

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

CEZA MUHAKEMESİNDE DİJİTAL DELİLLER

YÜKSEK LİSANS TEZİ

Uğur KAYNAKÇIOĞLU

Tez Danışmanı: Doç. Dr. Vesile Sonay EVİK

HAZİRAN 2015

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

CEZA MUHAKEMESİNDE DİJİTAL DELİLLER

YÜKSEK LİSANS TEZİ

Uğur KAYNAKÇIOĞLU

Tez Danışmanı: Doç. Dr. Vesile Sonay EVİK

HAZİRAN 2015

ÖNSÖZ

Teknolojinin gelişerek insan hayatına farklı yönlerden etki etmesiyle birlikte, hayatın kurallarını düzenleyen hukuk sistemi de bu gelişime ayak uydurmak zorunda kalmaktadır.

Bilgisayarın icadı ile başlayan süreç sonunda, bilgisayar hayatın her alanında kullanılan, vazgeçilmez bir aygıt halini almıştır. Bu nedenle, bilgisayarın işlemlerinin temelinde yer alan dijital veriler de yaygınlık kazanmışlardır. Hatta dijital veriler, getirdikleri kolaylıklar ve gelişimleri nedeniyle bilgisayarların dışındaki aygıtlarda da kullanılır hale gelmişlerdir. Dolayısıyla dijital veriler, artık hemen hemen tüm bilişim alanı işlemlerinin temelini oluşturmaktadırlar.

Dijital verilerin yaygınlığının bu kadar artması ile bu verilere yeterince hazır olmayan hukuk açısından bazı soru işaretleri ortaya çıkmıştır. Bu konuya ilişkin hukukun her alanında ihtiyaç duyulan yeni düzenlemelerin, ceza hukuku alanında da, yapılması gereği ortadadır. Bu konuda önceden yapılan ceza hukuku düzenlemelerinin yetersizliği sonucunda özellikle temel hak ve özgürlüklere müdahale açısından birçok problem ve bu problemler neticesinde de hak ihlalleri ortaya çıkmıştır. Ancak dijital delillerin uluslararası yaygınlık gösteren yapıları gereği, tüm bu problemlerin çözümü de sadece ulusal değil uluslararası kararlılık gerektirmektedir.

Ceza Muhakemesinde Dijital Deliller başlıklı bu çalışmada dijital verilerin ceza muhakemesinde delil olarak kullanımı ele alınacaktır. Çalışmada öncelikle ceza muhakemesi hukukunda delil teorisi ve dijital deliller genel olarak ortaya konmuştur. Böylece dijital delilin kapsamı, özellikleri ve elde edilmesinden hükme konu edilmesine kadar geçen süreçteki yeri anlatılmıştır. Bu bölümde ayrıca adli bilişime ilişkin de bazı bilgiler verilmiştir. Böylece dijital delil kavramı açıklığa kavuşturulurken, dijital delillerin delil teorisi içerisinde alacakları yer de belirlenmiş olacaktır. Daha sonra ise mevcut hukuki düzenlemeler ve mahkeme kararları içerisinde dijital delillerin nasıl yer buldukları incelenmiş, en son olarak da giderilmesi gereken bazı temel eksikler ortaya konmuştur.

Bu noktada öncelikle çalışmanın yapılması sürecinde bana değerli görüşleri ile katkıda bulunan tez danışmanım Doç. Dr. Vesile Sonay Evik'e verdiği desteklerinden dolayı teşekkürlerimi sunarım.

Beni fikri hür, vicdanı hür, irfanı hür bir şekilde yetiştiren eğitim hayatım boyunca sahip olduğum tüm öğretmenlerime, bir hukukçu olma yolunda verdikleri ile desteğini sadece eğitim sürecinde değil mezuniyet sonrası da her anımda hissettiğim Koç Üniversitesi Hukuk Fakültesi'nin her bir üyesine teşekkürü borç bilirim. Akademisyenliğe olan ilgime sadece hukukçulukları ile değil kişilikleri ile de etki eden ve hiçbir zaman değerli görüşlerini benimle paylaşmaktan kaçınmayan

Prof. Dr. Nur Centel, Doç. Dr. Ayfer Uyanık Çavuşoğlu ve Yrd. Doç. Dr. Murat Önok'a da teşekkür ederim.

Galatasaray Üniversitesi'nde yüksek lisans eğitimine başladığım andan itibaren desteğini ve değerli tavsiyelerini benden asla esirgemeyen değerli dekanımız Prof. Dr. Necmi Yüzbaşıoğlu'na teşekkür ederim. Yine Galatasaray Üniversitesi Kamu Hukuku Bölümü'nde yüksek lisans yapma şansını bana tanıyan Doç. Dr. Ümit Kocasakal, Doç. Dr. Şule Özsoy Boyunsuz ve Prof. Dr. Ahmet Ulvi Türkbağ'a minnettarım.

Ayrıca geç tanıştığım ancak bir abim olarak gördüğüm, bana çalışmalarım sırasında da yardımcı olan ve her konuda örnek bir insan olan Yrd. Doç. Murat Volkan Dülger'e de müteşekkirim.

Ayrıca çalışmanın aldığı süre sırasınca beni sabırla bekleyerek belki de çalışmanın bu kadar gelişmesinin görünmeyen kahramanları olan Kocaeli Üniversitesi Milletlerarası Hukuk Anabilim Dalı Başkanı Prof. Dr. Samir Salha ve çalışma arkadaşlarım Yrd. Doç. Dr. Ömer Faruk Direk ve Arş. Gör. Murat Esmer de teşekkürü hak etmektedirler.

Gününün çoğu zamanını kütüphanelerde geçirdiği bir süreç içerisinde beni verdiği tavsiyelerle yalnız bırakmayan ve belki de tezin son halini almasını sağlayan Ali Ergin Çelebi'ye de teşekkür etmek isterim.

Son olarak bana hayatım boyunca gereken her tür desteği veren ve beni yetiştirerek bugünlere getiren geniş aileme minnettarlığımı sunmak isterim. Annem Şenim Kaynakçioğlu, babam Batuhan Kaynakçioğlu, kardeşim Duygu Kaynakçioğlu, kardeşim Özgür Sayer, anneannem Şükran Aktan, dedem Prof. Dr. Nihat Aktan, teyzem Gamze Sayer, eniştem Doç. Dr. Sami Sayer ile rahmetli babaannem Nahide Kaynakçioğlu ve rahmetli dedem Senih Kaynakçioğlu bu çalışma aslında sizin eserinizdir.

Bu çalışmayı, Türkiye'nin farklı coğrafyalarında görevi dâhilinde ceza muhakemesi hukukunu doğru şekilde uygulamaya çalışan ve torununun da kendisi gibi bir hukukçu olduğunu göremeden vefat eden Cumhuriyet Savcısı Senih Kaynakçioğlu'na ve hukukun üstünlüğünü hakim kılmaya çalışan tüm hukukçulara adıyorum.

Arş. Gör. Uğur KAYNAKÇIOĞLU
Galatasaray Üniversitesi Hukuk Fakültesi
Beşiktaş / İSTANBUL 2015

İÇİNDEKİLER

ÖNSÖZ	ii
İÇİNDEKİLER	iv
KISALTMALAR	vii
RÉSUMÉ	ix
ABSTRACT	xiv
ÖZET	xviii
GİRİŞ	1
BİRİNCİ BÖLÜM: CEZA MUHAKEMESİNDE DELİL TEORİSİ VE DİJİTAL DELİLLERİN YERİ	4
I. Delilin ve ispat sistemlerinin tarihçesi	6
A. İlkel ispat sistemi	6
B. İnanca dayalı ispat sistemi	7
C. Akılcı ispat sistemleri	8
1. Kanuni ispat sistemi	9
2. Vicdani ispat sistemi	10
3. Bilimsel ispat sistemi	12
II. Delil ve ispat kavramları	13
A. Delil kavramı	13
B. İspat kavramı	17
1. İspatın konusu	19
2. İspat külfeti	20
III. Dijital delil kavramı	21
A. Dijital delil – elektronik delil kavramlarının benzerlikleri ve farkları	24
1. Elektronik kavramı	24
2. Analog kavramı	25
3. Dijital kavramı	25
4. Değerlendirme	25
B. Veri kavramı	28
C. Bilişim kavramı	30
IV. Dijital delillerin özellikleri	32
A. Delillerin genel özellikleri açısından	33

1. Hukuka uygunluk	33
2. Gerçekçilik	35
3. Akla uygunluk (Rasyonellik)	35
4. Olayı temsil edicilik (Maksada elverişlilik)	35
5. İspat bakımından önemli olmak	36
6. Müştereklik	36
7. Sağlamlık ve güvenilirlik	37
8. Elde edilebilirlik	37
B. Dijital delillerin kendilerine has özellikleri	37
1. Gizli yapıda bulunma	37
2. Kopyalanabilir olma	39
3. Kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olma	39
4. Yaygın ve uluslararası nitelikte olma	40
5. Aidiyet tespitinin zorluğu	40
6. Gelişim ve değişim gösterebilir olma	41
V. Dijital delil çeşitleri	41
VI. Dijital delillerin delil teorisine göre yeri	42
VII. Dijital delillerin elde edilmesi ve ispat gücü	46
A. Genel olarak delil elde etme süreci ve uygulamaları	46
1. Beyan delillerinin elde edilmesi	48
2. Belge ve belirti delillerinin elde edilmesi	49
B. Dijital delillerin elde edilmesi	50
1. Adli bilişim	52
2. Adli bilişimin evreleri	54
a. Toplama	55
b. İnceleme	57
c. Analiz	58
d. Raporlama	58
C. Dijital delillerin ispat gücü	59
İKİNCİ BÖLÜM: DİJİTAL DELİLLERE YÖNELİK HUKUKİ DÜZENLEMELER	61
I. Uluslararası hukukta dijital delillere ilişkin düzenlemeler	62
A. Birleşmiş Milletler	63
B. Avrupa Birliği	69
C. Avrupa Konseyi	73
II. Bazı yabancı hukuk düzenlerinde dijital delillere ilişkin düzenlemeler	79
A. Almanya	79
B. Amerika Birleşik Devletleri	83

C. Avustralya	89
D. Belçika	92
E. Birleşik Krallık	93
F. Çin	96
G. Endonezya	97
H. Fransa	98
I. Hollanda	101
J. İsviçre	103
K. Slovenya	106
III. Türk hukukunda dijital delillere ilişkin düzenlemeler	108
A. CMK kapsamındaki düzenlemeler	108
B. Diğer düzenlemeler	118
ÜÇÜNCÜ BÖLÜM: UYGULAMADA DİJİTAL DELİLLER VE CEZA	
MUHAKEMESİ BAKIMINDAN KONUYLA İLGİLİ ÇÖZÜM ÖNERİLERİ ...	
I. Avrupa İnsan Hakları Mahkemesi kararları	125
II. Avrupa Birliği Adalet Divanı kararları	133
III. Türkiye'deki mahkeme kararları	140
A. Balyoz güvenlik harekât planı davası	140
B. Askeri casusluk ve şantaj davası	155
C. Diğer kararlar	162
IV. Ceza muhakemesi hukuku bakımından konuyla ilgili çözüm önerileri	166
A. Uluslararası uyum ve işbirliğinin artırılması	166
B. Yeni hukuki düzenlemeler yapılması	168
1. CMK hükümlerinin SSS ile uyumlandırılması	169
2. Kişisel verilerin korunmasına ilişkin kanunun çıkartılması	172
3. Adli bilirkişilik kurumu kurulması ve bu konuda kanun çıkartılması	172
C. Dijital delillere ilişkin (hem CMK hem de SSS içerisinde yer almayan) bazı yeni düzenlemelerin uygulanabilirliğinin tartışılması	174
D. Adli birimlerin konuyla ilgili eğitimi	176
SONUÇ	180
KAYNAKÇA	183
ÖZGEÇMİŞ	195

