmesi üzerine yönlendirilmesi için doğru adli bilişim stratejisi geliştirilmelidir.

5.3. Ulusal Polis Hizmetlerini Geliştirme Kuruluşu şu sıralarda, bilgisayarları ve mobil telefonları kapsayan dijital inceleme süreciyle ilgili gereken formüller üzerinde çalışmaktadır. Okuyucular, dijital incelemede en iyi uygulama konusunda daha detaylı bilgi edinmek için bu süreçlere başvurmalıdır. Diğer dijital inceleme süreçleri de aşağıda özetlendiği gibi aynı ilkelere bağlı kalmalıdır.

5.4. Soruşturmacı dijital incelemenin tabiatını ve amaçlarını uygun bir biçimde değerlendirmelidir. Soruşturmacı, inceleme sürecinin önceliklerini iyi belirlemelidir, çünkü başka bir yerde bulunan dijital delilleri korumak için kilit bilgiye ulaşmak gerekebilir. Bu, özellikle fazladan delilin, failin ve kurbanın bulunduğu durumlarla ilgilidir.

5.5. Adli Bilişim Birimlerine deliller teslim edilirken, soruşturmacılar özel gereklilikleri sağlamalıdır. Dijital verilerin her bir parçasını incelemek pratik olarak mümkün olmadığı için adli bilişim uygulamacısının eldeki verilerden gerekli herhangi bir dijital delile ulaşabilmesini sağlamak için gereken görevlendirilme yapılmalıdır.

5.6. Daha karmaşık ve uzun soluklu soruşturmalarda, dijital delillerin bir ön gözden geçirme/öncelik belirleme (traj) safhasına tabi tutulması (hangi triaj aracının seçildiğine bağlı olmaksızın), hem soruşturmacılara hem de uygulamacılara eldeki dijital delillerin tabiatı hakkında daha iyi bir anlayışa sahip olma imkanını sunacaktır. Adli bilişim stratejisi, soruşturmanın gidişatında, adli bilişim incelemesi (örneğin, bir suç ortağının olduğunun eposta yoluyla ortaya çıkması) ya da başka bir yerdeki soruşturma (örneğin bir görgü tanığının başka bir şahsın da olayla ilgili olduğunu iddia etmesi) sonucunda oluşabilecek değişiklikleri hesaba katmak üzere düzenli olarak gözden geçirilmelidir. Bu nedenle, soruşturmacıyla adli bilişim uygulamacısının soruşturmanın ilerleyişi hususunda düzenli olarak iletişim halinde olmaları gerekmektedir.

5.7. Eğer büyük bir miktarda verinin içinden ilk inceleme sonuçları gözden geçirilecekse, bu gözden geçirme işlemini en iyi kimin yapabileceği konusu ele alınmalıdır. Sıklıkla, bunu en iyi yapacak olan, dosya hakkında daha fazla bilgi sahibi olması sebebiyle, soruşturmacıdır. Kaynağına bağlı olarak, bu veriler şunları kapsayabilir:

- İnternet geçmişi kayıtları
- Epostalar
- Anlık mesajlaşma kayıtları
- Medya dosyaları (resim ve görüntüler)
- Metin belgeleri
- Elektronik çizelgeler
- CCTV
- Metin mesajları

5.8. Adli Bilişim Birimiyle işbirliği halinde olmak, inceleme altındaki hiçbir verinin yanlış anlaşılmasını temin edecektir. Örneğin, silinen dosyalardaki anahtar kelime vuruşlarını incelerken, vuruşun yerinin öneminin bir uygulamacı tarafından açıklanması gerekebilir.

5.9. Mobil telefon incelemelerinde, cihaz hakkındaki istihbarata ve soruşturmanın gerekliliklerine bağlı olarak, farklı seviyelerde bir inceleme gerekebilir. Örneğin bir çekmecede bulunan bir telefon, sadece gerektiğinde telefonun fatura bilgilerini istemek için, ya da telefonun şüpheliye ait olup olmadığını tespit etmek için incelenebilir (seviye 1). Yüksek seviye bir soruşturmadaki bir şüpheli tarafından düzenli olarak kullanıldığı bilinen bir telefon ise, silinen verilerin geri kazanılmasını ve imkan dahilinde hafıza çiplerinin çıkartılıp incelenmesini de içeren çok daha derin bir incelemeye tabi tutulur (seviye 4). Bu inceleme seviyeleri NPIA mobil telefon standart operasyon usullerinde belirtilmiştir.

5.10 DİJİTAL VERİLERİN YORUMLANMASI

5.10.1. Diğer adli delillerde olduğu gibi, yorumlanma süreci dijital verilerin delil değeri taşıdığını ortaya koymalıdır. Dijital verileri yorumlayan uygulamacıların işlerinin ehli olması gerektiği gibi kendilerine verilen görevi yerine getirebilmek için gereken eğitimlerden de geçmiş olmaları gerekmektedir.

5.10.2. Örneğin, bir bilgisayarda çocuklara ait uygunsuz görüntülerin bulunmuş olması, bilgisayarın sahibinin bu görüntülerin varlığından haberdar olması anlamına gelmediği için, tek başına delil değeri taşımaz. Adli bilişim uygulamacısı, bilgisayar sahibinin bu görüntülerin varlığından haberdar olduğu ihtimalini tespit etmek için başka dijital delillerin varlığına kanaat getirmelidir (son zamanda açılan dosyalar, arama terimleri, uygunsuz görüntüleri içeren dosya ya da klasörlerin isimleri, ya da bilgisayarın şifreli olup olmaması gibi).

5.10.3. Dijital delillerin kaynağını tespit etmek de adli bilişim uygulamacısının bir diğer ana görevidir. Adli bilişim uygulamacısı, bilgi ve becerilerini, sadece dijital delillerin varlığını tespit etmek için değil, aynı zamanda bu delillerin oraya nasıl geldiğini tespit etmek için de kullanmalıdır. Bu, tüm adli tıp/bilişim disiplinleri için geçerlidir; örneğin, sanığın olay yerindeki bir şişenin üzerinde parmak izlerinin bulunmasının, şişenin oraya başka bir şahıs tarafından getirilmiş olması ihtimali sebebiyle, sanığın suçu işlediğinin ortaya çıkartılması doğrultusunda hiçbir şekilde gösterge değildir. Gerekli olduğu yerde, kaynağı ortaya çıkaracak analizi yapmak ve böylece bulguların yanlış yorumlanmasını önlemek adli bilişim uygulamacısının sorumluluğudur.

5.10.4. Adli bilişim uygulamacısının görevi genellikle, soruşturmacıları ve savcılarını, dijital delillerin hem sınırları/kısıtlılıkları hem de konusunda güçlü yönleri konusunda bilgilendirmektir.

5.10.5. Dijital teknolojinin dinamik olduđu ve uygulamacıların bilgilerine bu gerçeğin sürekli meydan okuduđu unutulmamalıdır. Bir adli bilişim soruşturmasının tüm yönleri üzerinde uzman olmak mümkün değildir; bir adli bilişim uygulamacısı hem bilgisinin sınırlarının hem de hangi noktada daha ileri araştırmanın ya da uzman bilgisinin gerekli olduğunun farkında olmalıdır.

6. KISIM 6: SUNUM

6.1. Bu aynı zamanda şunları kapsar:

- NPIA Adli Bilişim 21 süreç haritaları;
- Açıklama rehberi, ek K.

6.2. Bir adli bilişim soruşturmasının sonuçlarının sunulması birkaç yolla yapılabilir:

- Vaka boyunca sözel olarak soruşturmacıya/resmi görevliye;
- Vakanın kapatılmasını bildiren bir açıklama ya da raporla;
- Şahit bilgisi gerekiyorsa mahkemede

6.3. Tüm bu durumlarda adli bilişim uygulamacıları tarafsız kalma sorumluluklarının farkında olmalıdır ve ayrıca dijital delillerin hem kapsamı hem de sınırları hakkında bilgilendirme yapmak zorundadır. Bu, dijital delillerin tabiatı sebebiyle, hukukçu olmayan şahıslar (sıradan şahıslar, çevirmenin notu) tarafından anlaşılmasının mümkün olamayabileceği ihtimali sebebiyle gereklidir.

6.4. SÖZLÜ GERİBİLDİRİM

6.4.1. Bir soruşturma süreci boyunca sözlü geribildirim verilmelidir. Bu, ortaya yeni deliller çıktıkça yeni tahkik/inceleme doğrultuları bulmasına yardımcı olacak, ve uygulamacının incelemeyi daha iyi yapabilmesi için en güncel bilgiyi edinmesini sağlayacaktır.

6.4.2. Bu iletişimin ileriki zamanlarda açıklanması ihtimali üzerine kaydedilmesi önemlidir. En doğru uygulama, sözlü iletişimi eposta iletişimin takip etmesi, ya da eş zamanlı not alımı yoluyla kaydedilmesidir.

6.5. AÇIKLAMALAR YA DA RAPORLAR

6.5.1. Açıklama ya da rapor bir soruşturmanın nihai ürünüdür; soruşturmayı ve kurtarılan verileri ana hatlarıyla belirtmelidir. İlk rapor görece daha kısa olabileceken, uygulamacı sonraki aşamalarda gerekli olması halinde tam bir rapor üretebilmelidir.

6.5.2. Rapor okuyucunun anlayabileceği bir dille yazılmalıdır; bu doğrultuda bir terimler sözlüğü eklenebilir, gerekli maddeleri açıklamak için diagramlar/ekran görüntüleri kullanılabilir, örnekler verilebilir. Ayrıca teknik bir jargon kullanılmamalıdır.

6.5.3. Belli maddeler/parçalar bir raporda yeniden basıldığında/yayımlandığında, temsiliin sahi olduğu temin edilmelidir. Örneğin, resimler ancak raporda belirtilmek suretiyle boyutları değiştirilerek basılabilir. Rapor dijital olarak basılıyorsa, yeniden basılan parçalar mümkün oldukça orijinal görüntüsünde basılmalıdır. Bu uygun değilse (örneğin, dosyanın daha kolay incelenebilme amacıyla daha genel bir formata dönüştürülmesi gerekiyorsa), raporda bu dosyanın dönüştürüldüğü belirtilmelidir. Parçanın orijinal şekliyle görülmesini sağlayacak şekilde tekrar yayımlanamaması halinde, örneğin bir internet sitesi orijinal haline erişim sağlandıktan uzun bir süre sonra kurtarılmışsa, bu da raporda açıkça belirtilmelidir.

6.5.4. Rapor ulaşılan sonuçların gücünü belirtmelidir. Ayrıca, her nerede bir fikir öne sürülüyorsa, bunun gerçeklerden farklı olduğu, bir fikir olduğu da belirtilmelidir. Bir ekspertiz sunulduğunda, uygulayıcı bu sonuca hangi gerçeklere dayanarak ve nasıl bu sonuca ulaştığını açıklamalıdır.

6.6 TANIK DELİLİ

6.6.1. Bir uygulayıcının, soruşturmanın gidişatının yanı sıra, usulünün sıhhati/geçerliliği ve kendi tecrübe ve becerileri konusunda da tanıklık yapması gerekmektedir.

6.6.2. Tanıklık yapma konusuna aşina olduklarını ve tanıklar olarak sorumluluklarının farkında olduklarını temin etmek adına adli bilişim uygulayıcılarına bilirkişi eğitimi verilmesi tavsiye edilir. Bir adli bilişim uygulayıcısı her zaman bilirkişi beyanında bulunmayacağı için, bilirkişi beyanıyla gerçek kanıt arasındaki farkı açıkça bilmelidir.

6.6.3. Tanıklık ederken, adli bilişim uygulayıcıları, yukarıda belirtildiği üzere, nerede gerçekleri ifade ettiklerini, nerede uzman görüşü bildirdiklerini belli etmelidir. Uygulayıcılar, bilirkişi beyanında bulunurken, sadece kendi uzmanlık alanlarına giren hususlarda beyanda bulunmaya dikkat etmeli, kendilerini kimin bilgilendirdiğine bakılmaksızın, sorumluluklarının mahkemeye olduğunu unutmamalıdır.

6.7. EŞ ZAMANLI NOTLAR:

6.7.1. Bu noktada şu tekrar edilmeye değerdir; her bir işlemin tam kaydı alınmalıdır. Bu kayıtlar gelecekte daha ileri aşamada bir incelemenin yapılmasına sebep olabilecek olan müdafî tarafa gösterilmelidir. Böyle bir ileri incelemenin önemli bir kısmı ilk incelemenin fiillerini ve sonuçlarını doğrulama üzerine olacaktır. Bu kayıtlar ayrıca inceleme altındaki vakanın kullanılmamış materyalleridir.



**ASSOCIATION OF
CHIEF POLICE OFFICERS**

ACPO Good Practice Guide for Digital Evidence

The Association of Chief Police Officers has agreed to this revised good practice guide being circulated to, and adopted by, Police Forces in England, Wales & Northern Ireland.

It is NOT PROTECTIVELY MARKED under the Government Protective Marking Scheme and it is disclosable under the Freedom of Information Act 2000.

ACPO © 2012

Document information

Protective marking	NOT PROTECTIVELY MARKED
Author	DAC Janet Williams QPM
Force/Organisation	Metropolitan Police Service
ACPO Business Area	Crime BA
Contact details	020 7230 6800
Review date	As required
Version	5.0

This good practice guide has been produced by the ACPO Crime Business Area and was originally approved by ACPO Cabinet in December 2007. The purpose of this document is to provide guidance not only to assist law enforcement but for all that assists in investigating cyber security incidents and crime. It will be updated according to legislative and policy changes and re-published as required.

Any queries relating to this document should be directed to either the author detailed above or the ACPO Programme Support Office on 020 7084 8958/8959.

Contents

Section		Page
	Introduction to the Guide	4
	Foreword	5
1	Application of Guide	6
2	The Principles of Digital Evidence	6
3	Plan	7
4	Capture	8
5	Analyse	10
6	Present	11
7	General	13

Appendix A	Network Forensic and Volatile Data Collection
Appendix B	Crimes involving Websites, Forums and Blogs
Appendix C	Crime Scenes
Appendix D	Developing a Digital Investigation Strategy
Appendix E	ACPO Workbook

INTRODUCTION TO THE GUIDE FOR DIGITAL EVIDENCE

It gives me great pleasure to introduce the 5th version of the ACPO Good Practice Guide for Digital Evidence. Much effort has been put in to ensure that the right information is available to practitioners and managers in the fight against cyber crime. I would like to thank all those who contributed to its creation for their efforts in drawing together their expert knowledge in tackling the criminal misuse of current and emerging technologies. The review board drew together people from academia, private and the public sector and has been an excellent example of collaborative working.

Since taking the UK policing lead for e-Crime in April 2008, I have overseen the creation of the Police Central e-Crime Unit. The team has grown from strength to strength through partnership working leading to the formation of a centre of excellence for cyber crime and the successful prosecution of cyber criminals. It is only through bringing together the expertise in policing across the UK, the capability and best practice within industry, support of Government and the Criminal Justice System that we will combat those responsible for cyber crime.

I am pleased that there has been recognition of a need to co-ordinate the UK response to cyber security issues through the establishment of the Office of Cyber Security and the Cyber Security Operations Centre. This approach will combine the various industries, law enforcement and agencies' hard work to corral them into a single effort to gather intelligence, enforcement capability and create the right framework of policy and doctrine to better enable us all to tackle the major issues identified.

This guide has changed from version 4, where it centred on computer based evidence; the new revision reflects digital based evidence and attempts to encompass the diversity of the digital world. As such this guide would not only assist law enforcement but the wider family that assists in investigating cyber security incidents. I commend all to read and make use of the knowledge and learning contained in this guide to provide us with the right tools to carry out our role.

Janet Williams QPM
Deputy Assistant Commissioner
Metropolitan Police Service
ACPO lead for the e-Crime Portfolio.

FOREWORD

It seems that whenever a review of ACPO guidance is carried out we are in the middle of technological changes that have vast impact on the work that is done within digital forensic units. It is a testament to the authors of the original four guiding principles for digital forensics that they still hold today, and one of the key early decisions of the review board was to keep those four principles, with only a slight change of wording to principle four.

We work in an area of constant change. There is a continuing need to re-evaluate and revise our capacities to perform our duties. There is a need to recover and analyse digital data that can now be found within the many devices that are within day to day use, and can supply vital evidence in all our investigations.

Hence a second key early decision was to change the title of the document to ACPO Good Practice Guide for Digital Evidence. This would hopefully encompass all aspects of digital evidence and remove the difficulty about trying to draw the line to what is or isn't a computer and thus falling within the remit of this guide.

It is important that people who work within the arena of digital forensics do not just concentrate on the technology, as essential as that is, but that the processes we use are fit for the purpose, and that skills and capacities within units reflect the demands that are made on them.

A prime example of this is the use of the word 'triage'. It has been a subject of much discussion within the forensic community. It should be noted that it does not mean a single triage tool rather it is a complete process where certain tools will play a part but are not the whole solution.

This guide is not intended to be an A-Z of digital forensics, or a specific "how to do" instruction manual. It should paint an overall picture and provides an underlying structure to what is required within Digital Forensic Units (DFUs). Therefore, the guide has been produced as a high-level document without the specific guidance included in previous versions, as this guidance is now available elsewhere. Where relevant, links to other guidance documents will be given.

In this document Digital Forensic Unit is used to cover any type of group that is actively involved in the processing of digital evidence.

1. SECTION 1 – APPLICATION OF GUIDE

- 1.1 When reading and applying the principles of this guide, any reference made to the police service also includes the Scottish Crime and Drugs Enforcement Agency (SCDEA) and the Police Service for Northern Ireland (PSNI) unless otherwise indicated.
- 1.2 This guide is primarily written for the guidance of UK law enforcement personnel who may deal with digital evidence. This will include:
 - Persons who are involved in the securing, seizing and transporting of equipment from search scenes with a view to recovering digital evidence, as well as in the identification of the digital information needed to investigate crime;
 - Investigators who plan and manage the identification, presentation and storage of digital evidence, and the use of that evidence;
 - Persons who recover and reproduce seized digital evidence and are trained to carry out the function and have relevant training to give evidence in court of their actions. **Persons who have not received appropriate training and are unable to comply with the principles should not carry out this category of activity;**
 - Persons who are involved in the selection and management of persons who may be required to assist in the recovery, identification and interpretation of digital evidence.
- 1.3 Since the previous version of the guide was published, the Forensic Science Regulator has published new draft Codes of Conduct and Practice covering forensic science throughout the UK. All practitioners working in the field of digital forensics must abide by these codes.

2. SECTION 2 – THE PRINCIPLES OF DIGITAL EVIDENCE

2.1 PRINCIPLES

- 2.1.1 **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- 2.1.2 **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- 2.1.3 **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- 2.1.4 **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

2.2 EXPLANATION OF THE PRINCIPLES

- 2.2.1 All digital evidence is subject to the same rules and laws that apply to documentary evidence.
- 2.2.2 The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement.
- 2.2.3 Operating systems and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

- 2.2.4 In order to comply with the principles of digital evidence, wherever practicable, proportionate and relevant an image should be made of the device. This will ensure that the original data is preserved, enabling an independent third party to re-examine it and achieve the same result, as required by principle 3.
- 2.2.5 This may be a physical / logical block image of the entire device, or a logical file image containing partial or selective data (which may be captured as a result of a triage process). Investigators should use their professional judgement to endeavour to capture all relevant evidence if this approach is adopted.
- 2.2.6 In cases dealing with data which is not stored locally but is stored at a remote, possibly inaccessible location it may not be possible to obtain an image. It may become necessary for the original data to be directly accessed to recover the data. With this in mind, it is essential that a person who is competent to retrieve the data and then able to give evidence to a court of law makes any such access. Due consideration must also be given to applicable legislation if data is retrieved which resides in another jurisdiction.
- 2.2.7 It is essential to display objectivity in a court of law, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.
- 2.2.8 It should be noted that the application of the principles does not preclude a proportionate approach to the examination of digital evidence. Those making decisions about the conduct of a digital investigation must often make judgements about the focus and scope of an investigation, taking into account available intelligence and investigative resources. This will often include a risk assessment based on technical and non-technical factors, for example the potential evidence which may be held by a particular type of device or the previous offending history of the suspect. Where this is done it should be transparent, decisions should be justifiable and the rationale recorded.
- 2.2.9 Application of the four principles will also be informed by:
- The Forensic Science Regulator's forthcoming Codes of Practice and Conduct;
 - The guidance around digital forensic process improvements developed by the National Policing Improvement Agency's Forensic 21 programme and those engaged in the collection, examination or reporting of digital evidence should also refer to that guidance.

3. SECTION 3 – PLAN

- 3.1 This also refers to the:
- The NPIA Forensic21 HTCU Computer Examination Process, 2011
 - The SCDEA HTCU Guidance.
- 3.2 The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.
- 3.3 Digital evidence can be found in a number of different locations:
- Locally on an end-user device – typically a user's computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;
 - On a remote resource that is public – for example websites used for social networking, discussion forums, and newsgroups;
 - On a remote resource that is private – an internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's webmail account, and increasingly common, a user's remote file storage;

- In transit – for example mobile phone text messages, or voice calls, emails, or internet chat.

- 3.4 It would be quite common for evidence of a crime to be in more than one of the locations mentioned above. However it might be much easier to obtain the evidence from one location rather than another; careful consideration should be given to the resources required to obtain the evidence.
- 3.5 For example, if evidence is required of contact between two mobile phone numbers, the best method would be to obtain call data from the Communication Service Providers via the force SPOC, rather than to request a forensic examination of the mobile phones. The call data is likely to be more comprehensive than call logs from a mobile phone and the times and dates can be relied upon, which is not necessarily the case with logs from a mobile phone.
- 3.6 In addition, investigators seeking to capture 'in transit' evidence must be aware of the implications under the Regulation of Investigatory Powers Act (RIPA) and the need to seek appropriate authorities for doing so. Further information is available from force SPOCs.
- 3.7 With the above in mind, it is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence throughout their investigation.
- 3.8 Due consideration should always be given by the investigators of the benefits to the overall investigation of conducting any digital forensic work. Proportionality should be assessed when a digital forensic strategy is being considered to ensure that limited resources for digital forensic investigation are directed appropriately.

4. SECTION 4 – CAPTURE

- 4.1 This also refers to:

- Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0;
- Network forensics and volatile data collection – Appendix A;
- Crimes involving websites, forums and blogs – Appendix B.

4.2 PHYSICAL CRIME SCENES

- 4.2.1 There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined. This section is intended to assist individuals to ensure their actions in relation to seizure are correct.