KISALTMALAR

AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
ACPO	: Association of Chief Police Officers
a.g.e.	: adı geçen eser
AIHM	: Avrupa İnsan Hakları Mahkemesi
AIHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
akt.	: aktaran
alm.	: almanca
AÖAY	: Adli ve Önleme Aramaları Yönetmeliđi
AYM	: Anayasa Mahkemesi
bkz.	: bakınız
BM	: Birleşmiş Milletler
BÜPF	: Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BSTS	: Bilim ve Sanat Terimleri Sözlüğü
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CCA	: The Commonwealth's Crimes Act 1914
CD	: Ceza Dairesi
CDC	: Code d'instruction criminelle
CMA	: Computer Misuse Act
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
CMUK	: 1412 Ceza Muhakemeleri Usulü Kanunu
CPP	: Code de Procédure Pénale
CPPS	: Code de procédure pénale suisse
ÇASÖMK	: 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu
çev.	: çeviren
dn.	: dipnot
E.	: Esas numarası
ECPA	: Electronic Communications Privacy Act
fr.	: fransızca
FRE	: Federal Rules of Evidence
HMK	: 6100 sayılı Hukuk Muhakemeleri Kanunu
HSYK	: Hâkimler ve Savcılar Yüksek Kurulu
HUDOC	: Human Rights Documentation
HUMK	: 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu
INTERPOL	: Uluslararası Polis Teşkilatı
ing.	: ingilizce
K.	: Karar numarası
KUHAP	: Kitab Undang-Undang Hukum Acara Pidana
lat.	: latince

LSCPT	: Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
p.	: paragraf
PACE	: Police and Criminal Evidence Act
PVSK	: 2559 sayılı Polis Vazife Salahiyet Kanunu
RIPA	: Regulation of Investigatory Powers Act
s.	: sayfa
ss.	: sayfaları arası
SSS	: Avrupa Konseyi Siber Suçlar Sözleşmesi
SStPO	: Schweizerische Strafprozessordnung
StPO	: Strafprozessordnung
T.	: Tarih
TCK	: 5237 sayılı Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TIA	: Telecommunications (Interception and Access) Act
TİB	: Telekomünikasyon İletişim Başkanlığı
UYAP	: Ulusal Yargı Ağı Bilişim Sistemi
vd.	: ve devamı
vs.	: vesaire
WS	: Wetboek van Strafvordering
ZKP	: Zakon o kazenskem postopku

RÉSUMÉ

Le contenu de cette thèse, ayant comme titre les preuves numériques en procédure pénale, est préparé pour identifier où se trouvent les preuves qui possèdent les qualités des preuves numériques dans le système des procédures pénales et quelles sortes d'insuffisances il y a à propos de ce sujet dans les conditions courantes. En fait, on peut facilement indiquer que les preuves numériques sont devenues une partie indispensable du contenu des preuves qui sont utilisées comme un instrument permettant d'accéder à la réalité matérielle dans le système de procédure pénale, en considérant le monde passant par une ère numérique dans nos jours. Même si ce sujet est recherché dans le contexte de différentes discussions, il y a toujours des nouvelles considérations qui peuvent être examinés. Pour cette raison, cette étude contient non seulement des informations et des évaluations qui sont contestées et qui sont déterminées avec le temps, mais aussi des nouvelles informations et des évaluations qui viennent de se présenter. En outre, même si le fait que ce sujet contient une partie concernant le domaine informatique le rend interdisciplinaire, il ne doit pas être oublié que le contexte de cette étude est limitée à identifier où se trouve la notion des preuves numériques dans les procédures pénales. Les informations nécessaires qui se trouvent dans le domaine informatique sont utilisées et les détails inutiles sont évités. L'étude légale comprend la révision des dernières situations des législations nationales et internationales, ainsi que l'évaluation des décisions judiciaires prises à propos des réglementations concernées et la détermination des développements légaux qui sont attendus dans l'avenir dans ce sujet.

Dans la première section de l'étude, il est mentionné premièrement du développement des systèmes de preuves et de justification et leurs transformations en preuves numériques dans les procédures pénales. Ici, on a mentionné des systèmes rationalistes qui sont légaux, consciencieux et basés sur une justification scientifique, qui sont venues après les systèmes de justification primitifs et dogmatiques. On peut dire que dans la plupart des systèmes de procédure pénale de nos jours, les principes du système de justification consciencieux et de la liberté de preuve sont acceptés. Par contre, on voit que le système de justification consciencieux commence à être vaincu par le pouvoir de justification des preuves qui sont obtenues grâce à des méthodes scientifiques en particulier. Les preuves numériques figurent juste sur la fine limite qui se trouve entre ces deux systèmes.

A la suite de cette introduction historique, les concepts qui forment le concept de preuve numérique, c'est-à-dire la numérisation, la preuve et la justification en rapport avec les preuves, sont examinés et le contenu réel du sujet est identifié. Cette identification peut être indiquée comme la place où la fondation de cette étude est jetée. En conséquence, cette identification comprend ainsi ce que désigne la preuve numérique, ces différences avec le concept de preuve électronique, sa connexion avec la science informatique et le fait qu'elle est formée des données qui sont des valeurs fondamentales légales.

Cette identification est en même temps la première étape pour placer les preuves numériques dans la théorie générale de preuves. Les caractéristiques et les types de preuves numériques sont montrés après cette première étape. Une analyse des aspects similaires et différents des preuves numériques et des preuves classiques est réalisée spécialement quand les propriétés des preuves numériques sont examinées. À ce point, on a vu que les preuves numériques possèdent des caractéristiques particulières comme leurs caractères abstraits (se trouver dans une forme cachée), leurs propriétés d'être copiées, d'être facilement changées, détruites et supprimées, d'être répandue et d'être internationale, leurs difficultés d'identifier leur propriétaire et leurs pouvoirs de se développer et de changer. En outre, les types de preuves numériques sont comptés et le contenu du concept de preuve numérique est bien concrétisé. Même s'il est conclu dans cette section que la source principale des preuves numériques est l'ordinateur qui utilise intensivement la technologie numérique, il est aussi constaté que des dispositifs électroniques autres que l'ordinateur peuvent aussi fournir des preuves numériques dans les conditions de nos jours dans la vie quotidienne.

Après toutes ces déterminations, il est devenu plus facile de placer le concept de preuve numérique dans la théorie de preuve. Une opération de regroupement pour les preuves numériques est faite dans cette théorie de preuve qui sépare les preuves en tant que déclaration, document et signe. Quand tous les éléments précédemment identifiés sont tenus en compte lors de ce regroupement, on peut dire que les preuves numériques doivent se placer entre les preuves de signe. Cette détermination est importante pour les sujets d'obtention des preuves et leurs pouvoirs de justification qui sont les sujets qui affectent l'application des procédures pénales probablement le plus. La façon d'obtention et le pouvoir de justification changent ainsi en fonction du type de preuve. En outre, comme ces processus se reflètent directement à l'application, ils deviennent les sujets les plus déterminants au point de vue légal.

A ce point, nous voyons qu'en raison de leurs caractères particuliers, on s'adresse à des opérations techniques spéciales qui sont nommées comme informatique légale pour l'obtention des preuves numériques. Sans se noyer dans tous les détails techniques de l'informatique légale, nous avons mis l'accent sur comment se réalise cette chaîne d'opérations spéciales au sujet de l'informatique légale. Le sujet d'informatique légale est ainsi un sujet de thèse individuel pour les personnes qui s'occupent des domaines d'informatique ou d'électronique. Pour cette raison, nous nous sommes contentés de donner seulement des informations courtes et principales qui peuvent être légalement importantes. Après avoir considéré le sujet de l'informatique légale, nous avons parlé du pouvoir de justification des preuves numériques. On a désigné en ce sujet que le pouvoir de justification des preuves numériques valorisées dans le contexte des preuves de signe est le même que les signes et que les opérations d'informatique légale qui leur permettent d'être obtenu spécialement doivent être contrôlées en supplément.

Après la première section qui a un contenu techniquement et théoriquement pesant, les réglementations nationales et internationales qui concernent les preuves numériques sont examinées. Le droit international, le droit étranger et le droit turc sont considérés séparément lorsque ces réglementations sont examinées. De cette manière, tous les systèmes peuvent être vus plus facilement et séparément l'un de

l'autre. Il n'est ainsi toujours pas possible de dire qu'il y a un accord entre les preuves numériques, selon des différentes matières.

Les documents qui attirent l'attention lorsque le droit international est examiné sont généralement préparés par des associations internationales différentes. L'idée de faire une réglementation légale pour les crimes et les attaques effectuées en utilisant la technologie informatique développante est considérée comme base pour la création de tous ces documents. Entre les documents qui sont préparés dans le contexte de cette idée par les États Unis, où la technologie informatique s'est développée premièrement, ceux qui sont légalement importants pour la Turquie sont examinés en détail dans cette étude. Des exemples de ces types de documents sont le Manuel Stratégique des Nations Unies sur la Prévention et le Contrôle de la Criminalité Informatique et la Convention sur la Cybercriminalité du Conseil de l'Europe. Entre ces deux documents, l'importance du premier, c'est que c'est l'étude la plus approfondie dans la structure des Nations Unies au sujet des effets des preuves numériques sur les procédures pénales et que les déterminations prises ici ont jeté la fondation de ce sujet dans le domaine du droit international. L'importance du deuxième, c'est que c'est une convention qui est acceptée par une large participation dans l'échelle internationale. En outre, nous avons aussi mentionné des réglementations de l'Union Européenne en ce sujet en tenant compte que la Turquie est un pays qui est candidat à faire partie de l'Union Européenne.

Même s'il y a un volume d'information illimité qui peut être écrit dans la section montrant les réglementations concernant les preuves numériques dans le droit étranger, une restriction est faite et certains pays sont choisis. Non seulement les pays ayant des traditions de droit pénal différents, mais aussi les pays ayant des traditions de droit pénal similaires sont choisis dans cette sélection. Ça sera ainsi possible de faire une comparaison entre les différents systèmes et de voir les différences entre les réglementations différentes ayant des systèmes similaires.

Dans la deuxième section, il est conclu que ni les réglementations internationales, ni les réglementations nationales n'ont pu encore atteindre la perfection dans ce sujet. Par contre, la Convention sur la Cybercriminalité peut être acceptée comme un bon point d'origine parmi ces réglementations. Les données informatiques sont acceptées comme des éléments principaux légaux dans la convention. En outre, les précautions qui sont situées dans la convention et qui sont nommées en tant que précautions de protection informatique et les articles destinés à offrir une cohérence internationale attirent l'attention.

En outre, après avoir examiné toutes ces réglementations, c'est devenu possible de diviser les réglementations légales concernant les preuves numériques, selon leurs sujets. Quand les sujets qui sont dans ce contexte sont examinés, les domaines comme les précautions de protection informatique et la protection des données attirent l'attention.

Ensuite, les réglementations faites à propos des preuves numériques en Turquie sont examinées. Même s'il est constaté que les réglementations en Turquie se sont modernisées dans les termes des précautions nommées en tant que précautions de protection informatique, référées dans la Convention sur la Cybercriminalité, le fait que ces réglementations sont faites sans soins et seulement pour être faite attire l'attention. Ainsi, il est constaté que les réglementations

possèdent certaines bases, mais que ces bases ne sont pas suffisamment solides, donc il est identifié que ces réglementations possèdent des insuffisances. Les réglementations internationales dans ce sujet et les réglementations nationales autres que celle de la Turquie ont aidé à faire cette identification.

Dans la dernière section de l'étude, les décisions de justice qui peuvent affecter directement les preuves numériques, les réglementations qui sont nécessaires et l'avenir des preuves numériques sont prisent en considération. Nous avons spécialement fait attention à l'ordre chronologique lorsque nous avons examiné les décisions de justice et cela était important pour voir les différences qui se sont créés avec le temps dans les évaluations des tribunaux. Ici, au lieu de faire une étude en analysant une par une toutes les décisions de justice du monde, les décisions de justice qui peuvent être importantes pour la Turquie sont présentées au premier plan. Pour cette raison, la partie concernant les décisions de justice est limitée avec les décisions du CEDH, du CJUE et de la Cour Suprême.