4.3 PROPORTIONALITY ISSUES RELATING TO SEIZURE

- 4.3.1 Proportionality issues relating to seizure are:

- Before seizing an item, consider whether the item is likely to hold evidence. For example, is this a family computer or a computer belonging to a suspect?
- Ensure that details of where the item was found are recorded, which could assist in prioritising items for examination at a later stage;
- Consider when the offence was committed; when seizing CCTV, give consideration to narrowing down what is seized, by camera and/or time period. Check whether another system may be better placed to record the evidence;

- Differentiate between mobile phones found on a suspect (likely to be in current use) and phones found in a drawer (may not be in current use), as different levels of examination may be possible for these;
- Also consider that evidence may be stored online, or on an internet service provider's systems and end-user devices may only be needed to obtain the details necessary to request this evidence from the service provider. If so, it is best to seize items in current usage, i.e. computers connected to the internet.

4.3.2 Digital devices and media should not be seized just because they are there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of PACE Legislation Codes of Practice equally apply to digital devices and media in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant.

4.3.3 Due regard should also be given to the application of the European Convention of Human Rights.

4.4 BEFORE ATTENDING A SCENE TO CAPTURE DIGITAL EVIDENCE

4.4.1 Persons responsible for the seizure of digital devices, or for on-scene capture of data, should ensure:

- They have the necessary equipment. (Refer to the First Responder's Guide for a detailed breakdown);
- They have considered potential sources of evidence and know what is likely to be relevant, where possible.

4.4.2 Where an investigation is likely to involve the examination of user-created digital images, consideration should be given to the question of seizing of cameras and other devices capable of taking digital photographs. For example, in cases where a suspect is believed to have taken indecent photographs of children, seizure of devices capable of taking digital photos could be useful not only for the data they store, but also to link these devices to previously identified indecent photographs by the examination of digital metadata (EXIF data).

4.4.3 Where necessary, specialist advice from a force's Digital Forensic Unit should be sought in advance. If given sufficient information about the investigation, DFUs will be able to advise on which items are most likely to provide the evidence sought.

4.5 WHEN ATTENDING A SCENE

4.5.1 To comply with principle 3, records must be kept of all actions taken in relation to digital evidence, which could include photographs/diagrams of equipment locations, details of any information provided by persons present, and records of any actions taken at the scene.

4.5.2 Refer to the First Responder's Guide for detailed guidance on seizure for individual items. However, persons attending a scene should be especially aware that **systems which are powered on (running) need to be handled with care**, as there is the potential to make unwanted changes to the evidence if these are not dealt with correctly. Such systems should only be accessed by appropriately trained personnel. In addition, volatile data of evidential value may be lost.

4.6 CAPTURING ONLINE EVIDENCE

4.6.1 In some investigations the capture of digital evidence may be from an online rather than a physical location. Detailed guidance on securing this evidence can be found in 'Crimes involving websites, forums and blogs' and 'Network forensics and volatile data'.

4.6.2 Online evidence can roughly be split into that which is publicly available (e.g. forum postings, where the forum does not require a login to view) and that which is private (e.g. Facebook account information). There may be scope to obtain both (e.g. by capturing the text of a forum posting and then requesting the account details of the user who made the posting from the forum owner).

Investigators should be aware of the potential issues when capturing publicly available data, including the 'footprints' which are left when accessing a site, these can alert a website owner to law enforcement interest.

- 4.6.3 Records should be kept of all actions taken when capturing online evidence in order to comply with principle 3.

5. SECTION 5 – ANALYSE

- 5.1 This also refers to:

- The NPfA Forensics21 HTCU Computer Examination Process, 2011;
- Forensic Science Regulator's Codes of Practice and Conduct;
- Digital Imaging Procedure v2.1.

- 5.2 Devices seized as part of a search will typically be submitted to the force Digital Forensic Unit in accordance with force policy. Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data held on a device for review by investigators. Instead, a forensic strategy needs to be formulated to enable the examination to be focused on the relevant data.

- 5.3 The National Policing Improvement Agency is currently formulating suggested processes for digital examinations involving computer and phone devices. Readers should refer to these processes for more specific detail of best practice digital examination processes. Other types of digital examinations should follow the same principles, briefly summarised below.

- 5.4 The investigator needs to properly consider the nature and purpose of the digital examination. The investigator must be clear on what priorities are placed on the examination as it may well be that key information needs to be found in order to preserve evidence that may exist elsewhere. This is particularly the case where it relates to the existence of additional evidence, offenders and victims.

- 5.5 When submitting evidence to Digital Forensic Units, investigators must supply specific requirements. It is not practically possible to examine every item of digital data and clear tasking is needed to ensure that the digital forensic practitioner has the best chance of finding any evidence which is relevant to the investigation.

- 5.6 For more complex or lengthy investigations, an initial triage/review of the digital evidence (whether or not this is done using a specific triage tool) will give investigators and practitioners a better understanding of the nature of the digital evidence held. The forensic strategy should be regularly reviewed to take account of any changes in the direction of the investigation, which may occur as a result of digital forensic examination (for example, finding emails identifying a co-conspirator) or investigations elsewhere (a witness identifying another person as being of interest to the investigation). For this reason it is vital that the investigator and the digital forensic practitioner communicate regularly regarding the progress of the investigation.

- 5.7 If initial examination results in a large amount of data to be reviewed, consideration must be given to who is best placed to review that data. Often this will be the investigator, due to their greater knowledge of the case. Dependent on the source, this data may include:

- Internet history records;
- E-mails;
- Instant Messaging Logs;
- Media files (images and videos);
- Text documents;
- Spreadsheets;
- CCTV;
- Text Messages.

- 5.8 Collaboration with the Digital Forensic Unit will ensure that the significance of any reviewed data is not misunderstood. For example, when reviewing keyword hits which exist in deleted files, the significance of a hit's location may need explanation from a digital forensic practitioner.
- 5.9 For mobile phone examinations, different levels of examination may be appropriate depending on the intelligence relating to the device and the requirements of the investigation. For example, a phone which has been found in a drawer may be examined only to retrieve the necessary information to request billing details and to establish whether it is owned by the suspect (level 1). A phone which is known to be in regular use by a suspect in a high profile investigation may be subject to a much more in-depth examination involving the retrieval of deleted data and potentially the physical removal and examination of memory chips (level 4). These examination levels are outlined in the NPJA mobile phone SOPs.

5.10 INTERPRETATION OF DIGITAL DATA

- 5.10.1 As with other forensic evidence, interpretation is often required to ensure the evidential weight of recovered digital evidence is clear. Practitioners who undertake the interpretation of digital data must be competent to do so and have had sufficient training to undertake the task assigned to them.
- 5.10.2 As an example, the presence of indecent images of children on a computer would not in itself be sufficient evidence of possession, as the possessor must be aware of the existence of the images. A digital forensic practitioner may interpret the presence of other digital evidence (such as a list of recently opened files, recent search terms, the name and location of folders/files containing the material, or whether or not the computer is password protected) to establish the likelihood of the user being aware of the existence of these images.
- 5.10.3 Establishing the provenance of digital evidence is another key task of the forensic practitioner, who must use their knowledge and skills to identify not just that the evidence exists but also how it came to be there. This is common to all forensic disciplines; for example, the presence of a defendant's fingerprint on a bottle at the crime scene may not have any bearing on whether the defendant committed the crime if the bottle may have been carried there by someone else. It is the responsibility of the practitioner to carry out analysis to identify provenance where necessary, to mitigate the risk of their findings being misinterpreted.
- 5.10.4 Often the role of the digital forensic practitioner will be to make investigators and prosecutors aware of the limitations of the digital evidence as well as its strengths.
- 5.10.5 It must also be borne in mind that the development of digital technology is dynamic and the practitioners may well face significant challenges to their knowledge. It is not possible to be an expert in all aspects of digital forensic examination, but a practitioner should be aware of the limits of their knowledge and where further research or additional specialist knowledge is required.

6. SECTION 6 – PRESENT

- 6.1 This also refers to:
- NPJA Forensics21 process maps;
 - CPS disclosure manual, annex K.
- 6.2 Communication of the results of a digital forensic examination may be through a number of means:
- Verbally to an investigator/officer throughout a case;
 - By a statement or report on conclusion of the case;
 - In court if witness evidence is required.

- 6.3 In all cases a digital forensic practitioner must be aware of their duty of impartiality and that they must communicate both the extent and the limitations of the digital forensic evidence. This is especially important as, due to the nature of digital forensic evidence, it is not always immediately understandable by the layman.

6.4 VERBAL FEEDBACK

- 6.4.1 This should be given regularly throughout the progress of an examination. In this way it will enable the investigator to pursue relevant lines of enquiry as these become evident, and will ensure that the practitioner is up-to-date with any information required to better target their investigation.
- 6.4.2 It is important that this communication be recorded for potential disclosure at a later date. Good practice would be for a verbal conversation to be followed up via email, or to be recorded in contemporaneous notes.

6.5 STATEMENTS OR REPORTS

- 6.5.1 The statement or report is the ultimate product of the examination. It should outline the examination process and the significant data recovered. Whilst an initial report may be relatively brief, the practitioner should be in a position to produce a full technical report should one later be required.
- 6.5.2 The report should be written to be understandable to the reader; this may include the use of a glossary, diagrams/screenshots to illustrate points, the use of examples and avoidance of technical jargon.
- 6.5.3 When particular items are reproduced in a report, care should be taken to ensure that the representation is accurate. For example, pictures should not be reproduced at a larger size without this being made clear in the report. If a report is produced digitally, items should be reproduced where possible in their original file formats, to ensure that those viewing will see the item as close as possible to its original appearance. If this is not appropriate (for example, if a file needs to be converted to a more common format for reviewing) then the fact that it has been converted must be stated in the report. Where it is not possible to reproduce the item as it would have originally been viewed, for example, when a webpage is retrieved some time after the original page was accessed, this must also be clearly stated in the report.
- 6.5.4 The report should make clear the strength of any conclusions reached and always identify where an opinion is being given, to distinguish this from fact. Where opinion evidence is provided, the practitioner must state the facts on which this is based, and how he or she came to this conclusion.

6.6 WITNESS EVIDENCE

- 6.6.1 A practitioner may need to testify about not only the conduct of the examination, but also the validity of the procedure and their experience and qualifications to conduct the examination.
- 6.6.2 Expert witness training should be considered for digital forensic practitioners so they are familiar with the process of giving evidence and aware of their responsibilities as witnesses. A digital forensic practitioner will not always be giving expert evidence and should clearly understand the distinction between expert evidence and evidence of fact.
- 6.6.3 When giving evidence, practitioners must make clear when they are expressing facts and when they are giving opinions, as above. Practitioners, when giving expert evidence, must take care to do so only where it relates to their own area of expertise and remember that their duty when giving evidence (whether it be in report form or as a witness) is to the court, regardless of which party has instructed them.

6.7 CONTEMPORANEOUS NOTES

- 6.7.1 It is worth repeating at this point that full records should be made of all actions taken. These must be disclosed to the defence who may subsequently cause a further examination to be conducted. A significant part of such an examination will be to validate the actions and results of the original examination. Such records are also part of the unused material for the case under investigation.

7. SECTION 7 – GENERAL

7.1 TRAINING AND EDUCATION

- 7.1.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations ('Managers' Guide').

- 7.1.2 The general principle of training in digital investigation significantly differs from usual police training. Owing to the rapidly changing environment of technology, there is a requirement for the continuous but essential retention and updating of skills.

- 7.1.3 Readers should refer to the section concerning training in the Good Practice and Advice Guide for Managers of e-Crime Investigations.

- 7.1.4 It is also the personal responsibility of any person working within the area of digital forensics to maintain their knowledge of the subject areas they are involved in. Formal training is just one route, but there is also a vast amount of open-source information available for self development and awareness. (Practitioners should be mindful that the veracity of open-source information cannot always be established, and should critically evaluate any information sourced in this way.) Professional development can also be progressed by attending conferences and technical workshops, conducting independent research, participating in online specialist forums or by discussions with subject matter experts in other forces or agencies.

- 7.1.5 Police personnel should also be aware of POLKA (Police On-Line Knowledge Area), an information sharing resource where there are digital forensic communities that discuss numerous topics and a library of some relevant documentation.

7.2 WELFARE IN THE WORKPLACE

- 7.2.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations.

- 7.2.2 There are a number of aspects concerning the welfare of staff working within the digital forensic area and the risks associated with that type of work:

- The psychological effect of viewing disturbing material including indecent images of children (IIOC);
- Electrical safety;
- Ergonomics, including working with Display Screen Equipment (DSE);
- Biohazards.

- 7.2.3 Both staff and managers should be aware of the potential impacts of these and take steps to minimise their effect. For further details, refer to the Managers' Guide.

7.3 DIGITAL FORENSIC CONTRACTORS

7.3.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations;
- Forensic Regulator's Codes of Practice and Conduct.

7.3.2 Where the services of commercial forensic service providers are required by law enforcement, it is important to select external consulting witnesses/forensic practitioners carefully. Any external practitioner should be familiar with, and agree to comply with, the principles of digital evidence referred to in this guide.

7.3.3 Selection of external providers, particularly in the more unusual or highly technical areas, can be a problem for the investigator. Digital forensic units may be able to offer more advice on the criteria for selection.

7.3.4 Readers should refer to the ACPO Managers' Guide for further suggestions on the practical aspects of selecting an external forensic service provider (including such aspects as security clearance and physical security requirements or procurement issues). They should also ensure that any forensic service provider engaged on law enforcement work is able to work in accordance with the Forensic Regulator's Codes of Practice and Conduct which requires ISO accreditation (ISO 17025 and ISO 17020). The Regulator will expect compliance for all digital forensic services by 2014, but procurement frameworks and contracts should be looking at compliance for external service providers in advance of this date.

7.3.5 When engaging the services of digital forensic contractors, processes and policies for the retention of case-related data should be considered, both on an ongoing basis and following the termination of the contract. Contractors and those engaging them must comply with the terms of the Data Protection Act, and with any local policies of the engaging organisation.

7.4 DISCLOSURE

7.4.1 Also refers to:

- Attorney General's Guidelines on Disclosure (revised April 2005);
- CPS Disclosure Manual.

7.4.2 The particular issues relating to disclosure of digital evidence are typically those of volume. A digital investigation may involve the examination of a vast amount of data and it is not always straightforward for investigators and prosecutors to discharge their disclosure obligations in respect of this. For example, the average hard disk is now larger than 200 gigabytes and this, if printed out on A4 paper, would be 10,000,000 pages long. In addition, the nature of digital evidence means it is not always possible to create a static representation which preserves the nature of the original evidence (e.g. of a database) and in some cases data can only be disclosed electronically, such as CCTV.

7.4.3 The Criminal Procedure and Investigations Act 1996 (CPIA) came into force on 1 April 1997¹. The Act, together with its Code of Practice, introduced a statutory framework for the recording, retention, revelation and disclosure of unused material obtained during criminal investigations commenced on or after that date.

7.4.4 Additional guidance for investigators and prosecutors to assist them in complying with their statutory duties is set out in the Attorney General's Guidelines on Disclosure (revised April 2005). ACPO and the CPS have also agreed detailed joint operational instructions for handling unused material, currently set out in the Disclosure Manual.

¹ It has recently been amended in key respects following the implementation of some of the provisions of Part V of the Criminal Justice Act 2003, as of 4 April 2005

- 7.4.5 What follows should be regarded as a very brief summary of some of the relevant guidance in the Disclosure Manual. It is not intended as a replacement for the detailed guidance provided in the Manual itself.
- 7.4.6 Even in relatively straightforward cases, investigators may obtain, and even generate, substantial quantities of material. Some of this material may in due course be used as evidence: for example, physical exhibits recovered from the scene of the crime or linked locations, CCTV material, forensic evidence, statements obtained from witnesses and tape recordings of defendants interviewed under caution before charge. The remaining material is the 'unused material', and it is this material which is the subject of the procedure for disclosure created under the CPIA.
- 7.4.7 Generally material must be examined in detail by the disclosure officer or the deputy but, exceptionally, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form. For example, it might be reasonable to examine digital material by using software search tools. If such material is not examined in detail, it must nonetheless be described on the disclosure schedules accurately and as clearly as possible. The extent and manner of its examination must also be described together with justification ²for such action.
- 7.4.8 The CPIA Code of Practice also provides guidance concerning the duty to pursue all reasonable lines of enquiry, in relation to computer material³. Examination of material held on a computer may require expert assistance and, in some cases, Digital Evidence Recovery Officers (DEROs) may be commissioned to help extract evidence and assist with unused material. DEROs may be police officers, police staff or external service providers. The use of DEROs and related matters is discussed in detail in Annex H of the Disclosure Manual.
- 7.4.9 It is important that the material is inspected and described on the unused material schedule, in accordance with the above guidance, as it is the schedules (non-sensitive and sensitive) which are, in due course, revealed to the prosecutor, in order that the latter can comply with the duty under section 3 CPIA to provide primary disclosure to the accused (or initial disclosure, where the criminal investigation in question has commenced on or after 4 April 2005).
- 7.4.10 Whether the material is disclosed under section 3 of the CPIA, following service of a statement, or after an application for specific disclosure under section 8 of the Act, disclosure may be in the form of providing a copy or copies of the material in question to the defence. It may also be by permitting the defence (or a suitable expert, instructed by the defence) access to the actual material. Guidance concerning this is set out in the Disclosure Manual, 30.8 – 30.13.
- 7.4.11 It is important to note that where the computer material consists of sensitive images falling within section 1(1) (a) of the Protection of Children Act 1978, the guidance set out in the Memorandum of Understanding Between CPS and ACPO concerning Section 46 Sexual Offences Act 2003 (signed on 4th October 2004) should be followed.
- 7.4.12 In Scotland, the question of disclosure is fundamentally different from that in England and Wales and is one specifically for the Procurator Fiscal. The question of disclosure was judicially considered in the case of McLeod Petitioner, 1988, SLT233. There is no obligation upon the Crown to produce every document in their possession that has any connection with the case. It is the duty of the Procurator Fiscal to disclose anything that is relevant to establish the guilt or innocence of the accused. The court will not lightly interfere with the view of the Procurator Fiscal.

² Paragraph 27, Attorney General's Guidelines on Disclosure (2005)

³ CPIA Code of Practice, paragraph 3.5

7.5 LEGISLATION

7.5.1 Also refers to:

- Legislation.gov.uk;
- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations.

7.5.2 A wide variety of legislation may apply in examinations of digital evidence. Some of the most relevant is detailed below.

i. **Computer Misuse Act 1990 (UK Wide)** (<http://www.legislation.gov.uk/ukpga/1990/18/introduction>)

S1 Unauthorised Access To Computer Material

- It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer. It will be necessary to prove the access secured is unauthorised and the suspect knows this is the case. This is commonly referred to as 'hacking'.
- The Police and Justice Bill 2006 amended the maximum penalty for Section 1 offences. The offence is now triable either way, i.e. in the Magistrates Court or the Crown Court. The maximum custodial sentence has been increased from six months to two years.

S2 Unauthorised Access with Intent to Commit Other Offence

- An offence is committed as per S1 but the S1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. The offence to be committed must carry a sentence fixed by law or carry a sentence of imprisonment of 5 years or more. Even if it is not possible to prove the intent to commit the further offence, the S1 offence is still committed. Max penalty: 5 years imprisonment.

S3 Unauthorised Acts with Intent to Impair Operation

- An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer. This 'impairment' may be such that access to data is prevented or hindered or that the operation or reliability of any program is affected. This offence carries a maximum penalty of ten years imprisonment. This offence is used instead of the Criminal Damage Act 1971, since it is not possible to criminally damage something that is not tangible. The Police and Justice Bill 2006 amended the original Section 3 Computer Misuse Act offence, unauthorised modification, and increased the maximum penalty to ten years imprisonment.

S3A Making, Supplying or Obtaining

Article for Use in S1 or S3 offences

- The Police and Justice Bill 2006 created a new S3A offence of making, supplying (including offers to supply) or obtaining articles for use in S1 or S3 computer misuse offences. The maximum penalty for this offence is two years imprisonment.

S10 Saving For Certain Law Enforcement Powers

- This section explains that S1 of the Act has effect without prejudice to the operation in England, Wales or Scotland of any enactment relating to powers of inspection, search and seizure.

S17 Interpretation

- This section assists by explaining the meaning of some of the words and phrases used within the Act.

ii. The Police & Criminal Evidence Act 1984

(<http://www.legislation.gov.uk/ukpga/1984/60/contents>)

- This legislation does not apply in Scotland unless officers from England, Wales and Northern Ireland are using their cross-border policing powers and procedures.
- Schedule 1 details the procedure by which special procedure material and excluded material can be obtained.
- A circuit judge can order that such material be produced to a constable for him to take away or that such material be made available for the constable to access within seven days of the order. For information held on a computer, an order can be made that the material is produced in a visible and legible form in which it can be taken away.

Or, an order can be made giving a constable access to the material in a visible and legible form within seven days of the order.

S8 Search Warrant

- A justice of the peace can issue a search warrant, if it is believed an indictable offence has been committed and evidence of that offence is on the premises. This warrant may, as per S16 of PACE, also authorise persons who can accompany the officers conducting the search – for example a computer expert.

S19 General Power of Seizure

- This details the power by which an officer can seize items and the circumstances in which they can be seized.

S20 Extension of Powers of Seizure to Computerised Information

- This section details the power for requiring information held on a computer to be produced in a form in which it can be taken away and in which it is visible and legible.

S21 Access and Copying

- This section details the power in relation to having items seized accessed and copied to other relevant parties.

S22 Retention

- This details the circumstances in which seized property can be retained.

S78 Exclusion of Unfair Evidence

- The court can exclude evidence where, with regard to all the circumstances, it would have an adverse effect on the fairness of the proceedings.

iii. Criminal Justice & Police Act 2001 (England, Wales & NI.)

(<http://www.legislation.gov.uk/ukpga/2001/16/contents>)

S50 (re search and seizure – bulk items)

- Describes the power by which an item can be seized, if it is believed it may be something or it may contain an item or items for which there is a lawful authorisation to search.

S50 (1)

- Where a person is lawfully on premises carrying out a search and it is not practicable to determine at the time if an item found is something that he is entitled to seize, or if the contents of an item are things that he is entitled to seize, the item can be taken away for this to be determined. There must be reasonable grounds for believing the item may be something for which there was authorisation to search.

S50 (2)

- Where a person is lawfully on premises and an item for which there is a power to seize is found, but it is contained within an item for which there would ordinarily be no power to seize and it is not practicable to separate them at the time, both items can be seized.

7.5.3 Factors to be considered prior to removing such property:

- How long would it take to determine what the item is or to separate the items?
- How many people would it take to do this within a reasonable time period?
- Would the action required cause damage to property?
- If the items were separated, would it prejudice the use of the item that is then seized?
- Once seized, the items must be separated or identified as soon as practicable. Any item found, which was seized with no power to do so, must be returned as soon as reasonably practicable. Items of legal privilege, excluded material and special procedure material, should also be returned as soon as practicable, if there is no power to retain them.

7.5.4 It should be noted that the use of this act gives additional rights (such as the right to be present during examination) to the owner of the property.

7.5.5 Equivalent powers in Scotland are granted under:

- Civic Government Scotland Act 1982;
- Criminal Procedure Scotland Act 1995;
- Common Law.