Il est nécessaire de suivre attentivement les décisions du CEDH pour pouvoir déterminer les violations des droits et les normes minimales dans le cadre de la Convention Européenne des Droits de l'Homme, dans laquelle la Turquie fait partie. Ces décisions contiennent ainsi les solutions des conflits entre les méthodes d'obtention des preuves numériques, qui sont nommées en tant que précautions de protection informatique, et les droits fondamentaux. Il est généralement constaté que ces conflits apparaissent en fonction du droit à la vie privée et du droit à la protection de la propriété. Le suivie régulier des décisions du CEDH du point de vue de la Turquie sera aussi important pour l'évaluation de la législation nationale.

Les décisions du CJUE doivent aussi être attentivement examinées avec le point de vue de la Turquie qui est un pays qui est un pays candidat à faire partie de l'Union Européenne. Il faut remarquer que les décisions du CJUE à propos des preuves numériques sont habituellement au sujet du respect à la vie privée et de la protection des données personnelles dans le contexte de la Charte des Droits Fondamentaux de l'Union Européenne.

Les décisions de la cour suprême sont les décisions qui montrent de la meilleure façon la position de la Turquie à propos des preuves numériques. Nous avons essayé d'inclure à peu près toutes les décisions en ce sujet qui peuvent être accédées au premier instant dans cette étude. Par contre, nous avons mis l'accent sur l'affaire du plan d'opération de sécurité de Balyoz comme elle a occupé vastement l'opinion publique et comme elle a un important contenu à propos des preuves numériques. Il peut être conclu de cela que plus le sujet est appris d'une meilleure façon avec le temps, plus les décisions de la cour suprême sont formées des contenus plus réguliers. Néanmoins, on voit de temps en temps des décisions qui peuvent être l'objet des critiques.

La dernière section de l'étude est la partie complémentaire. L'accent est mis ainsi sur comment ça sera possible de créer le tableau qui se dessine après l'investigation détaillée des réglementations légales et les décisions de justice à propos des preuves numériques, dans le système international et en Turquie. Pour cette raison, cette section est non seulement une partie du sujet, mais aussi une évaluation entière qui contient des suggestions pour l'avenir. La vérité qui résulte des identifications qui sont faites dans ce sujet montre la nécessité d'augmenter la

cohérence et la coopérativité internationale relative aux réglementations à propos des preuves numériques, de changer les réglementations existantes ou de préparer des nouvelles réglementations en Turquie.

ABSTRACT

The scope of this thesis titled digital evidence in criminal procedure is prepared both to determine how the evidence possessing digital evidence characteristic takes place in criminal law, and the deficiencies in this matter regarding current situation. As a matter of fact, we can easily say that the digital evidences in terms of a world going through a digital era, became an essential part of the item evidence which is used as a means to reach the material fact in criminal procedure system. Although this matter has been studied within many different discussions, there are still many points to be studied. Therefore, the study includes both information and assessments matured through discussions in time and some newer information and assessments emerging nearly every other day. Additionally, it must be kept in mind that the scope of this study is limited by the place digital evidence concept takes in criminal law, even if the part of the matter regarding information technologies makes it an interdisciplinary subject. At this point, the necessary information in the information technologies area has been used, so the assessments in this study avoid unnecessary details. In the legal study, as well as studying both current international and national legislations, the court decisions made in terms of the relevant regulations are assessed and the legal developments expected to happen in the field in the future are conveyed.

In the first chapter of the study, the evolution and change of the evidence and proof systems within criminal procedure went through until the present period is addressed. This chapter addresses rational systems based on legal, conscientious and scientific proofs, after the primitive proof systems based on beliefs. We may say that most of the current criminal procedure systems accepts conscientious proof and principle of circumstantial evidence. However, it has become clear that conscientious proof systems are becoming defeated by especially the conclusive force of the evidences obtained through scientific methods. And the digital evidence stands just on the thin line in the middle of these two systems.

After this historical introduction, the scopes of digital, evidence and proof concepts creating the digital evidence concept are analyzed and the real scope of the subject is determined. This determination may be phrased as the foundation of the study. As a matter of fact, this determination includes what digital evidence represents, its difference from electronic evidence, the connection with the information technologies and the fact that it is formed by the data which is a legal core value.

This determination is the first step in the placement of digital evidence in general evidence theory. After this first step, the properties and variations of digital evidences are delivered. Especially during the study of the properties of digital evidences, the similarities and differences of digital evidences from the classical evidences are analyzed. At this point, it has been clear that digital evidences have some characteristics such as intangibility (presence in latent structure),

reproducibility, alterability, perishability, destructibility, its common and international quality, the difficulty of ownership determination and formative structure. In addition, the scope of digital evidence concept is concretized giving the variations of digital evidences. Although this chapter reaches a conclusion that basic sources of digital evidence are gathered on the computers on which digital technology is commonly used, we have seen that other electronic devices that may provide digital evidence are used in current life.

All these determinations help in providing a placement of digital evidence concept in evidence theory. A matching process is conducted within an evidence theory where the evidences are distinguished by statement, documents and indications. During this matching, considering all the matters stated before, we can say that digital evidence should be addressed within indication evidences. These determinations are important in terms of the obtainment of the evidences which probably is the most effective application of criminal procedure and conclusive forces. As a matter of fact, the obtainment form and conclusive force changes per the type of evidence. Besides, these processes are legally the most determinant subjects since they are directly reflected to application.

At this point, because of the characteristics of digital evidences, some special technical processes named computer forensics are used in the obtainment. Within computer forensics, the conduct of these special process sequences are emphasized, without giving too much technical details about computer forensics. As a matter of fact, the subject of computer forensics is a thesis subject for the people interested in computer or electronics fields. Therefore, solely legally important, short and basic information is given in this field. After addressing computer forensics, conclusive force of digital evidences are discussed. In this matter, the fact that the conclusive force of digital evidences considered within indications, and also the necessity to control the computer forensics processes where they are specially obtained is stated.

After the first chapter, which is strong on both technical and theoretical content, national and international legal regulations regarding digital evidences are studied. International law, foreign law and Turkish law are discussed separately during the study of these regulations. Therefore, each system can easily be observed separately. As a matter of fact, it is not possible to say that a complete harmony has been established in the matter of digital evidence.

During the study of international law, it is seen that the prominent documents are prepared by different international organizations. The formation of all these documents are based on the notion that a legal regulation should be made towards the crimes and assaults conducted using the developing information technologies. Among the documents prepared pursuant to this notion, first proposed by USA where computer technology first emerged. However only the ones with legal importance for Turkey are discussed in more details within the study. United Nations Manual on the Prevention and Control of Computer-Related Crime and the Convention on Cybercrime prepared by the Council of Europe may be given as examples of such documents. The first of these two documents is important since it is the most comprehensive study in terms of the effect of digital evidence in criminal procedure within UN and, the foundation of this subject in international law through the determinations made herein. The importance of the other document is that it is a treaty accepted internationally by many countries and Turkey is one of the

signatories. Other than these, considering that Turkey is an applicant country to European Union, the regulations of European Union regarding this subject are also discussed.

Although there are almost unlimited information regarding digital evidence in the foreign laws, only some of the countries are chosen after some restrictions. During this choice, both countries with different criminal law traditions and countries with similar criminal law traditions are chosen. Therefore, it is possible to make comparisons between different systems. Also the differences in the regulations with same systems can be seen.

In the conclusion of the second chapter, it is clear that perfection has not been achieved neither in international nor national regulations regarding this subject. However, among these regulations, Convention on Cybercrime can be accepted as a valuable starting point. The computer data within the treaty is taken as a basis legal value. Other than this, the measures included in the Convention and the articles regarding the assurance of international harmony are also important.

Additionally, it is possible to divide the legal regulations regarding digital evidences into subjects after studying all these regulations. Considering the subjects in this context, measures included in the Convention and protection of personal data stand out.

Thereafter, the regulations made in Turkey regarding digital evidences are studied. Although we can see that the regulations in Turkey catch up with the era in terms of the measures included in the Convention on Cybercrime, these regulations are prepared imprecisely and in a such a way that just the presence of these regulations would be enough. Namely, it has been determined that these regulations have some certain basics but these basics does not have strong foundations and therefore there are deficiencies in these regulations. What made this determination easier is the international and national regulations in the same subject.

The last chapter of the study discusses the court decisions that may directly affect digital evidences and the regulations that need to be made, as well as the future of digital evidences. During the analysis of court decisions, considering choronological order became especially important in seeing the differences occurred in the assessments of courts in time. Also in this chapter, the court decisions that may be legally important for Turkey are highlighted rather than preparing a study that scans all the court decisions in the world. Therefore, the court decisions part is limited to ECHR, CJEU and Supreme Court of Appeals decisions.

ECHR decisions should be closely followed in terms of determining violation of rights and minimum standards within ECHR, in which Turkey is an affiliated party. As a matter of fact, these decisions generally include the conflicting points of digital evidence obtainment methods and fundamental rights. These conflicting points generally emerge from the right of privacy and the right of protection of ownership. For Turkey, it would be beneficial to follow the ECHR decisions for the development of domestic legislations.

CJEU decisions should also be carefully followed by Turkey, an applicant to EU. The decisions CJEU made in terms of digital evidence are mostly about respect to private life and protection of personal data within the scope of Charter Of Fundamental Rights Of The European Union.

The decisions of Supreme Court of Appeals are the decisions that best demonstrates the position on Turkey in terms of digital evidences. Nearly all decisions that can be reached from the very beginning are included in the study. However, due to the mass media coverage and the essential content regarding digital evidences, "Balyoz" security operation plan is discussed in more detail. The conclusion herein shows that the decisions made by the Supreme Court of Appeals has starts to include more proper content through better understanding of the subject in time. However, some decisions that may arise criticism are made from time to time.

The last part of the study is the complementary part. As a matter of fact, after the detailed examination of legal regulations and court decisions regarding digital evidences, the forthcoming state can be formed both in international system and Turkey. Therefore, this part is not a direct part of the subject and includes a whole assessment about prospective suggestions. At last, the fact as a result of the determinations in this subject shows the necessity of an alteration of the current regulations in Turkey or making new ones as well as enhancement of international harmony and cooperation in terms of regulations regarding digital evidences.

ÖZET

Ceza muhakemesinde dijital deliller başlıklı bu tezin içeriği; dijital delil niteliğini haiz delillerin, ceza muhakemesi sisteminde ne şekilde yer bulduğuna ve mevcut durumda bu konuda ne gibi eksikliklerin bulunduğuna yönelik olarak hazırlanmıştır. Nitekim günümüzde dijital çağı yaşayan bir dünya açısından dijital delillerin, ceza muhakemesi sisteminde maddi gerçeğe ulaşma vasıtası olarak kullanılan delil unsurunun vazgeçilmez bir parçası haline geldiği rahatlıkla söylenebilir. Bu konu daha önce pek çok farklı tartışma kapsamında incelenmiş de, konuyla ilgili incelenecek yeni hususlar hâlâ bulunmaktadır. Bu nedenle çalışmanın içerisinde hem zamanla tartışılarak oturmuş bulunan bilgiler ve değerlendirmeler, hem de belki gün aşırı ortaya çıkan bazı daha yeni bilgiler ve değerlendirmeler bulunmaktadır. Ayrıca konunun bilişim alanını ilgilendiren yanının bulunması konuyu disiplinler arası bir hale getirir de, çalışmanın kapsamının dijital delil kavramının ceza hukuku kapsamında nasıl yer bulduğu ile sınırlı olduğu unutulmamalıdır. Bu noktada bilişim alanına giren gerekli bilgilerin kullanılarak, gereksiz detaylardan kaçınılması yoluna gidilmiştir. Yapılan hukuki incelemede ise gerek uluslararası gerekse ulusal mevzuatların son durumlarının incelenmesinin yanı sıra, ilgili düzenlemeler konusunda alınan mahkeme kararlarının değerlendirilmesi ve bu alanda gelecekte gerçekleşmesi beklenen hukuki gelişmelerin iletilmesi yolu kullanılmıştır.