7.5.6 SEXUAL OFFENCES ACT 2003 (<http://www.legislation.gov.uk/ukpga/2003/42/contents>)
46 Criminal proceedings, investigations etc. E+W+N.I.

(1)After section 1A of the Protection of Children Act 1978 (c. 37) insert—
"1B Exception for criminal proceedings, investigations etc.

- (1) In proceedings for an offence under section 1(1)(a) of making an indecent photograph or pseudo-photograph of a child, the defendant is not guilty of the offence if he proves that—
- (a) it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world,
 - (b) at the time of the offence charged he was a member of the Security Service, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of the Service, or
 - (c) at the time of the offence charged he was a member of GCHQ, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of GCHQ.

(2) In this section "GCHQ" has the same meaning as in the Intelligence Services Act 1994."

7.5.7 CORONERS AND JUSTICE ACT 2009 (Came into force on 06 April 2010)
(<http://www.legislation.gov.uk/ukpga/2009/25/contents>)

7.5.8 CPS guidance regarding prohibited images of children can be found at:

https://www.cps.gov.uk/legal/p_to_r/prohibited_images_of_children/

- Sections 62-68 deal with "possession of prohibited images of children".

7.5.9 The offence targets certain non-photographic images of children, possession of which is not covered by previously existing legislation.

7.5.10 A prohibited image is pornographic and concentrates on genitals or shows a sex act and is grossly offensive, disgusting, or otherwise of an obscene character.

7.5.11 An image is of a child if impression conveyed is that of a child or the predominant impression is that of a child despite some physical characteristics shown are not those of a child.

7.5.12 If the image is in a series then the context of the series can be used to determine if the individual image is prohibited or not.

7.5.13 Classified films are excluded (unless an individual is in possession of a still or clip that has been extracted solely or principally for the purpose of sexual arousal).

7.5.14 There is a defence of having a legitimate reason for possession, or having not seen the image and not knowing, nor having cause to suspect, it was a prohibited image.

7.5.15 The maximum penalty is 3 years' imprisonment.

7.6 OTHER LEGISLATION

7.6.1 For additional guidance or information in relation to legislation not listed, investigators may wish to consult the Police National Legal Database (PNLD) or the UK Legislation website (which replaces the Office of Public Sector Information (OPSI) and Statute Law databases), available online at <http://www.legislation.gov.uk>.

GLOSSARY OF TERMS/ABBREVIATIONS USED IN THIS GUIDE

ACPO: Association of Chief Police Officers

DFU: Digital Forensic Unit

NPIA: National Police Improvement Agency

IIOC: Indecent Images Of Children

SPOC: Single Point Of Contact

RIPA: Regulation Of Investigatory Powers Act

RIPSA: Regulation Of Investigatory Powers (Scotland) Act

DPA: Data Protection Act

CCTV: Closed Circuit Television

IP Address: Internet Protocol Address - numerical address assigned to device in a computer network that uses the Internet protocol for communications.

PACE: Police & Criminal Evidence Act 1984

SIM: A subscriber identity module or subscriber identification module (SIM) on a removable SIM card securely stores the service-subscriber key (IMSI) used to identify a subscriber on mobile telephony devices (such as mobile phones and computers).

PUK: PIN Unlock Key (PUK)

CSP/ISP: Communications Service Provider/Internet Service Provider

REFERENCES

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations ('Managers' Guide')
http://www.acpo.police.uk/documents/crime/2011/20110301%20CBA%20ACPO%20managers_guide_v10.1.4%20for%20ecrime%20investigations_2011.pdf
- Attorney General's Guidelines on Disclosure (revised April 2005)
http://www.cps.gov.uk/legal/a_to_c/attorney_generals_guidelines_on_disclosure/
- Crimes involving websites, forums and blogs
- CPS disclosure manual
http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/
- Digital Imaging Procedure v2.1
[http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_\(Web\)47aa.html?view=Standard&pubID=555512](http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512)
- First Responder's Guide
- Forensic Science Regulator's Codes of Practice and Conduct
<http://www.homeoffice.gov.uk/publications/agencies-public-bodies/fsr/codes-conduct-practice?view=Standard&pubID=868070>
- Network forensics and volatile data collection
- NPIA Forensics21 *HTCU Computer Examination Process, 2011*
- NPIA mobile phone SOPs
- Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0
http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev13c4f.html?view=Standard&pubID=585513
- SCDEA guidance

ACKNOWLEDGEMENTS

Review Board members

Paul Birch (Serious Fraud Office)
Lisa Burrell (Police Central e-Crime Unit)
Rick Conway (Surrey Police)
Steve Edwards (Police Central e-Crime Unit)
Dennis Edgar-Neville (Canterbury University/British Computer Society)
Danny Faith (NTAC/F3)
Steve Guest (IACIS)
Dan Haagman (7-Safe)
Sonny Hanspal (NPJA)
Keith McDevitt (SCDEA)
Jelle Niemantsverdriet (VerizonBusiness)
Bev Nutter (MPS-DEFS)
Harry Parsonage (Nottingham Police)
Peter Salter (PSNI)
Lindy Shepherd (Cranfield University)
Paul Slater (PWC)
Rob Watson (7-Safe)
Alastair Wilson (SCDEA)
Mark Wilson (MPS-DOI)
Paul Wright (VerizonBusiness)

Other acknowledgments

Esther George (CPS)
Jane Stevenson (Workplace Wellbeing)
Eddie Fisher (MPS-DEFS)

APPENDIX A

NETWORK FORENSICS

Home and corporate network environments

Networks of computers are becoming more common in the domestic environment and are well established in corporate settings. In the home, they are usually based around the broadband Internet connection, which often also offers functionality to set up a small internal (and often wireless) network within the household. In corporate environments, more advanced network setups can be found, for which no generic description can be given.

The use of wireless networks in both the corporate and home environment is also increasing at a considerable rate. To the forensic investigator, this presents a number of challenges and an increased number of potential artefacts to consider. Owing to the potential complexity of 'technical' crime scenes, specialist advice should be sought when planning the digital evidence aspect of the forensic strategy.

Wireless devices

A whole range of wired and wireless devices may be encountered:

- Network devices which connect individual systems or provide network functionality: Switches, hubs, routers, firewalls (or devices which combine all three).
- Devices to connect individual computers to the network, such as network cards (which can also be embedded within the computer)
- Devices to set up a wireless network: Wireless Access Points.
- Printers and digital cameras.
- Bluetooth (small range wireless) devices – PDAs, mobile phones, dongles.
- Hard drives which can be connected to the network.

Wireless networks cannot be controlled in the same way as a traditionally cabled solution and are potentially accessible by anyone within radio range. The implications of this should be carefully considered when planning a search or developing the wider investigative strategy. A device, such as a computer or a hard drive, may not be located on the premises where the search and seizure is conducted.

Home networks and data

If devices are networked, it may not be immediately obvious where the computer files and data, which are being sought, are kept. Data could be on any one of them. Networks, both wired and wireless, also enable the users of the computers to share resources; such as printers, scanners and connections to the Internet. It may well be the case that if one of the computers is connected to the Internet, some or all of the others are also.

With the widespread use of broadband type Internet subscriptions such as ADSL and cable, the Internet connection is nowadays likely to be of an 'always on' type connection. This implies that even if no-one is apparently working on a computer or using the Internet, there may be data passing to and from computers or between the network and the Internet.

If a wired network is present, there will usually be a small box (called a 'hub' or a 'switch') also present, connecting the computers together. Hubs, switches and routers look very much the same as one another. The network cables are usually connected at the rear.

The network may also be connected to another device (called a Cable Modem or a ADSL Modem) providing access to the Internet. Sometimes, the hub/switch/router mentioned before are combined with these modems in one device.

One wire from a modem will usually be connected to the telephone or television cable system and another wire will be connected either to one of the computers present or directly to the network hub, or the modem itself may be incorporated within the hub in a modem/router.

Operation planning in networked environments

When planning an operation involving a network, consider carefully the possibility of remote access, i.e. person(s) accessing a network with or without permissions from outside the target premises. Investigators should consider the possibility of nefarious activity being carried out through the insecure network of an innocent party. The implications of such a scenario are that search warrants could be obtained on the basis of a resolved Internet Protocol address, which actually relates to an innocent party. The implications are potentially unlawful searches, legal action taken against the relevant investigative agency and a waste of resources.

Consider also the possibility of a computer's access to remote online storage, which may physically reside in a foreign jurisdiction. This can include web-based services for email, photo or document storage or other applications offered via the Internet. There will be legal issues in relation to accessing any such material. Legal advice should be sought prior to any access or retrieval and often the provider of the particular service will have to be contacted to ensure that material is preserved while the relevant mutual legal assistance requests are being arranged.

Network detection

Network detecting and monitoring is a specialist area and should not be considered without expert advice. Recommendations for dealing with networks and wireless implementations involve the following steps:

- Identify and check network devices to see how much network or Internet activity is taking place. Consider using a wireless network detector to determine whether wireless is in operation and to locate wireless devices. Consideration should also be given to mobile Internet devices such as 3G or GPRS dongles or phones, which operate using the mobile phone network;
- As you do so, consider photographing the layout of the network and the location of the machines connected to it, so as to allow a possible future reconstruction;
- Once satisfied that no data will be lost as a result, you may isolate the network from the Internet. This is best done by identifying the connection to the telephone system or wireless communications point and unplugging it from the telephone point. Keep modems and routers running, as they may need to be interrogated to find out what is connected to them. Owing to their nature, it is particularly difficult to ascertain what is connected to a wireless network;
- Trace each wire from the network devices to discover the computer to which it is connected. This may not be possible in premises where cables may be buried in conduits or walls (advice in this case should be sought from the local IT administrator, if available, as to the set up of the system). Make a note of each connection. Note which computer is connected to which number 'port' on the network device (hub / switch / router or multi function device). Label each connection in such a way that the system can be rebuilt exactly as it stands, should there be any future questions as to the layout. It is highly recommended that pictures be taken of the setup;
- Consider making a connection to the access point/router in order to establish the external IP address. Most modern networks use Network Address Translation (NAT) which means that they communicate with an internal IP address and never get assigned an external IP one.

In a wireless environment, remember that no cables are used between a PC and other devices. However, there will still be some physical cabling to each device (which could include a network cable to the wired network, power cables etc.), the configuration of which should be recorded. Please also note that Cable / ADSL modems can have wireless capabilities built in.

- Once satisfied that the evidential impact is acceptable, you may remove each connection in turn from the network device once it has been identified. This will isolate each computer in turn from the network. The same can be done with cabling into wireless devices;
- Seize and bag all network hardware, modems, original boxes and CDs / floppy disks etc. (provided they are easily removable);

- Subsequently treat each device as you would a stand-alone device;
- Remember that the data which is sought may be on any one of the computers on the network. Officers should make a decision based on the reasonable assumption that relevant data may be stored on a device before seizing that device;
- Bear in mind the possibility that the network may be a wireless network as well as a wired one, i.e. certain computers may be connected to the network via conventional network cabling. Others may be connected to that same network via the mains system, and others may be connected via a wireless link;
- Also, bear in mind that any mobile phones and PDAs may be wireless or Bluetooth enabled and connected to a domestic network.

Concerns with remote wireless storage often focus around the inability to locate the device. In this instance, it would be impossible to prove that an offence had been committed. Artefacts on seized computers might provide evidence that a remote storage device has been used, however the analysis of such artefacts will take time and this cannot often be done during the onsite seizure.

Corporate network environments

When dealing with computer systems in a corporate environment, the forensic investigator faces a number of differing challenges. If the system administrator is not part of the investigation then seek their assistance. The most significant is likely to be the inability to shut down server(s) due to company operational constraints. In such cases, it is common practice that a network enabled 'forensic software' agent is installed, which will give the ability to image data across the network 'on-the-fly', or to a network share or a locally connected removable storage medium such as a USB hard drive.

Other devices could be encountered which may assist the investigation. For example, routers and firewalls can give an insight into network configuration through Access Control Lists (ACLs) or security rule sets. This may be achieved by viewing the configuration screens as an administrator of the device. This will require the user names and passwords obtained at the time of seizure or from the suspect during interview.

By accessing the devices, data may be added, violating Principle 1 but, if the logging mechanism is researched prior to investigation, the forensic footprints added during investigation may be taken into consideration and therefore Principle 2 can be complied with.

In the case of large company networks, consider gaining the advice and assistance of the network administrator/ support team (assuming that they are not suspects).

VOLATILE DATA COLLECTION

In certain circumstances, it may be necessary or advisable for computer forensic investigators to gather evidence from a computer whilst its running or in a 'live' state. This technique has become a common practice as, even though some changes to the original evidence will be made, this method often allows access to evidence which would have been unavailable if the power is removed from a system. In order to capture volatile data on a device the device WILL have to be accessed. Therefore changes WILL be caused by the examiner.

Special consideration should be given to Principle 2 of the guidelines, as conducting live-forensics implies access to the original evidence. Any person doing this needs to be competent and fully aware of the impact their actions have and should be prepared to explain their reasons for taking this route.

Live forensics approach

By profiling the footprint of trusted forensic tools used to gather volatile data, the digital forensic examiner can understand the impact of using such tools and can explain any artefacts left by the tools.

In order to ensure that a consistent approach is used and the chance of errors is minimized, it is recommended to use a scripted approach using a number of basic and trusted tools. Regardless of the tools used, it is advisable to start with capturing the contents of RAM, the volatile memory.

If other tools are used before the contents of the RAM are stored, it is very likely that running the forensic tools will overwrite parts of the RAM.

Other examples of information, which might be available in the dump of the RAM contents, can be retrieved using different tools:

- listings of running processes;
- logged on and registered users;
- network information including listening, open and closing network ports;
- ARP (address resolution protocol) cache;
- Registry information.

The tools used to capture this volatile information are generally run from removable media like a USB stick, DVD or CD-ROM or a floppy disk. A USB stick is generally most convenient, as the output of the tools can be written back to the stick. Writing tool output to the original drive should be avoided whenever possible, as this changes the contents of the hard drive and can destroy potential evidence. Again, principle 2 does allow the investigator to do this, but a conscious decision will have to be made and the process written down.

When inserting USB devices the examiner must ensure that they know the details of the serial numbers of the devices they are connecting so that they can be eliminated when analysing the data captured.

When in doubt as to whether or not to use live forensics, consult with the digital forensic examiner for advice. And, it should be noted that in live forensics it is not always possible to know upfront which approach will yield the best results. Whichever method is chosen, remember to take meticulous notes – as dictated by principle 3.

Summary of steps

A summary of the steps to be taken is shown below. Documentation of all actions, together with reasoning, should also apply when following such steps:

- Perform a risk assessment of the situation – Is it evidentially required and safe to perform volatile data capture?
- If so, install volatile data capture device to a removable data carrier (such as a USB stick) – preferably, this has already been done prior to starting the operation;
- Plug the data carrier into the machine and start the data collection script;
- Once complete, stop the device (particularly important for USB devices, which if removed before proper shutdown can lose information);
- Remove the device;
- Verify the data output on a separate forensic investigation machine (not the suspect system);
- Immediately follow with standard power-off procedure.

The capture and analysis of volatile data no doubt presents the investigator with technical challenges. However, as cases become more complex and connectivity between devices and public networks proliferate, with an increase in more advanced malware, which cannot always be retrieved using more traditional disk forensics, the above recommendations will need to be considered.

It is vitally important that only someone with the relevant training and is competent to do so should take any of these actions.

APPENDIX B

CRIMES INVOLVING WEBSITES, FORUMS, AND BLOGS

Where a crime involves evidence displayed on a website the most convenient method of recovering the evidence may be by engaging the assistance of suitably trained staff to visit the website and take copies of the evidential content. In order to do this the officer taking report of the matter needs to obtain the address of the website, for example, <http://www.acpo.police.uk>, or if it is a specific page within the site.

http://www.acpo.police.uk/about_pages/structure.html.

When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the investigator is recorded in a log. The recommended method for copying a website is to visit the site and record the relevant pages using video capture software so there is a visible representation of how they look when visited at the time. If video capture software is not available then the pages can be saved as screenshots. It is also advisable to follow this by capturing the web pages themselves either by using website copying software or saving the individual pages. Copying the pages themselves, as well as obtaining a visual record, means that the code from the web pages is also secured should that become relevant later.

This work should be conducted from a computer which has been specifically set up to be non-attributable on the Internet. Failure to use an appropriate system may lead to the compromise of other police operations. Anyone visiting a website generally exposes a certain amount of information to the website, for example it is common on police systems to have a web browser which is branded with the forces name. This branding is exposed to a website being visited and so may be recorded in logs on the site along with other information amongst which, will include the pages visited.

If it appears likely that the evidence on the website might be lost by a delay in carrying out the above procedures then the person reporting may be asked to make a copy of the evidence by whatever means they are capable of (either printing, screenshot or saving pages), alternatively this could be done by the person receiving the report. Before taking these steps every effort should be made to secure the services of a competent person to carry out this work as failing to capture the information correctly could have a detrimental impact on the investigation.

Where there is difficulty in capturing the evidence by visiting the site it might be possible to make an official request to the owner of the site by whatever legal procedures are required within the jurisdiction. The CSP/ISP SPOC or Digital Forensic Unit can usually advise on the appropriate procedures.

By making a request to the service provider hosting the site it may be possible to recover evidence of who has created the web page or posting. It is not unusual for details of the user such as name, address, phone number, banking details, email address, and alternative email address to be recorded by a host.

If there is a requirement to identify who has committed some activity on a website, for example where a fraud has been committed by purchasing goods from a website or by posting a message on a website, the likelihood is that the suspect may be traceable from logs on the site. When any user accesses the Internet they are allocated a unique address known as an IP address and their Internet Service Provider (ISP) keeps logs of the times and dates and the identity of the user allocated any IP address.

When a user visits a site and conducts some activity, for example logs on, posts a message, or makes a purchase, it is likely that the user's IP address has been logged by the website. It is often possible to obtain copies of logs from websites if there is a requirement to see who has been active on a website by making a request via the force CSP/ISP SPOC.

If the evidence is no longer available to be retrieved by any of the above means, and where the use of resources can be justified by the seriousness of the case, it may be possible to recover evidence of the site contents from an end user device that has been used to view the site by conducting a forensic examination of the device.

Where investigators wish to carry out open source intelligence research on the Internet they should be trained to do so and conduct the research from a computer which cannot be attributed to the investigator's agency.

Covert Interaction on the Internet

In circumstances where investigators wish to communicate covertly with an online suspect they **MUST** use the services of a Nationally Accredited and Registered (CII). CIIs have received specialist training which addresses the technical and legal issues relating to undercover operations on the Internet.

Crimes involving email communication

There are generally two methods of sending and receiving email, one by using a web browser and accessing email online for example at the Hotmail, Windows Live, Yahoo or Google websites. In these circumstances the mail is stored on the webmail server and is read through the user's browser. The other method is to access email using a program such as Outlook or Windows Mail to download mail to the user's computer. The program is used to view and store the emails locally.

Where the evidence in a case involves an email sent from a person who the police want to trace the key evidence is usually found in what is known as the email's "Full Internet Header". Each email sent over the Internet contains this header which is normally not visible to the user. It contains details of the route taken across the Internet by the email and includes the IP address of the sender. Even where an email has been sent with a fictitious email address which has been registered with false details, it is often possible to identify the sender from the Full Internet Header.

In order to obtain the Full Internet Header the person taking the incident report needs to ascertain which of the two methods the recipient uses to access their email. Where it is web based identify the webmail host (i.e. Hotmail, Yahoo etc.) or if by a program on the computer ascertain what program and version number of the program. The version number can usually be found in the program's Help on the menu bar under an item called "About".

Each webmail provider and email program treat the Full Internet Header differently and if the officer or user does not know how to display the header the details of the webmail provider or program need to be passed to a specialist in the Digital Forensic Unit or CSP/ISP SPOC who will be able to provide advice.

Once the header has been exposed the relevant email should be printed together with the header, and may also be saved electronically. Depending upon the seriousness of the case and the volume of email evidence, advice may be sought from the digital forensics unit on the most appropriate method of securing and retaining the email evidence.

Once the full header has been obtained the force CSP/ISP SPOC will be able to use this to conduct enquiries to attempt to identify the sender from the originating IP address.

Where an email address of a suspect is known but there is no email available from which a full header can be obtained, it may be possible to identify the user of the email address and their location. Depending upon the email service provider various details of the user may be recorded together with the first registration IP address and a varying period of IP address login history. These details may be obtained by making an appropriate CSP/ISP SPOC request for the email address. In conducting such enquiries it needs to be recognised that it is a trivial exercise to send an email with a false email address in the "From:" field of an email.

On some occasions the investigating agency might access a user's email account with written authority from the user in order to secure evidence. Where this is the case, if third party material is exposed as a consequence of viewing the user's emails, advice should be sought as to whether a Directed Surveillance Authority should be in place in addition to the user's authority. Even if the password and log in details are available. For example as a result of the Forensic examination authority and formal authority is required to access the email account.

Where justified by the investigation, consideration may be given to accessing messages on an email provider's server by obtaining the appropriate RIPA authority.

Crimes Involving Internet Chat

Users can employ a number of different devices to engage in chat on the Internet. There are three main ways to chat - using a website's chat facility, for example Facebook, using an instant messenger program like Windows Live Messenger, or much less commonly, using Internet Relay Chat (IRC).

Where an incident is reported which involves the use of chat the person taking the report needs to ascertain what method of chat was being used, i.e. what is the name of the website hosting the chat and its full Internet address, or what program is being used. The key evidence to be secured is

- any information which may identify the suspect party, and
- the content of any chat.

If the chat is web-based the details of the website, any chat room name and the user name of the suspect should be obtained together with the times and dates of any chat activity. If the chat facility is part of a social networking site the user will most likely have a unique ID number as well as a user name. This is usually visible in the web browser's address bar when viewing a user's profile or when the mouse pointer is moved over the user name. The force CSP/ISP SPOC or Digital Forensic Unit can provide help in finding this ID number. If the chat is by instant messenger program then the user name of the suspect should be obtained together with the associated email address which is usually available from the contact list of the person reporting. Generally a user's contact list can be accessed from any computer connected to the Internet so if it is considered that the user's computer might be retained for a forensic examination then it should not itself be used to access the contact list.

There is usually an option for a user to save chat logs but more often than not the default setting is for logs not to be saved. If the user has saved chat logs that contain evidence, the logs should be saved to removable media for production as evidence, if no removable media is available they should be printed out. Users are able to engage in chat from many types of device in addition to computers. Where the circumstances of the case warrant it, an end-user device could be submitted for forensic examination in order to recover evidence of the suspect's contact details and chat content.

Where a suspect's user details are obtained it may be possible to identify the suspect by making the appropriate CSP/ISP SPOC requests.

In the event that the chat has been conducted using IRC the following details should be obtained - the IRC program used, the name of the IRC server, the channel and any usernames. Further advice should then be sought from the Digital Forensic Unit.