Çalışmanın ilk bölümünde öncelikle, ceza muhakemesi içerisinde delil ve ispat sistemlerinin dijital delillere gelinen sürece kadar geçirdiği gelişim ve değişimden bahsedilmiştir. Burada ilkel ve inanca dayalı ispat sistemlerinin ardından gelen kanuni, vicdani ve bilimsel ispata dayalı akılcı sistemlerden bahsedilmiştir. Günümüz ceza muhakemesi sistemlerinin çoğunda vicdani ispat sistemi ile delil serbestisi ilkesinin kabul edildiği söylenebilir. Ancak vicdani ispat sisteminin özellikle bilimsel yöntemlerle elde edilen delillerin ispat gücüne yenik düşmeye başladığı görülmektedir. İşte dijital deliller de tam bu iki sistem arasındaki ince çizgide bulunmaktadır.

Bu tarihsel girizgâhtan sonra dijital delil kavramını oluşturan dijital, delil ve delile bağlı olarak ispat kavramlarının içeriği incelenerek aslında konunun gerçekten içerdiği kapsamın bir tespiti yapılmıştır. Bu tespit belki de çalışmanın temelinin atıldığı yer olarak ifade edilebilir. Nitekim dijital delilin neyi ifade ettiği, elektronik delil kavramı ile farklılığı, bilişim bilimi ile bağlantısı ve hukuki bir çekirdek değer olan verilerden oluştuğu hep bu tespitin içerisinde yer almaktadır.

Bu tespit aynı zamanda dijital delillerin delil teorisi içerisine oturtulması yolundaki ilk adım olmuştur. Bu ilk adımdan sonra ise, dijital delillerin özellikleri ve çeşitleri ortaya konulmuştur. Özellikle dijital delillerin özellikleri incelenirken, dijital delillerin klasik deliller ile benzer ve farklı yönlerinin bir analizi yapılmıştır. Bu noktada dijital delillerin kendilerine has özellikleri olan gizli yapıda bulunma, kopyalanabilir olma, kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olma,

yaygın ve uluslararası nitelikte olma, aidiyet tespitinin zorluğu ile gelişim ve değişim gösterebilir olma unsurlarına sahip olduğu görülmüştür. Ayrıca dijital delil çeşitleri de sayılarak dijital delil kavramının içeriği iyice somutlaştırılmıştır. Bu bölümde dijital delillerin temel kaynağının dijital teknolojinin yoğun olarak kullanıldığı bilgisayar üzerinde toplandığı sonucu ortaya çıksa da, günümüz koşullarında bilgisayar dışında dijital delil sağlayacak başka elektronik aygıtların da yaşam içerisinde bulunduğu görülmüştür.

Tüm bu tespitlerden sonra dijital delil kavramını delil teorisi içerisine oturtmak daha kolay hale gelmiştir. Delillerin beyan, belge ve belirti olarak ayrımının yapıldığı bir delil teorisi içerisinde dijital deliller açısından bir eşleştirme işlemi yapılmıştır. Bu eşleştirme sırasında daha önce belirtilmiş tüm hususlar göz önünde bulundurulduğunda, dijital delillerin belirti delilleri içerisinde yer almaları gerektiği söylenebilir. Bu belirleme, ceza muhakemesi uygulamasını belki de en çok etkileyen delillerin elde edilmesi ve ispat güçleri konuları açısından önemli olmaktadır. Nitekim delilin çeşidine göre elde edilme şekli ve ispat gücü değişmektedir. Ayrıca bu süreçler doğrudan uygulamaya yansındıkları için hukuki açıdan en belirleyici konular olmaktadır.

Bu noktada dijital delillerin kendilerine has özellikleri nedeniyle, elde edilmelerinde adli bilişim adı verilen bazı özel teknik işlemlerin aracılığına başvurulduğu görülmektedir. Adli bilişim konusu içerisinde adli bilişimin tüm teknik detaylarında boğulmadan, işbu özel işlemler silsilesinin ne şekilde yürüdüğü üzerinde durulmuştur. Nitekim adli bilişim konusu bilgisayar ya da elektronik alanıyla ilgilenen kişiler için başlı başına bir tez konusudur. Bu nedenle sadece hukukten önemli olacak kısa ve temel bilgilerin verilmesi ile yetinilmiştir. Adli bilişim konusu ele alındıktan sonra dijital delillerin ispat gücünden bahsedilmiştir. Bu konuda ise belirti delili kapsamında değerlendirilen dijital delillerin ispat gücünün belirtiler ile aynı güçte olduğu ve buna ek olarak özel şekilde elde edildikleri adli bilişim işlemlerinin de kontrolünün gerekliliği belirtilmiştir.

Hem teknik hem de teorik içeriği ağır olan birinci bölümden sonra dijital delilleri ilgilendiren uluslararası ve ulusal hukuki düzenlemeler incelenmektedir. İşbu düzenlemeler incelenirken, uluslararası hukuk, yabancı hukuk ve Türk hukuku ayrı bir şekilde ele alınmıştır. Böylece her bir sistem birbirinden ayrı olarak daha rahat olarak görülebilecek duruma gelmiştir. Nitekim dijital deliller konusunda pek çok farklı husus açısından hâlâ tam bir uyumun sağlandığını söylemek mümkün değildir.

Uluslararası hukuk incelenirken dikkat çeken belgeler genellikle farklı uluslararası örgütler tarafından hazırlanmıştır. Tüm bu belgelerin oluşturulmasında, gelişen bilişim teknolojisi kullanılarak işlenen suçlara ve yapılan saldırılara yönelik hukuki düzenleme yapılması fikri temel alınmıştır. İlk olarak bilgisayar teknolojisinin ortaya çıktığı ABD tarafından ortaya atılan bu fikir çerçevesinde hazırlanan belgelerin Türkiye açısından hukuki önemi yüksek olanları, çalışma içerisinde daha detaylı bir şekilde incelenmiştir. Bu belgelere örnek olarak Birleşmiş Milletler Bilgisayarla Gerçekleştirilen Suçların Önlenmesi ve Kontrolüne İlişkin Strateji Metni ile Avrupa Konseyi tarafından hazırlanmış olan Siber Suçlar Sözleşmesi gösterilebilir. Bu iki belgeden ilkinin önemi, BM bünyesinde dijital delillerin ceza muhakemesine etkisi bakımından yapılmış en kapsamlı çalışma olması ile burada yapılan tespitler aracılığıyla konunun uluslararası hukuk açısından temelini atmasıdır. Diğerinin önemi ise, bu konuda uluslararası çapta geniş katılımlı

kabul gören iyi bir sözleşme olması ile Türkiye'nin de bu sözleşmeye taraf olup onaylamış durumda bulunmasıdır. Bunlar dışında Türkiye'nin Avrupa Birliği üyeliğine aday bir ülke olması göz önünde bulundurularak, Avrupa Birliği'nin konuyla ilgili düzenlemeleri üzerinde de durulmuştur.

Yabancı hukuklar içerisinde dijital delillere yönelik düzenlemelerin ortaya konulduğu bölüm hakkında ise yazılabilecek neredeyse sınırsız hacimde bilgi bulunsa da, bu konuda bir kısıtlama yapılarak belli ülkeler seçilmiştir. Bu seçim yapılırken birbirinden farklı ceza hukuku geleneği bulunan ülkelerin yanı sıra birbirlerine benzer ceza hukuku geleneği bulunan ülkeler de seçilmiştir. Böylece hem farklı sistemler arasında bir karşılaştırma yapılabilecek, hem de aynı sisteme sahip farklı düzenlemeler içerisinde bulunan farklar da görülebilecektir.

Gerçi ikinci bölümde sonuç olarak, bu konuda gerek uluslararası gerekse ulusal düzenlemelerin hiçbirinin henüz mükemmeliyeti yakalayamadığı görülmektedir. Ancak bu düzenlemeler içerisinde Siber Suçlar Sözleşmesi iyi bir başlangıç noktası olarak kabul edilebilir. Sözleşme içerisinde bilgisayar verisi hukuki değer olarak temel alınmaktadır. Bunun dışında yine Sözleşme içerisinde yer alan ve bilişim koruma önlemleri olarak da adlandırılan tedbirler ile uluslararası uyumun sağlanmasına yönelik maddeler dikkat çekmektedir.

Bunlara ek olarak, tüm bu düzenlemeleri inceledikten sonra dijital delillere ilişkin hukuki düzenlemelerin konulara bölünmesi de mümkün hale gelmiştir. Bu kapsamda bulunan konulara bakılırsa, bilişim koruma tedbirleri ve kişisel verilerin korunması gibi alanlar dikkat çekmektedir.

Daha sonra ise Türkiye'de dijital delillere yönelik yapılmış düzenlemeler incelenmiştir. Bu noktada Türkiye'deki düzenlemelerin özellikle Siber Suçlar Sözleşmesi'nde bahsedilen bilişim koruma önlemleri olarak adlandırılan tedbirler açısından çağrı yakaladığı görülse de, bu düzenlemelerin özensiz bir şekilde ve adeta yeter ki bulunsun havasında yapıldığı dikkat çekmektedir. Yani yapılan düzenlemelerin belli temellerinin bulunduğu, ancak bu temellerin kendilerinin ve üstlerinin sağlam bir şekilde doldurulmadığı, dolayısıyla düzenlemelerde eksikliklerin bulunduğu tespit edilmiştir. Bu tespitini yapılmasını kolaylaştıran ise aynı konuda bulunan uluslararası ve Türk hukuku dışındaki ulusal düzenlemelerdir.

Çalışmanın son bölümünde ise dijital delillere ilişkin doğrudan etki doğurabilecek mahkeme kararları ve yapılması gereken düzenlemeler ile dijital delillerin geleceği ele alınmıştır. Mahkeme kararları incelenirken kronolojik sıraya özellikle dikkat edilmiş; bu husus mahkemelerin zamana göre yaptığı değerlendirmelerde oluşan farklılıkların görülmesi açısından önemli olmuştur. Yine burada da dünyadaki tüm mahkeme kararları tek tek taranarak bir çalışma yapmak yerine, Türkiye açısından hukuki önemi olabilecek mahkeme kararları ön plana çıkartılmıştır. Bu nedenle mahkeme kararları kısmı AİHM, ABAD ve Yargıtay kararları ile sınırlı tutulmuştur.

Türkiye'nin de taraf olduğu AİHS kapsamındaki hak ihlallerini ve asgari standartları belirleme açısından AİHM kararlarının her zaman için dikkatle takip edilmesi gereklidir. Nitekim bu kararlar genel olarak, bilişim koruma tedbirleri olarak da adlandırılan dijital delil elde etme yöntemlerinin temel haklar ile çatıştığı noktaların çözümlerini içermektedir. Genellikle bu çatışan noktaların özel hayatın

gizliliği hakkı ile mülkiyetin korunması hakkı açısından ortaya çıktığı görülmüştür. Özellikle AİHM kararlarının Türkiye açısından düzenli olarak takip edilmesi iç mevzuatın geliştirilmesi yolunda da önemli olacaktır.

ABAD kararları ise yine AB üyeliği adayı bir ülke olan Türkiye açısından dikkatle incelenmelidirler. ABAD'ın dijital deliller konusunda verdiği kararların ise daha çok Avrupa Birliği Temel Haklar Bildirgesi kapsamındaki özel hayata saygı ile kişisel verilerin korunması konusunda olduğu dikkat çekmektedir.

Yargıtay kararları ise Türkiye'nin dijital deliller konusunda bulunduğu pozisyonu en iyi şekilde gösteren kararlardır. Bu konuda ilk anda erişilebilecek hemen hemen tüm kararlar çalışmaya dâhil edilmeye çalışılmıştır. Ancak gerek kamuoyunda geniş çaplı yer alması, gerekse dijital delillere ilişkin önemli içeriğe sahip olması nedeniyle Balyoz güvenlik harekât planı davası üzerinde daha detaylı olarak durulmuştur. Burada çıkan sonuç ise belki de konunun zamanla daha iyi bir şekilde öğrenilmesiyle, Yargıtay'ın verdiği kararların giderek daha düzgün içeriklerden oluştuğu yönündedir. Ancak yine de arada sırada, eleştiri konusu olacak bazı kararların da verildiği görülmektedir.

Çalışmanın en son kısmı ise tamamlayıcı nitelikte bir kısımdır. Nitekim dijital delillere ilişkin hukuki düzenlemelerin ve mahkeme kararlarının detaylı bir şekilde incelenmesi sonucunda ortaya çıkan tablonun, gerek uluslararası sistemde gerekse Türkiye'de ne şekilde oluşturulabileceği üzerinde durulmuştur. Bu nedenle bu kısım sadece konunun doğrudan bir parçası olmamakta, ileriye dönük önerileri de içeren bir değerlendirme bütünü de içermektedir. Bu konuda yapılan tespitler sonucunda ortaya çıkan gerçek ise dijital delillere yönelik düzenlemeler konusunda uluslararası uyum ve işbirliğinin arttırılmasının yanı sıra Türkiye'de mevcut düzenlemelerin değiştirilmesi veya yeni düzenlemelerin yapılmasının gerekliliğini ortaya koymaktadır.

GİRİŞ

Suçla konu olabilecek olayların çözümü açısından gerekli olan maddi gerçeğin ortaya çıkarılması hususu, ceza muhakemesinin temelini oluşturmaktadır. Bu temelini yapıtaşları ise, maddi gerçeğe ulaşmada vasıta olan, delillerdir. Bu nedenle ceza muhakemesine ilişkin tartışmalarda nelerin delil olabileceği ve hangi delillerin yargılamada kabul edilebileceği meselesi genelde ceza muhakemesi açısından asıl problem olmuştur. Günümüz ceza muhakemesi sistemlerinin çoğunda bu konudaki genel ilke, delil serbestisi ilkesi olarak belirlenmiştir. Delil serbestisi ilkesi gereği, maddi gerçeğin ortaya çıkarılmasına katkısı olabilecek her şey delil olarak kullanılabilir. Ancak her şeyin delil olarak kullanılabilmesi, her şeyin delil olarak kabul edileceği anlamına gelmemektedir. Burada hâkimler, öncelikle delillerin yargılamada kabul edilebilmeleri için sahip olmaları gereken özelliklere uygunluklarının tespitini yapacaklardır. Bu tespit ile yargılamada kullanılacak yani hâkimi vicdani kanaatine göre bir hükme ulaştıracak vasıtalar belirlenmiş olacaktır.

Son yıllarda yaşanan gelişmeler ile dijital teknoloji hayatın her alanına girdiği gibi, ceza muhakemesi hukuku içerisinde de kendisine yer bulmuştur. Dijital teknolojinin getirdiği imkânlar sayesinde birçok gelişme yaşanmış, bunun karşılığı olarak muhakeme işlemleri ve deliller dijitalleşmiştir. Dolayısıyla artık hâkimlerin önüne, eski zamanın klasik delilleri yerine, bu dijitalleşmenin sonucu olarak, dijital deliller olarak adlandırılan vasıtalar daha sıklıkla gelmektedir. Hatta bu durumu sadece hâkimlerle sınırlandırmadan savcı, avukat, kolluk vs. gibi mesleklerden oluşan diğer tüm adli birimlerin de dijital delillerle karşılaşma oranının arttığı söylenebilir. Nitekim dijital teknolojinin getirdiği kolaylıklar ile suç işleme biçimleri de evrimleşmiş, işlenen suçlarda dijital teknoloji kullanımı büyük bir artış göstermiştir. Böylece suç işleme oranları artarken, suç konusu olan olayların çözümü de dijital delillere bağlı hale gelerek zorlaşmıştır.

Buna ek olarak, dijital teknolojinin ceza hukuku açısından yarattığı bu domino etkisi karşısında, suçla ve suçlulukla etkin bir mücadele yürütülebilmesi için ceza muhakemesi hukukunda kullanılan araç ve yöntemlerin güçlendirilmesi, dijital delillere yönelik tedbirlerin hayata geçirilmesi zorunluluğu doğmuştur. Ancak dijital delillere ilişkin tedbirlerin, hukukçular tarafından yakından takip edilmesi gereklidir. Özellikle ceza hukuku açısından konunun iyi şekilde bilinmemesinin, uygulamada özel hayatın gizliliği hakkı kapsamında pek çok ihlale neden olabileceği göz önünde bulundurulmalıdır. Bu nedenle aslında ceza muhakemesinde dijital deliller başlığının teknik içeriğine bakılarak, işbu konuda çıkacak problemlerin hayatın merkezinde yer aldığı göz ardı edilmemelidir. İşte bu nedenle belki de yakın gelecekte ceza muhakemesi delil sisteminin en önemli kaynağı olacak dijital delillerin bir çalışmada kapsamlı olarak incelenmesi önem arz etmektedir.

Bilgisayarın icadı ve yaygınlaşması ile gelişen dijital delillerin hukuki değer olarak soyut yapıda bulunan veriyi merkez alan içeriği, maddi gerçeklik üzerinden kurulmuş hukuk düzenlemelerinin uyarlamalarında yaşanan sıkıntıların temelini oluşturmaktadır. Ayrıca bu konudaki sıkıntılar dijital teknolojinin sınır aşan özelliği nedeniyle uluslararası toplumun gündeminden de hiç düşmemiş, konuyla ilgili çalışmalar ve düzenlemeler günden güne geliştirilmiştir. Ancak bu uluslararası düzenlemelerin ulusal hukuklara aktarım süreci henüz tamamlanmadığı gibi, yapılan mevcut düzenlemeler de şimdiden çağın gerisine düşmeye başlamışlardır. Bu düzenlemeler aracılığıyla elde edilen dijital delillerin ceza muhakemesindeki yeri konunun ana omurgasını oluşturmaktadır.

İşbu düzenlemeler açısından, daha önceleri dijital delillere ilişkin en büyük problem konuya yönelik yeterli düzenlemenin bulunmaması iken, günümüzde mevcut düzenlemelerin geliştirilerek mevcut koşullara ve eksikliklere uyarlanması sıkıntısı bulunmaktadır. Bu eksikliklerin daha çok terim ve kavram kargaşası ile gelişen teknolojilere ayak uydurulamaması nedenlerine bağlı olarak bulunduğu söylenebilir. Ayrıca buradan yola çıkılarak dijital delillerin nasıl elde edileceği ve elde edilen dijital delillerin güvenliklerinin nasıl sağlanacağına ilişkin yöntem sorunu da konuyla ilgili temel bir problem olarak dikkat çekmektedir.

Tüm bu gelişmeler bu çalışmanın ortaya çıkmasını sağlamış ve bu çalışma içerisinde ceza muhakemesinde dijital delillerin son durumunun adeta bir röntgeni çekilmeye çalışılmıştır.

Bu noktada çalışmanın ilk bölümünün içerisinde, delil ve ispat sistemlerinin tarihsel gelişimi sonucunda geldiği nokta ile dijital delil kavramının neyi ifade ettiği, dijital delillerin özellikleri ortaya konmuştur. Daha sonra dijital delillerin ceza muhakemesindeki yeri, dijital delillerin nelerden oluştuğu, elde edilme yöntemleri ve nitelikleri gereği ceza muhakemesi alanında getireceği değişiklikler belirlenmiştir. Bu çerçevede öncelikle dijital delil kavramının delil teorisi içerisindeki yeri incelenerek, dijital deliller ceza muhakemesi sistemi içerisinde konumlandırılacaktır. Böylece dijital delillerin delil teorisi içerisinde alması gereken yer ortaya çıkacaktır ki, bu konu günümüzde gerek kamuoyu gerek akademisyenler tarafından pek çok güncel ceza davası ile ilgili olarak birçok tartışmaya yol açmış, ceza muhakemesinde deliller açısından yeni bir çağın başlangıcına işaret edilmiştir.

Teorik ve doktrinel tespitlerden sonra gelen ikinci bölümde dijital delillere ilişkin hukuki düzenlemeler incelenmektedir. Hukuki düzenlemeler incelenirken konuyla ilgili daha geniş bir bakış açısı sağlanabilmesi için, uluslararası hukuk ile ulusal hukuklar ayrı ayrı ve bağlantılı olarak ele alınmışlardır.

Üçüncü bölümde ise konuyla ilgili gerek ulusal gerekse uluslararası mahkeme kararları incelenmiştir. Bu yolla hem hukuki düzenlemelerde eksik kalan kısımlar, hem de mahkemelerin değerlendirmelerinde yani uygulamada eksik kalan yönler tespit edilmeye çalışılmıştır. Son olarak ise konuyla ilgili eksiklikler üzerine yapılan tespitler çözümsüz bırakılmamış, gelecekte yapılması beklenebilecek ve hatta tavsiye edilebilecek, gerek sistemsal gerek hukuki değişikliklere ilişkin bir yol haritası ortaya konmuştur.

BİRİNCİ BÖLÜM: CEZA MUHAKEMESİNDE DELİL TEORİSİ VE DİJİTAL DELİLLERİN YERİ

Muhakeme hukuku, hukuki bir uyumsuzluğun yargısal çözümüne katılanların yaptığı işlemleri düzenleyen hukuk normlarının bütününe verilen addır¹. Ceza muhakemesi hukuku ise, ceza muhakemesinin nasıl yapılacağı hususundaki kurallar ile bu sürece katılan kişilerin hak, yetki ve yükümlülüklerini düzenler (CMK 1). Görüldüğü gibi ceza muhakemesi hukuku, ceza kanunlarının ortaya koyduğu statik genel kuralları harekete geçiren ve bu kuralları günlük hayat akışı içerisinde dinamik hale getiren bir hukuk dalı olarak, ceza hukukunun önemli bir parçasıdır². Delil de bu önemli parçanın içerisinde bulunan, hâkime hükme yönelik değerlendirme yapabilmesinde yardım eden, bir araçtır.

Delilin ceza muhakemesi açısından sahip olduğu bu işlev göz önüne alındığında, kanunlarda suç olarak tanınan ve karşılığında ceza öngörülen eylemlere yönelik değerlendirmelerin, içerisinde bulunulan çağın gereklerini yerine getirmeye çalışan bir anlayış ile ele alındığı görülmektedir. Bu anlayış içerisinde yapılan ceza yargılamasında, delillerin çeşitlenip çoğalması da mümkün hale gelmiştir. Böylece modern çağın ve teknolojinin getirdiği pek çok yenilik de ceza yargılaması içerisinde kendisine yer bulabilmektedir. Günümüzü ele alırsak; bilgisayar teknolojisinin yaygınlaşması, bilgisayarın temelini oluşturan dijital teknolojinin de yaygınlaşması sonucunu doğururken, dijital teknolojiye sahip eşya da ceza muhakemesinde delil olarak yer bulmaya başlamıştır.

Ceza hukuku ile ilgili olaylar suç oluşturdıklarına dair bir şüphe halinde ilgili adli makamların önüne gelirler. Bu olaylar adli makamlarının önüne geldiklerinde, birer gizem halinde bulunmaktadır. Bu gizemin araştırılıp aydınlatılması için,

¹ Nevzat Toroslu/Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, 7. Baskı, Ankara: Savaş Yayınları, Eylül 2009, s. 1.

² Tahir Taner, **Ceza Muhakemeleri Usulü**, 2. Bası, İstanbul: Duygu Matbaası, 1950, s. 3.

olayın mantıki ve kronolojik yönden birbirine bağılı olan yönleri ortaya çıkarılarak, gerçeğe ulaşmaya çalışılır. Buna ceza uyuşmazlığının maddi yönü de denilmektedir³. Görüldüğü gibi ceza muhakemesi hukukunun ve bunun ifadesini oluşturan ana kanunun temel amacı gerçeğe ulaşmaktır; ancak bu hedef, insan hak ve özgürlüklerini vurgulayan adil yargılanma hakkına uygun biçimde gerçekleştirilmelidir⁴.