Communications in the course of a transmission

Digital evidence in transit may be any form of communication using the Internet or a telecommunications network such as email, chat, voice calls, text messages, and voice-mail. Where such evidence is sought advice should be obtained from the force Covert Authorities Bureau.

APPENDIX C

CRIME SCENES

There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined. This section is intended to assist individuals to ensure their actions in relation to seizure are correct.

The following guidance deals with the majority of scenarios that may be encountered. The general principles, if adhered to, will ensure the best chance of evidence being recovered in an uncontaminated and, therefore, acceptable manner.

Items found during a search will normally fall into the broad categories of computer-based media items, CCTV systems and mobile devices. These are considered separately below.

Proportionality

Before seizing an item, consider whether the item is likely to hold evidence (eg, is this a family computer or a computer belonging to a suspect?) Ensure that details of where the item was found are recorded. Consider when the offence was committed; when seizing CCTV, give consideration to narrowing down what is seized, by camera and/or time period. Check whether another system may be better placed to record the evidence. Differentiate between mobile phones found on a suspect and phones found in a drawer, as different levels of examination may be possible for these. Also consider that evidence may be stored online, or on an internet service provider's systems, and end-user devices may only be needed to obtain the details necessary to request this evidence from the service provider. If so, it is best to seize items in current usage, i.e. computers connected to the internet.

Digital devices and media should not be seized just because it is there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of PACE Legislation Codes of Practice equally apply to digital devices and media in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant.

Due regard should also be taken concerning any possible contravention of the European Convention of Human Rights.

What to take to a scene

The following is a suggested list of equipment that might be of value during planned searches. This basic tool-kit should be considered for use in the proper dismantling of digital systems as well as for their packaging and removal:

- Property register;
- Exhibit labels (tie-on and adhesive);
- Labels and tape to mark and identify component parts of the system, including leads and sockets;
- Tools such as screw drivers (flathead and crosshead), small pliers, and wire cutters for removal of cable ties;
- A range of packaging and evidential bags fit for the purpose of securing and sealing heavy items such as computers and smaller items such as PDAs and mobile phone handsets;
- Cable ties for securing cables;
- Flat pack assembly boxes - consider using original packaging if available;
- Coloured marker pens to code and identify removed items;
- Camera and/or video to photograph scene in situ and any on-screen displays;
- Torch;
- Forensically sterile storage material.

In addition, the following items may be useful when attending scenes to retrieve CCTV:

- Laptop with USB and network connectivity. A selection of proprietary replay software could be installed, to enable the downloaded data to be checked;
- External CD/DVD writer;
- USB hard drives.

Records to be kept

To comply with principle 3, records must be kept of all actions taken in relation to digital evidence, for example:

- Sketch map/photographs of scene and digital equipment;
- Record location and contact details;
- If a business, record opening hours;
- Details of all persons present where digital equipment is located;
- Details of digital items - make, model, serial number;
- Details of connected peripherals;
- Remarks/comments/information offered by user(s) of equipment;
- Actions taken at scene showing exact time;
- Notes/photographs showing state of system when found.

Computer based devices and media

This includes desktop or laptop PCs and Apple Macintosh systems, digital cameras, memory cards, USB sticks, external hard drives and games consoles, amongst other items. Mobile devices which have wireless connectivity/ communications capability (such as tablet computers and satellite navigation systems) fall under the heading of 'mobile devices'.

Systems which are powered on (running) need to be handled with care, as there is the potential to make unwanted changes to the evidence if these are not dealt with correctly. Such systems should only be accessed by appropriately trained officers. In addition; volatile data of evidential value may be lost. Be aware of the potential to lose other valuable data, particularly when dealing with business systems, which could give rise to a claim for damages. In these cases expert advice should be sought before seizing a business system which is powered on.

Desktop and laptop computers/games consoles

The scene should be fully documented by written notes and/or a photographic record.

If a device is powered on, it needs to be handled carefully to preserve any volatile data and to avoid unwanted changes to the stored data.

Consider removing the device from any network, as devices can be remotely accessed, causing alteration to the data - but balance this against the possibility of losing data of evidential value, such as the list of currently open connections. If unsure, seek expert advice.

Seizure steps:

1. Secure and take control of the area containing the equipment;
2. Move people away from any computers and power supplies and do not allow any interaction with digital devices by suspect;
3. Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date;
4. Allow any printers to finish printing.

If switched off:

5. Do not, in any circumstance, switch the computer on;
6. Make sure that the computer is switched off, by moving the mouse – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on;
7. Be aware that some laptop computers may power on by opening the lid. Remove the battery from the laptop. Seize any power supply cables for future use.

If switched on:

8. Record what is on the screen by photographing it and by making a written note of the content of the screen;
9. Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the investigator should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video it and note its content. If password protection is shown, continue as below, without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances. (For games consoles, or tablet computers, the equivalent would be moving the controller joystick or touching the touchscreen);
10. If the system may contain valuable evidence in its current state (for example, if it is currently displaying a relevant document or an instant message conversation), seizing officers should seek expert advice from their local digital forensic unit as this may be lost if the power is lost. This is especially important if the suspect is a technically knowledgeable user who may be using encryption, as there may be no way to retrieve evidence stored in encrypted volumes once the power is lost;
11. Consider advice from the owner/user of the computer but make sure this information is treated with caution;
12. Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss. This is normally evident by a small LED (light) lit on the casing. In this case, officers should seek advice from their local digital forensic unit;
13. Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket). When removing the power supply cable, always remove the end connected to the computer, and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power supply is fitted. If the equipment was switched on, do not close down any programs or shut down the computer, as this will cause changes to the stored data and may trigger wiping software to run, if this is installed;
14. Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the digital forensic unit;
15. Search the area for diaries, notebooks or pieces of paper with passwords on them, often attached or close to the computer;
16. Ask the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately;
17. Allow the equipment to cool down before removal;
18. Track any cables that can be seen as they made lead you to other devices in other rooms.

Mobile devices

This includes mobile phones, smartphones, and other devices which may have wireless connectivity/communications capability such as tablet computers, personal digital assistants (PDAs), personal media players and satellite navigation systems.

1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;
2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;

3. If the device is switched on, power it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.

However, in exceptional circumstances the decision may be made to keep the device on. Timely access to the handset data is critical the decision may be made to leave the device switched on. Consideration may be given to place the handset in a Faraday environment to further prevent signal reception. In such circumstances advice should be sought from the DFU.

4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;
5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;
6. Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period. Submit items for examination as soon as possible.

Handling and transporting digital evidence

Digital Devices

Handle with care. If placing in a car, place upright where it will not receive serious physical shocks. Keep away from magnetic sources (loudspeakers, heated seats & windows and police radios).

Hard disks

As for all digital devices protect from magnetic fields. Place in anti-static bags, tough paper bags or tamper-evident cardboard packaging or wrap in paper and place in aerated plastic bags.

Removable storage

floppy disks, memory sticks, memory cards, CDs/DVDs) Protect from magnetic fields. Do not fold or bend. Do not place labels directly onto floppy disks or CDs/DVDs. Package in tamper-force approved packaging to avoid interaction with the device whilst it is sealed.

Other items

Protect from magnetic fields. Package correctly and seal in plastic bags. Do not allow items to get wet.

Other Considerations

1. If fingerprints or DNA evidence are likely to be required, always consult with the investigator;
2. Using aluminium powder on electronic devices can be dangerous and result in the loss of evidence. Before any examination using this substance, consider all options carefully.

The equipment should be stored at normal room temperature, without being subject to any extremes of humidity and free from magnetic influence such as radio receivers. Dust, smoke, sand, water and oil are also harmful to electronic equipment. Some devices are capable of storing internal data (such as the time and date set on the system) by use of batteries. If the battery is allowed to become flat, internal data will be lost. It is not possible to determine the life expectancy of any one battery. However, this is an important consideration when storing a device for long periods before forensic examination and should be addressed in local policy.

APPENDIX D

DEVELOPING A DIGITAL INVESTIGATION STRATEGY

The investigation of crimes and incidents in which digital evidence is involved, particularly the Internet, presents some unique challenges to the investigator. The explosion of the availability and use of technology, the growth of virtual storage, development of 'Cloud Services' (online services) and the convergence of mobile and traditional computer technology has resulted in most investigations having a digital element of some description.

Investigators need to have a greater understanding of the use of digital evidence if interviews of witnesses and suspects are to be effective. This is particularly the case in serious or complex investigations where a failure to identify and secure volatile digital data could have a significant impact on the conduct of the investigation.

It is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence. Irrespective of the size or complexity the investigator should consider five primary stages.

- Data Capture and search and seizure at crime scenes;
- Data Examination;
- Data Interpretation;
- Data Reporting;
- Interview of Witness and Suspects.

Investigators should seek the advice of their force Telecoms/ISP SPOC, Network Investigators and Digital Forensic Units at the earliest opportunity to formulate a written digital forensic strategy.

Due consideration should always be given by the investigators of the benefits to the overall investigation of conducting any digital forensic work

DATA CAPTURE STRATEGY

The investigator should develop a Data Capture Strategy to identify and secure all relevant digital evidence. Other than a requirement to react to immediate events the investigator should be able to plan this strategy in advance.

Where a crime or incident is reported, early consideration should be given to the potential to glean evidence from the Internet or end user devices which have a digital memory capacity and from which evidence / intelligence may be retrieved.

Social Network Sites

Priority – Establish the use of Social Networking, Online Communities, Online Storage and other Cloud Services by witnesses and suspects. Whilst this may be revealed by the examination of seized devices it may be gleaned more quickly if asked during interview.

Many current investigations involve Social Networking Sites. It is imperative that early consideration is made around securing Social Networking Profiles that fall within the investigation. The best evidence is available from the service provider however they are often located outside of the UK and may or may not secure the content on the appropriate request via the force CSP/ISP SPOC. As such the investigator should always secure a copy of what is seen by them as this may be the only opportunity to secure this evidence before it changes.

Open Source Research

The internet is a huge repository of information much of it of value to the investigator. Research by properly **trained** staff, preferably with access to a stand alone computer, will enable the investigator to get the best from the vast amount of information that is now held online. In addition to this the force CSP/ISP SPOCs will be able to give advice on the type of data that can potentially be obtained from ISP's, web mail and web based providers.

Care should be taken when undertaking Internet research from any computer linked to the Police National Network (pnn) as a digital footprint will be left and may reveal the law enforcement interest. This will not be obvious to the general internet user but will most certainly be clear to the hosts or providers of the service and those who are particularly technically aware and monitoring IP addresses.

Registration details are often asked for and whilst in some instances they will inevitably be fictitious, on many occasions they will include the following;

- IP log on;
- Name and Address;
- Landline and Mobile phone Numbers;
- Banking data;
- Emails used;
- Username and passwords;
- Linked accounts.

Whilst law enforcement are used to working with RIPA, RIPA and the DPA to obtain information this legislation only applies within the UK. Many services are based outside of the UK based organisations.

It is essential that the CSP/ISP SPOC is engaged at the earliest opportunity to these enquiries with the objective of preserving known time critical data.

National Technical Assistance Centre (NTAC)

If encrypted files are located or suspected it is important that the suspect is asked for them, failure to do so may result in an offence under sec 49 of RIPA. Encryption is difficult to break and assistance can be sought via the Digital Forensic Unit from the National Technical Assistance Centre (NTAC) in London.

The National Technical Assistance Centre (NTAC) provides technical support only to public authorities, particularly law enforcement agencies and the intelligence services. It includes a facility for the complex processing of lawfully obtained protected electronic information.

NTAC is the leading national authority for all matters relating to the processing of protected information into an intelligible format and the disclosure of key material.