Böylece ortaya çıkacak olayın ayrıntıları, hâkimin vicdani kanaati ile varacağı hükme öncülük edecektir. Ortaya kişinin özgürlüğünü kısıtlama gibi önemli bir sonuç dahi çıkarabilecek olan bu hüküm, gerçeğin hâkimin düşüncesinde şüpheye yer vermeyecek şekilde canlanması sonucuna göre verilecektir. Daha sonra hâkim gerçeğin oluşturduğu bu olayı hukuki yönden inceleyecek, sonuç olarak olay içerisinde suç teşkil eden bir hususun sübut bulduğu veya bulmadığı kanaatine ulaşacaktır⁵. Yani hukuki incelemeden önce maddi olayın varlığı ispat edilecektir. Deliller ise çalışmanın bu bölümünde daha detaylı olarak da ortaya konulacağı üzere, tam da bu noktada, uyuşmazlığın maddi yönünü oluşturan gerçeğin yeniden canlandırılmasındaki ispat vasıtaları olarak ortaya çıkacaklardır. Tüm bu zincirleme çıkarım bütünlüğünün de gösterdiği üzere, ceza muhakemesinde delil, hükmün kurulmasına etki eden en önemli unsurdur. Hatta Jérémie Bentham'a göre, usul delilleri kullanabilmek sanattır⁶.

Çalışmanın ilk bölümümü oluşturan bu kısımda, ceza muhakemesinin bu unsuru, daha detaylı bir şekilde ele alınarak somutlaştırılacaktır. Dijital delillerin de detaylı olarak incelenerek, delil teorisi içerisindeki yerinin tespitin yapılacağı bu bölümde kavram incelemeleri öncesinde ceza muhakemesinde delilin yaşadığı tarihsel süreç incelenecektir.

³ Erdener Yurtcan, **Ceza Muhakemeleri Usulü Kanunu Şerhi ve İlgili Mevzuat**, 2. Cilt, İstanbul: Kazancı Hukuk Yayınları, 1988, s.167; Toroslu/Feyzioğlu, **a.g.e.**, s. 169.

⁴ 5271 sayılı CMK genel gerekçesi, s. 2, www.ceza-bb.adalet.gov.tr/mevzuat/cmkmaddegerekce.doc (Erişim tarihi: 19.03.2014)

⁵ Nurullah Kunter/Feridun Yenisey/Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 18. Baskı, İstanbul: Beta Yayınevi, 2010, s. 1325.

⁶ Faruk Erem, **Diyaletik Açısından Ceza Yargılaması Hukuku**, 6. Baskı, Ankara: Işın Yayıncılık, 1986, s. 355.

I. Delilin ve ispat sistemlerinin tarihçesi

Ceza hukuku tarihçesine göz atıldığında, ceza hukukunun en eski hukuk dalı olduğu söylenebilir⁷. Nitekim henüz devlet teşkilatının bulunmadığı dönemde bile bazı ceza hukuku uygulamaları bulunmaktadır⁸. Suç oluşturup oluşturmadığı konusunda şüphe bulunan olayların aydınlatılmasında yol gösterici olarak işlev gören deliller de, devlet önceki dönemden itibaren ceza hukuku içerisinde bulunmaktadırlar. Hatta günümüze kadar gelen süreçte delil sistemlerinin ceza hukuku sistemlerine paralel bir biçimde geliştiği de görülebilir. Delilin ceza hukuku açısından sahip olduğu önem göz önüne alındığında, bu olağan olarak ortaya çıkan bir sonuçtur.

A. İlkel ispat sistemi

Bu konu ile ilgili olarak devlet teşkilatının henüz bulunmadığı döneme baktığımızda, delillerin otorite boşluğu nedeniyle kişisel ve keyfi değerlendirmelerle belirlendiği söylenebilir. Bu kişisel ve keyfilik temel olarak uyulması gereken bir kurallar bütününe bulunmamasından ileri gelmemekle birlikte daha çok, suçun yalnızca aleyhine suç işlenen kişiyi veya kişinin mensubu bulunduğu toplumsal zümreyi ilgilendirdiği temeline dayanmaktadır⁹. Böylece suç işlenip işlenmediğine ilişkin yapılacak değerlendirme tamamen suçtan zarar gören kişiye veya onun mensubu bulunduğu toplumsal zümrenin ölçütlerine kalmış bulunmaktaydı. İlkel ispat sisteminin hakim olduğu bu dönemde ceza infaz hukukunda ise öç alma usulü hakim bulunmaktaydı¹⁰.

Devlet teşkilatının ortaya çıkmasıyla birlikte ceza hukukuna hakim olan kişisel öç alma anlayışı ile ilkel ispat sisteminin toplumsal barışa ve kamu düzenine verdiği zarar görülmüştür. Böylece zaman içerisinde suçların sadece kişileri veya zümreleri değil, ayrıca toplumunun tümünü ilgilendirecek eylemler oldukları anlayışı

⁷ Sulhi Dönmezer/Sahir Erman, **Nazarî ve Tatbikî Ceza Hukuku: Genel Kısım**, Cilt: I, 5. Bası, İstanbul: Sulhi Garan Matbaası Vârisleri Koll. Şti., 1973, s. 16.

⁸ Nur Centel/Hamide Zafer/Özlem Çakmut, **Türk Ceza Hukukuna Giriş**, 4. Bası, İstanbul: Beta Yayıncılık, 2006, s. 7.

⁹ Mehmet Emin Artuk/Ahmet Gökçen/A. Caner Yenidünya, 3. Baskı, **Ceza Hukuku Genel Hükümler I**, Ankara: Seçkin Yayınevi, 2002, s. 43; Centel/Zafer/Çakmut, **a.g.e.**, s. 7; Taner, **a.g.e.**, s. 9.

¹⁰ Artuk/Gökçen/Yenidünya, **a.g.e.**, s. 44; Centel/Zafer/Çakmut, **a.g.e.**, s. 8; Taner, **a.g.e.**, s. 159.

güçlenmiştir. Bunun sonucu olarak da ceza hukukunda kişisel öç alma yöntemlerinin kısıtlanması ve kişilerin tazminat ödemelerine dayanan bir uzlaşma anlayışını yayma çabası dikkat çekmiştir¹¹.

O tarihlerde ceza muhakemesinde sistem olarak, bugün dahi Anglosakson ceza hukuku sistemine sahip olan ülkelerde (en başta Amerika Birleşik Devletleri ve İngiltere olmak üzere) ve ayrıca bu hukuk sistemini model alan ülkelerde, günümüzde çok daha modern bir şekli uygulanan itham sistemi etkindi¹². İtham sisteminde, bir kişinin cezalandırılabilmesi için başka bir kişi tarafından suçlanarak itham edilmesi ve itham eden kişinin, ithamının gerçekliğini ispat etmesi esası uygulanmaktadır¹³. İtham sistemi daha açık, aktif ve sözlü bir yargılamaya ön ayak olmaktaydı. Ancak bu sistem içerisinde bazı olaylara kimsenin ilgi göstermediği durumlar da mevcut olmuş ve suçluların işledikleri kimi suçlar yanlarına kâr kalmıştır¹⁴.

B. İnanca dayalı ispat sistemi

Devlet teşkilatının gelişmeye başlaması ile devlet örgütlenmesi de gelişmeye başlamış, otoriteyi elinde bulunduranlar toplum barışı ve kamu düzeninin sağlanması bakımından insanları yönlendiren uygulamalarda bulunmuşlardır. Bunlardan uzlaşma anlayışını yayma çabası üzerinde ilkel ispat sistemini anlatırken durulmuştu. İlerleyen dönemlerde ise bu uygulamaların temelleri inançlara dayalı olarak oluşmuştur. Bunun bir nedeni, otoriteyi elinde bulunduranların bu otoritenin kaynağı olarak ilahi güçleri göstermesi olmuştur. Kişisel öç alma döneminin ve dolayısıyla kişisel ve keyfî delillere dayanan ilkel ispat sisteminin de sonu olacak bu dönemde, inanca dayalı bir ceza hukuku sistemi ve ispat sistemi ortaya çıkmıştır.

Bu dönemin özelliği, cezaların toplumsal öç ve ibret temeline dayanmasıdır¹⁵. Deliller açısından ise artık insanlar kendilerini suçluların belirlenmesi konusunda yeterli görmeyerek, inançları doğrultusunda ilahi gücü ispat vasıtası saymış, ilahi

¹¹ Centel/Zafer/Çakmut, **a.g.e.** , s. 8; Taner, **a.g.e.** , s. 9.

¹² Taner, s. 10; Mehmet Yayla, “Ceza Yargılamasında İspat İçin Yenilmesi Gereken Şüphe; Türkiye ve Amerika Birleşik Devletleri Sistemlerinin İncelenmesi”, Ankara Barosu Dergisi, 2013/3, s. 295.

¹³ Mehmet Yayla, **a.g.e.** , s. 296.

¹⁴ Taner, **a.g.e.** , s. 10.

¹⁵ Centel/Zafer/Çakmut, **a.g.e.** , s. 8.

gücün işaretlerini delil olarak değerlendirmişlerdir¹⁶. İlahi gücün işaretinin anlaşılabilmesi için itham edilen kişiye yönelik olarak bazı ilahi imtihanlar¹⁷ yapıldı. Bu ilahi imtihanlardan kendisini kurtaran kişinin, kendisine ilahi güç tarafından yardım edildiği için korunduğu düşünülmüştür. Bu nedenle kişinin masum olup olmadığı kanaati de ilahi imtihanın sonucuna bağlanmıştır. İlahi imtihanda başarısız olanlar ise suçlu olarak kabul edildikleri için mahkûm edilmekteydiler. Bu dönemde suçların aynı zamanda günah olarak da değerlendirilmesi nedeniyle, suçlunun günahlarından arınması için acı çekeceği cezalara çarptırılması ve bu yolla işledikleri günahın kefaretiyi ödemelerinin sağlanmasına inanılmaktaydı¹⁸.

Görüldüğü gibi bu dönemde ceza muhakemesinde etkin olan itham sistemi de yerini yavaş yavaş sanığı daha ziyade bir muhakeme objesi olarak gören tahkik sistemine bırakmaktadır. İlahi ispat sisteminin hakim olduğu dönemin tahkik sisteminde, ilahi gücün hata yapmayacağı düşüncesiyle, inanca dayalı usuller ceza muhakemesi hukuku olarak benimsenmiş ve uygulanmıştır¹⁹. Yani tahkiki gerçekleştiren ilahi güçtür.

C. Akılcı ispat sistemleri

Zamanla inanca dayalı ilahi imtihanların şiddetli ceza infaz uygulamaları toplum içerisinde eleştirilmeye başlandı. Bu eleştirilerin sonucunda ceza hukukunda bazı yeni uygulamalar yapılması önerileri ortaya çıktı. Özellikle Fransız İhtilali ile birlikte ceza hukuku alanında ortaya konan pek çok yeni ilke bulunmaktaydı. Bu dönemin popüler anlayışlarından biri olan suçların ve cezaların kanuniliği ilkesi doğal olarak dönemin delil ve ispat uygulamalarına da yansdı.

Bu dönemde ceza muhakemesinde etkin olmaya başlayan sistem, tahkik sistemidir. Günümüzde Almanya, Avusturya, Fransa ve Hollanda ceza muhakemesi

¹⁶ Taner, **a.g.e.** , s. 159.

¹⁷ Bkz. Taner, **a.g.e.** , s. 10, 159; bunların kişiye kızgın demir basılması veya kişinin üzerine kaynar su dökülmesi gibi örnekleri bulunmaktadır. Ancak içlerinde belki de en dikkat çekici olanı adli düellodur. Adli düelloda davacı ile itham edilen kişi hâkim önünde dövüşürler, itham edilen kişi kazanırsa masum sayılır; ancak kaybederse suçlu sayılarak ölüsü cezalandırılırdı. Bu dönemde cezaların uygulanma yöntemleri için bkz. Centel/Zafer/Çakmut, **a.g.e.** , s. 8.

¹⁸ Centel/Zafer/Çakmut, **a.g.e.** , s. 8.

¹⁹ Mehmet Yayla, **a.g.e.** , s. 298.

sistemleri tahkik sistemine örnek olarak gösterilebilir²⁰. Tahkik sistemi, itham sisteminden farklı olarak tarafsız bir hâkimin, delilleri araştıran ve yargılama içerisinde en etkin konumda olmasına dayanmaktadır. Ancak bu sistemde de hâkim ilk olarak, tahkik sisteminin işleyişinin dayandırıldığı kanunla sınırlandırılmaktaydı. Vicdani ispat sistemi sonrasında ise hâkimler kanaatlerinde özgürleşmişlerdir.

Kanuniliğin etkisinin artması sayesinde, akıl dışı bir ispat sistemi olan ilahi ispat sistemi gücünü kaybetmiştir. Sonuç olarak sanığı adalet mekanizmasının ezici gücünden korumak amacıyla akılcılığı öne çıkaran kanuni ispat sistemi benimsenmiştir. Önceden belirlenmiş katı kurallara göre yürüyen bu ispat sistemi ile gerçeğe ulaşılacağı düşünülmüştür²¹. Böylece inanca dayalı ispat sistemi de yerini kanuni ispat sistemine, bu aşamaya kadar gelen akıl dışı ispat sistemleri de yerini akılcı ispat sistemlerine bırakmış olmaktadır²².

1. Kanuni ispat sistemi

Akılcı bir ispat sisteminin ilk örneği olan kanuni ispat sisteminde delillerin kanunda belirlenmesi esas olarak kabul edilmiştir. Kanunda belirlenen fiillerin işlenip işlenmediğinin hangi delillerle ispat edileceği kanun tarafından belirlenmiş, hâkime bu konuda herhangi bir takdir hakkı tanınmamıştır²³. Kanunda öngörülen delillerin varlığı halinde, hâkim kanaati kişinin suçsuz olduğuna yönelik olsa bile, mahkûmiyet kararının verilmesi zorunludur. Aksi halde, yani kanunda öngörülen delillerin bulunmaması halinde ise, hâkimin kanaati kişinin suçlu olduğuna yönelik olsa bile, kişinin mahkûm edilmesi mümkün değildir²⁴. Böylece hâkim yalnızca delillerin kanunda belirlenenlere uygun olup olmadığını denetleme ve kararını da bu delillere bağlı olarak verme yetkisi ile sınırlandırılmaktaydı.

²⁰ Mehmet Yayla, **a.g.e.**, s. 295.

²¹ Toroslu/Feyzioğlu, **a.g.e.**, s. 60.

²² Bahri Öztürk/Mustafa Ruhan Erdem/Veli Özer Özbek, **Uygulamalı Ceza Muhakemesi Hukuku**, 7. Baskı, Ankara: Seçkin Yayıncılık, 2002, s. 411, dn. 7.

²³ Ali Kemal Yıldız, **Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi**, Doktora Tezi, Tez Danışmanı: Kayıhan İçel, İstanbul, 2002, s. 11.

²⁴ Taner, **a.g.e.**, s. 160.

2. Vicdani ispat sistemi

Zamanla maddi gerçeğe ulaşma amacının kanuni ispat sistemiyle gerçekleşemeyeceğinin anlaşılması ile kanuni ispat sisteminde görülen sakıncalar ve zorluklar üzerine ortaya konan vicdani ispat sisteminde ise, hâkim delillerin takdirini, vicdani kanaatine göre yapmaktadır. Ancak bu durum kararların keyfi olarak verileceği anlamına gelmemektedir²⁵. Hâkimin delillerin takdiri konusunda sahip olduğu serbestinin sınırlarının yine elde edilen delilde saklı olduğunu unutmamak gerekir. Çünkü zaten delile bağlı olmayan bir şekilde oluşan vicdani kanaat, karar konusunda keyfiliğe yol açacaktır.

Ayrıca değerlendirmenin hâkime bırakılması nedeniyle, maddi gerçeği aydınlatmak için sınırlama olmaksızın her türlü delil serbestçe getirilecektir. Görüldüğü gibi vicdani kanaat kavramı ancak delil serbestisi kuralı ile birlikte anlam kazanmaktadır²⁶. Delil serbestisi kuralı hem delillerin mahkemeye sunulması bakımından hem de mahkemeye sunulan delillerin değerlendirilmesini kapsamaktadır²⁷. Bu noktada mahkeme tarafından hükmün verilmesi konusunda, delillerin değerlendirilmesi önem kazanacaktır. Ayrıca, hiçbir delilin hâkimi bağlayıcı olmaması nedeniyle delilin sağlamlığının değerlendirmesi de hâkim tarafından yapılacaktır. Ancak bu değerlendirmede mantık kuralları, tecrübe ve bilimsel veriler sınırlayıcı olacaktır²⁸.

Vicdani kanaatini ortaya koyan hâkimin, delillere yönelik yapacağı değerlendirmenin gerekçeli olması gereği de unutulmamalıdır. Çünkü hüküm, hâkimin delillerden yola çıkarak edindiği vicdani kanaatin hukuki karşılığını içermektedir. Görüldüğü gibi vicdani ispat sistemini, salt yalın vicdani kanaate dayalı olmayan, somut delillere dayalı gerçek hukuksal gerekçesi gösterilerek izah edilmiş bir sübut kanaati olarak anlamak gerekir²⁹. Ancak bu şekilde yargılamadaki adalet dengesinin bozulmasının önüne geçilebilmektedir. Aksi takdirde her hâkim ayrı bir hukuk kaynağı oluşturacaktır.

²⁵ Taner, **a.g.e.** , s. 160.

²⁶ Erem, **a.g.e.** , s. 351.

²⁷ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1327.

²⁸ Yıldız, **Ceza Muhakemesinde İspat...** , ss. 147-148.

²⁹ Yener Ünver, **“Ceza Muhakemesinde İspat, CMK ve Uygulamamız”**, Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, Aralık 2006, s. 106.

Vicdani ispat sisteminin devreye girmesi ile birlikte ceza muhakemesinde, itham ve tahkik sistemlerinin farklı özelliklerini bir araya getiren işbirliği sistemi ortaya çıkmıştır. Günümüzde İtalya ve Türkiye ceza muhakemesi sistemleri işbirliği sistemine örnek olarak gösterilebilir³⁰. İddia, savunma ve yargılama makamları arasındaki işbirliğine dayanan bu sistemde, ne tarafların itham sistemindeki yoğunlukta diyalogu, ne de tahkik sistemindeki şekilde sadece hâkimin monoloğu etkilidir. Yani işbirliği sistemi, bu üç makamın gerçekleştirdiği bir işbirliğidir³¹. Türkiye'nin mevcut ceza muhakemesi hukuku sistemi ise daha çok tahkike dayalı bir işbirliği sistemi olarak çalışmaktadır³².

Delil serbestisini esas alan vicdani ispat sistemi günümüzde pek çok ülke tarafından kullanılmaktadır. Örneğin, Fransız Ceza Usul Kanunu'nun 427. maddesi ile kanunun aksini belirttiği durumlar haricinde her tür delilin mahkemeye getirilebileceği ve hâkimin bu delillere dayanarak vicdani kanaati ile karar vereceği belirtilmiştir³³. Yine Alman Ceza Usul Kanunu'nun 261. maddesinde, mahkemenin kendisine sunulan delillerin değerlendirilmesi sürecinde, duruşmalardan edindiği özgür vicdani kanaatine göre karar vereceği belirtilmiştir³⁴. Anglosakson ceza hukuku sisteminde ise delillerin değerlendirilmesinde gerek kanuna gerek mahkeme kararlarına dayanan daha karmaşık kurallar mevcuttur³⁵.

Türkiye'nin ceza muhakemesi sisteminde de vicdani ispat sisteminin kabul edildiği söylenebilir. Bu husus öncelikle Anayasa'nın 38. maddesinden yola çıkılarak ortaya konulabilir. Nitekim ilgili madde içeriğine göre hâkimler; Anayasa'ya, kanuna ve hukuka uygun olarak vicdani kanaatlerine göre hüküm verirler³⁶. Bu husus CMK'nin 217. maddesinde de açıkça ortaya konmuştur. Madde içeriğine göre; hâkim kararını verirken, duruşmaya getirilmiş ve huzurunda tartışılmış delilleri vicdani

³⁰ Mehmet Yayla, **a.g.e.** , s. 295.

³¹ Toroslu/Feyzioğlu, **a.g.e.** , s. 43.

³² Mehmet Yayla, **a.g.e.** , s. 304.

³³ Code de Procédure Pénale (CPP) Article 427, www.legifrance.gouv.fr/content/download/1958/13719/.../Code_34.pdf. (Erişim tarihi: 02.05.2014)

³⁴ Strafprozeßordnung (StPO) Article 261, Alman Ceza Usul Kanunu'nun İngilizcesi için bkz. http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html. (Erişim tarihi: 02.05.2014)

³⁵ Bununla ilgili örnekler için ikinci bölümde bazı yabancı hukuk düzenlerinde dijital delillere ilişkin düzenlemeler başlığı altında (bkz. s. 79 vd.) delil değerlendirme kurallarından bahsedilen ABD, Avustralya ve Birleşik Krallık örneklerine bakılabilir.

³⁶ Bu maddenin amacı hakkındaki tartışmadan yola çıkılarak delillerin serbestliği unsurunun bir Anayasa prensibi olarak kabul edilmemesi gereği ve medeni usul hukuku bakımından bu konunun yaratacağı sıkıntılar için bkz. Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1327, dn. 9.

kanaatiyle serbestçe takdir edecektir. Sonuç olarak hiçbir delil hâkimi bağlayıcı değildir. Ama bu noktada, ayrıca delillerin özellikleri başlığı altında da ele alınacağı üzere³⁷, delil serbestisinin sınırsız bir serbesti olmadığı da görülmektedir.

Ceza muhakemesinde delil serbestisinin sınırları ise ispat bakımından delil özellikleri ile çizilebilir. Delillerin ispata yeterli olabilmeleri için hukuk sisteminde tanımlanmış olan özellikler iyi bir sınır çizmektedir. Bu özelliklerden ilki ve en önemlisi delilin hukuka uygun olması gereğidir. Hukuka uygunluk delili elde etme yasağı bulunan sanığın ve tanığın susma hakkı (çekinmesi) gibi kurallarının yanı sıra kanuni ispat kuralları³⁸ gibi kurallar aracılığıyla da çizilebilir³⁹.

Daha önce de belirtildiği gibi, vicdani ispat sisteminin hâkim olduğu ceza muhakemesinde delil serbestisi ilkesi kuşkusuz kabul görecektir. Ancak bu gelişme sadece ceza muhakemesi hukukuna özgü bir durum değildir. Medeni usul hukukunda da delil serbestisi giderek önem kazanmaktadır. Nitekim HMK 198. maddesine göre hâkim; kanuni istisnalar dışında delilleri serbestçe değerlendirecektir. Ancak yine de ceza hukuku sisteminin yanında medeni usul hukukunda pek çok kanuni istisna bulunduğu ve kanuni ispat sisteminin etkilerini yoğunlukla sürdürdüğü de bir gerçektir⁴⁰.

3. Bilimsel ispat sistemi

Günümüzde vicdani ispat sisteminin yetersiz olduğu görüşündekiler, bu sistemin yerini bilimsel ispat sisteminin alması gerektiğini ileri sürmüşlerdir. Genel olarak vicdani ispat sistemi geçerliliğini korumakla birlikte ceza muhakemesi hukukunun bilimsel ispat sistemine doğru hızla ilerlediği iddia edilmektedir. Bilimsel yöntemlerle elde edilen deliller maddi gerçeğin araştırıldığı ceza muhakemesi hukukunda, maddi gerçeğe ulaşılması konusunda, vicdani kanaate göre daha doğru sonuçlar verecektir. Nitekim bilimsel yöntemlerle elde edilen bir sonuçla çelişen ve

³⁷ CMK 217 delillerin müşterekliği ilkesi açısından da önemli bir maddedir. Ayrıca diğer delil özellikleri için bkz. s. 33 vd.