All public authorities should consult with NTAC at the earliest opportunity when considering exercising the powers in Part III of the Regulation of Investigatory Powers Act (RIPA).

A public authority cannot serve any notice under Section 49 of RIPA or, when the authority considers it necessary, seek to obtain appropriate permission, without the prior written approval of NTAC.

Investigating Crimes where Digital Evidence may be present

The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.

Digital evidence can be found in a number of different locations,

- Locally on an end-user device - typically a users computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;

- On a remote resource that is public - for example websites used for social networking, discussion forums, and newsgroups;
- On a remote resource that is private – an Internet Service Provider’s logs of users’ activity, a mobile phone company’s records of customers’ billing, a user’s webmail account, and increasingly common, a user’s remote file storage;
- In transit – for example mobile phone text messages, or voice calls, emails, or Internet chat.

Investigating Different Types of Crime and Identifying Sources of Evidence

It would be quite common for evidence of a crime to be in more than one of the locations mentioned above. However it might be much easier to obtain the evidence from one location rather than another; careful consideration should be given to the resources required to obtain the evidence.

For example, if evidence is required of contact between two mobile phone numbers, the best method would be to obtain call data from the Communication Service Providers via the force SPOC, rather than to request a forensic examination of the mobile phones. The call data is likely to be more comprehensive than call logs from a mobile phone and the times and dates can be relied upon, which is not necessarily the case with logs from a mobile phone.

COVERT FORENSIC COMPUTING

Some investigations may require consideration of gathering digital intelligence in a covert manner. It is evidently not appropriate to discuss covert tactics within this document however opportunities exist to capture digital data online and physically from devices in a covert manner where the appropriate authorities are in place.

DATA EXAMINATION STRATEGY

Devices seized as part of a search will be forwarded to the force Digital Forensic Unit in accordance with force policy.

The investigator needs to properly consider the nature and purpose of the digital examination. The investigator must tailor the needs of the digital examination not only based on the investigation requirements but the ability of the Digital Forensic Unit to deliver it. The better the briefing the better the advice will be.

The Investigator must be clear on what priorities are placed on the examination as it may well be, as previously stated, that key information needs to be found in order to preserve evidence that may exist elsewhere. This is particularly the case where it relates to the existence of additional evidence, offenders and victims. A preview of content may be appropriate albeit the limitations of this approach will require to be properly understood.

Priorities may also be set on the type of data to be extracted and viewed by persons other than the Digital Forensics Unit as this may reduce the burden on the unit and increase the likelihood of the delivery of the data. This will of course depend on the nature of the examination. But could include;

- Internet History;
- Emails;
- Evidence of webmail;
- Instant Messaging Logs;
- Media Files (images & videos);
- Social Networks;
- Forums & Chat Rooms;
- Cloud Services / Virtual Storage;
- File Sharing programs;
- Usernames / Passwords;
- Encrypted Files;
- Word Documents;
- Spreadsheets.

The discussion between the investigator and digital forensic unit should result in an agreed digital extraction / examination plan to achieve an agreed outcome. The plan may need to be reviewed as the evidential picture and priorities change.

DATA INTERPRETATION STRATEGY

Staff tasked by the investigator to undertake the digital data extraction / examination must be competent to do so and have had sufficient training to undertake the task assigned to them. It must be borne in mind that the development of digital technology is dynamic and the examiners may well face significant challenges to their knowledge.

It is the role of the Digital Evidence Examiner to provide the investigator with a report/statement accounting for the examination of the devices as part of the investigation. The report should account in full for the parameters set for the examination, data extracted and data examined. There should also be provision to provide an interpretation of technical aspects of the examination relevant to the provision of evidence in the case.

The investigator should have a full discussion with the examiner ahead of the production of any reports to ensure all the relevant evidence is contained in the report and that the processes used adhered to the ACPO Principles governing handling digital based evidence. These principles are explained in the section headed "The Principles of Digital Evidence" in this guide.

DATA REPORTING

The report is the ultimate product of the examination. It should outline the examination process and the significant data recovered. Whilst an initial report may be relatively brief, the examiner should be in a position to produce a full technical report should one later be required.

Examination notes must be preserved for disclosure or testimony purposes and, if required, the preparation of a full technical report. In Scotland, they will be preserved as productions to be used as evidence in court.

An examiner may need to testify about not only the conduct of the examination, but also the validity of the procedure and their experience and qualifications to conduct the examination.

The role of the examiner is to secure from any seized material true copy of any data that they may contain. Forensic hardware should be subject to initial and periodic testing. It is worth repeating at this point that full records should be made of all actions taken. These can be made available to the defence who may subsequently cause a further examination to be conducted. A significant part of such an examination will be to validate the actions and results of the original examination. Such records are also part of the unused material for the case under investigation.

It is important to remember that legislation continues to change to keep up with technological and societal change. It is important, therefore, to consider the legal requirements and restrictions when examining digital evidence. Recent case law and precedents set at higher courts are important considerations when preparing an evidence package for an investigator. This applies, in particular, to the use of the Internet and files downloaded from the Internet; or material accessible from foreign jurisdictions i.e. online data stores.

Interview of Witnesses and Suspects

The interview of witnesses/suspects is a crucial opportunity to identify key information about the nature and use of digital data relative to the investigation in hand. As such those involved must be properly briefed and competent to undertake the interview having the necessary understanding of the areas to explore.

Consideration should be given to consulting with a trained Interview Advisor with a view to the compilation of an appropriate interview strategy.

Bear in mind that the digital examination of devices seized will take time and may not necessarily reveal vital information that the witness / suspect may be aware of. Typically this may include;

- Web Mail Addresses / Username & Passwords / shared or sole use;
- Social Network Profiles / Username & Passwords / shared or sole use;
- Use of Forums & Chat Rooms / Username & Passwords;
- Use of Cloud Services / Username & Passwords / shared or sole use;
- Use of Virtual Storage / Username & Passwords / shared or sole use;
- Use of Role Play Gaming Sites / Username & Passwords / shared or sole use;
- Use of Auction sites / Username & Passwords / shared or sole use;
- Use of Online Banking;
- List of User Names;
- Use of Encryption / Encryption Keys;
- User Names of contacts;
- Use of the devices;
- Websites Visited;
- Internet Service Provider.

This list is not exhaustive

WORKBOOK FOR THE CREATION OF ACPO GUIDANCE/PRACTICE ADVICE

This workbook, with all sections completed, must be included in the final document as an Appendix and submitted, through the Head of the Business Area, to the Programme Support Office for quality assurance prior to submission to Cabinet for approval as ACPO Doctrine.

ACPO EQUALITY IMPACT ASSESSMENT TEMPLATE (DIVERSITY AUDIT) AS AGREED WITH THE CRE

1. Identify all aims of the guidance/advice

1.1 Identify the aims and projected outcomes of the guidance/advice:
To provide coherence to police policy and practice in relation to evidence obtained from digital media
1.2 Which individuals and organisations are likely to have an interest in or likely to be affected by the proposal?
Police, CPS, HMRC, SOCA, CEOP, SFO, PCeU, SCDEA

2. Consider the evidence

2.1 What relevant quantitative data has been considered?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
2.2 What relevant qualitative information has been considered?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
2.3 What gaps in data/information were identified?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	v
2.4 What consideration has been given to commissioning research?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A

3. Assess likely impact

3.1 From the analysis of data and information has any potential for differential/adverse impact been identified?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
3.2 If yes explain any intentional impact:	
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	
3.3 If yes explain what impact was discovered which you feel is justifiable in order to achieve the overall proposal aims. Please provide examples:	
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	
3.4 Are there any other factors that might help to explain differential/adverse impact?	
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	

4. Consider alternatives

4.1 Summarise what changes have been made to the proposal to remove or reduce the potential for differential/adverse impact:
N/A
4.2 Summarise changes to the proposal to remove or reduce the potential for differential/adverse impact that were considered but not implemented and explain why this was the case:
N/A
4.3 If potential for differential/adverse impact remains explain why implementation is justifiable in order to meet the wider proposal aims:
N/A

5. Consult formally

5.1 Has the proposal been subject to consultation? If no, please state why not. If yes, state which individuals and organisations were consulted and what form the consultation took:	
Early drafts of the work have been consulted on with law enforcement and those in the specialist ecrime private sector.	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
5.2 What was the outcome of the consultation?	
Additional revisions based on good practice in this specialist area of investigation. There were no revisions based on the 6 diverse areas.	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
5.3 Has the proposal been reviewed and/or amended in light of the outcomes of consultation?	
5.4 Have the results of the consultation been fed back to the consultees?	

6. Decide whether to adopt the proposal

6.1 Provide a statement outlining the findings of the impact assessment process. If the proposal has been identified as having a possibility to adversely impact upon diverse communities, the statement should include justification for the implementation:
N/A

7. Make Monitoring Arrangements

7.1 What consideration has been given to piloting the proposal?
N/A
7.2 What monitoring will be implemented at a national level by the proposal owning agency and/or other national agency?
N/A
7.3 Is this proposal intended to be implemented by local agencies that have a statutory duty to impact assess policies? If so, what monitoring requirements are you placing on that agency?
N/A

8. Publish Assessment Results

8.1 What form will the publication of the impact assessment take?
N/A

ÖZGEÇMİŞ

Elif Gökşen 1988 yılında Lefkoşa’da doğmuştur. İlk, orta ve lise eğitimini Ankara Özel Tevfik Fikret Lisesi’nde tamamlamıştır. 2010 senesi’nde Bilkent Üniversitesi Hukuk Fakültesi’nden onur öğrencisi olarak mezun olmuştur. 2012-2013 eğitim yılında British Council Chevening Bursu kapsamında London School of Economics and Political Science Üniversitesi’nde yüksek lisans yapmıştır.

Elif Gökşen’in Suç ve Ceza Dergisi’nin Şubat 2012 basımında “Amerika Birleşik Devletleri’nde Organize Suçluluk” isimli bir makalesi ve Köksal Bayraktar’a Armağan kitabında “Dünya Çapında Jüri Sistemleri” (Valerie P. Hans) adlı makale tercümesi bulunmaktadır.

TEZ ONAY SAYFASI

Üniversite	Galatasaray Üniversitesi
Enstitü	Sosyal Bilimler Enstitüsü
Adı Soyadı	Elif Gökşen
Tez Başlığı	Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri
Savunma Tarihi	13 Mayıs 2014
Danışmanı	Doç. Dr. Ümit Kocasakal

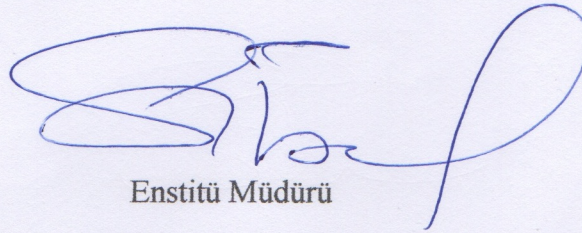
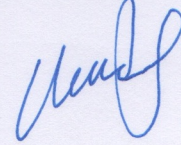
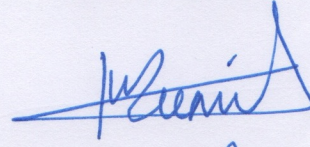
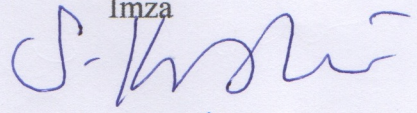
JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı
Prof. Dr. Serap KESKİN KIZIROĞLU

Doç. Dr. Ümit KOCASAKAL

Doç. Dr. Vesile Sonay EVİK

İmza



Enstitü Müdürü

Prof. Dr. Sibel YAMAK