³⁸ CMK 222’de yer alan bu hükümle kanun, duruşmanın nasıl yapıldığı, kanunda belirtilen usul ve esaslara uygun olarak yapılıp yapılmadığının ancak tutanakla ispat olunabileceğini belirtmiş; böylece ispat gücüne sahip olacak delilleri sınırlandırmıştır.

³⁹ Yıldız, **Ceza Muhakemesinde İspat...**, s. 151.

⁴⁰ H. Yavuz Alangoya/M. Kâmil Yıldırım/Nevhis Deren-Yıldırım, **Medenî Usul Hukuku Esasları**, 6. Bası, İstanbul: Alkım Yayınevi, 2006, s. 324 vd.

başka hiçbir dayanağı olmayan herhangi bir ispat aracına dayanılarak hüküm kurulması çok doğru görünmemektedir⁴¹. Ancak aksi durumda da güvenilir bilimsel yöntemlere dayanan bir bilimsel delilin hâkim tarafından reddedilmesi mümkün gözükmemektedir⁴². Bu durum, bir anlamda kanuni ispat sistemine geri dönülmesi sonucunu doğuracağı gerekçesiyle eleştirilmiştir⁴³.

Belirli bir bilim dalının kural ve yöntemleri ile elde edilen deliller ise bilimsel deliller olarak adlandırılmaktadırlar. Bu deliller ilgili oldukları olay ile ilgili bazı konularda ispat açısından kesin sonuçlar verebilmektedirler. Ancak bilimsel güvenilirliğe sahip her delilin mutlak bir şekilde olayı ispatlayacağı ileri sürülemez⁴⁴.

Bunun yanı sıra her bilimsel delilin de objektif sonuç doğurmayacağı ileri sürülebilir. Bilimsel açıdan tereddüde yer vermeyecek sonuçlar dışında kalan bilimsel sonuçların, bir açıdan sübjektiflik taşıdığı da ileri sürülebilir⁴⁵.

II. Delil ve ispat kavramları

Delilin ve ispat sistemlerinin tarihçesini inceledikten sonra delil ve ispatın günümüzde ceza muhakemesi açısından sahip olduğu değerin görülmesi için bu kavramların açıklığa kavuşturulması gereklidir. Dolayısıyla bu başlık altında delil ve ispat kavramları detaylı olarak incelenecektir.

A. Delil kavramı

Delil ve delalet kelimeleri dilimize Arapçadan geçmişlerdir. Delil kelimesi delalet kelimesinin sıfat halidir. Yol gösterme, kılavuzluk ve rehberlik kavramlarını karşılayan delalet kelimesi, “*kendisinin bilinmesi, başka bir şeyin bilinmesini zorunlu kılan şeydir ki bu; bir şeyin, bilinmekle başka bir şeyin bilindiği bir durumda olması*”

⁴¹ Öztürk/Erdem/Özbek, **a.g.e.**, s. 416.

⁴² Nur Centel/Hamide Zafer, **Ceza Muhakemesi Hukuku**, 6. Bası, İstanbul: Beta Yayınevi, 2008, s. 646, dn. 10.

⁴³ Taner, **a.g.e.**, s. 161.

⁴⁴ Yıldız, **Ceza Muhakemesinde İspat...**, s. 13; Örneğin, hırsızlık yapılan olay mahallinde bulunan parmak izinin sahibinin suçu işlediğini ispatı değil, bu kişinin olay yerinde bulunduğunu ispatı gerçekleşmiş olur.

⁴⁵ Kunter/Yenisay/Nuhoğlu (2010), **a.g.e.**, s. 1333.

anlamına gelir⁴⁶. Delil kavramı da böylece, kendisinin bilinmesi ile başka bir şeyin bilinmesi için yol gösteren, kılavuzluk yapan ve rehberlik eden şey olarak tanımlanabilir.

TDK Güncel Türkçe Sözlük'e göre delil ve kanıtın hukuki manada aynı anlama geldiği belirtilmekle birlikte delilin tanımı ise “*İnsanı aradığı gerçeğe ulaştırabilecek iz, emare.*” şeklinde yapılmıştır⁴⁷. Genel çerçeveden bakınca ise, kelime anlamının da ortaya koyduğu üzere, delilin insanı var olan ama bilinmeyen ve araştırılan bir gerçeğe götürebileceği, ayrıca iz ve emareyi de kapsadığı görülmektedir.

Hukuki anlamda delil kavramı araştırıldığında ise Türk Hukuk Lûgatı'nda bulunan tanım dikkat çekmektedir. Türk Hukuk Lûgatı'na göre delil (*lat. probatio, argumentum – alm. Beweis, Beweismittel – fr. moyen de preuve – ing. evidence, proof*), “*Nizaa sebebolaran fiili veya hukuki vakıanın, olduğuna veya olmadığına hâkimin kanaatini çekmek için usul hukukunun kullanılmasına müsaade ettiği ispat vasıtasıdır. Beyyine, ispat vasıtası, sübut sebepleri, esbab-ı sübutiye, sübut vasıtası da aynı anlamda kullanılır... Delil, emareyi de içine alır...*”⁴⁸ olarak tanımlanmıştır. Yani delilin önceden gerçekleşen bir olayın ispatına yarayan, hukuk tarafından kabul edilmiş bir vasıta olması belirtilmişken, emareyi kapsamı ise yine burada da ortaya konmuştur. Emare ile delil arasındaki fark dijital delillerin delil teorisine göre yeri başlığı altında da ayrıca incelenecektir⁴⁹.

Türkiye’de normlar içerisinde kendisine ne kadar yer bulduğu incelendiğinde ise, delil kavramının üst norm niteliği taşıyan Anayasa’da kendine yer bulmuş olması, delilin hukuk sistemi açısından da ne kadar önem verilen bir kavram olduğunun anlaşılması için ilk işaretlerdendir. Delil kelimesi Anayasa’da, kişi hürriyeti ve güvenliği başlıklı 19. maddede bir kez, suç ve cezalara ilişkin esaslar başlıklı 38. maddede ise iki kez geçmektedir. Toplamda Anayasa’da üç kez geçen delil kelimesi, burada herhangi bir tanımı verilmemekle birlikte, kişi hürriyetini

⁴⁶ Akt. Mehmet Ali Şimşek, “**Delalet Kavramı Çerçevesinde Lafız ve Anlam İlişkileri**”, Nüsha Şarkiyat Araştırmaları Dergisi, Yıl: 1, Sayı: 2, Yaz 2001, s. 82, dn. 15 (el-Mu’cemu’l-vasîf, İstanbul 1990, s. 294).

⁴⁷ TDK Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts. (Erişim tarihi: 26.03.2014)

⁴⁸ Türk Hukuk Lûgatı, 3. Baskı, Ankara: Başbakanlık Basımevi, 1991, s. 66.

⁴⁹ Bkz. s. 42 vd.

sınırlayan bir tedbir olan tutuklama uygulamasının yanı sıra kişinin kendisi ve yakınları aleyhine delil vermeye zorlanması yasağı (*nemo tenetur*) ile kanuna aykırı delil kullanma yasağı gibi konular açısından ele alınmıştır.

CMK’de de delilin herhangi bir tanımı yapılmamıştır. Ancak delilin muhakeme ile yargılama işlemlerinin önemli bir unsuru olduğu, kanun içerisinde delillere yönelik yapılmış birçok düzenlemeden de açıkça anlaşılmaktadır. HMK’de de delil, kelime olarak sıkça geçmekte ve pek çok düzenlemeye konu olmakta iken kelimenin kendisinin başlı başına bir tanımının yapıldığı söylenemez.

Bu konuda Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik⁵⁰ delilin ne olduğuna dair bir tanımda bulunan tek normatif düzenlemedir. Bu yönetmeliğin 3. maddesinde delil, “*meydana gelen bir suçun aydınlatılması ve suç sanıklarının tespitine yarayan her türlü ispat vasıtası*” olarak tanımlanmaktadır.

Normlar içerisinde kendisine sıkça yer verilmiş ve hatta bir yönetmelik içerisinde tanımı yapılmış olan delilin, doktrinde yapılan tanımları da incelenerek bu kavramla ilgili daha detaylı bilgiye sahip olunabilir.

Doktrindeki tanımlardan birinde, içerisinde bulunduğu delil kuramı başlığının altında deliller; ceza davasının dayandığı şüphenin yakın derecesine götürülmesi veya giderilmesi suretiyle işin gerçeğini ortaya çıkarma gayesine varmak için kullanılacak vasıtalar olarak tanımlanmıştır⁵¹. Bir başka tanıma göre ise deliller, önceden gerçekleşmiş olayın gerçeğini ortaya çıkarmaya yönelik olarak bugün mevcut olan ve varlığını duyularımızla öğrenebildiğimiz şeylerdir⁵². Bu noktada, delilin taraflar bakımından ispat, hâkim bakımından sabit görme ve maddi yön bakımından da sübut bulma denilen faaliyetlerin vasıtası olması sebebiyle, delilleri kapsayan kuramın da ispat kuramı olarak adlandırılması ve delil kelimesinin anlamsal olarak yalnızca ispat vasıtası olarak kullanılması gereği ileri sürülmüştür⁵³.

⁵⁰ Resmi Gazete, Tarih: 17 Şubat 1983, Sayı: 17962.

⁵¹ Taner, **a.g.e.** , s. 156.

⁵² Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1326.

⁵³ Nurullah Kunter, **Ceza Muhakemesi Hukuku**, 5. Bası, İstanbul: Sermet Matbaası, 1974, s. 382.

Bu konuda yine bir başka tanım şöyledir: “*Delil (ispat vasıtası), ceza uyuşmazlığının konusu olan olayı temsil eden, olayın mahkeme önünde canlandırılmasına yarayan araçtır.*”⁵⁴

Yine bir başka tanım da şu şekilde verilmiştir: “*Yargıcın muhakeme sonucunda maddi olayı çözmesine ve böylece bunu sabit görmesine veya görmemesine hizmet eden araçlara delil denir.*”⁵⁵

Benzer bir başka tanım ise şudur: “*Yargılama konusu olayın açıklığa kavuşturulması, başka anlatımla maddi gerçeğin bulunabilmesi için ispat amacıyla kullanılan araçlara delil denir.*”⁵⁶

Medeni usul hukuku doktrinde de bazı delil tanımları ortaya konulmuştur. Bunlardan birine göre deliller, bir vakıanın ispatı için başvurulacak araçları ifade etmektedir⁵⁷. Diğer bir esere göre ise deliller, “*ispatı gerekli olan vakıaların vuku buldukları veya bulmadıkları hususunda hâkimde kanaat yaratmak için başvurulacak araçlar*”⁵⁸ olarak tanımlanmıştır. Sonuç olarak ceza muhakemesi ve medeni usul ilkeleri açısından delilin tanımlanmasında çok da büyük bir farklılık göze çarpmamaktadır. İki hukuk dalı arasındaki temel farklılık ise, yine bu başlık içerisinde de değinileceği üzere, ispata yönelik olarak ortaya çıkacaktır⁵⁹.

Tüm bu tanımlardan da yola çıkarak delil kavramının ceza muhakemesi açısından bir değerlendirmesi yapıldığında, ceza muhakemesinde delilin öncelikli olarak; ceza uyuşmazlığının maddi yönünü oluşturan olayla ilgili gerçeğe ulaşma konusunda hâkime yol gösterecek bir vasıta olması gerekir. Bu gerçek, delil yoluyla ispat edilecektir, çünkü hukuk düzeninin ispat uygulamasında kabul ettiği vasıtalar delillerdir⁶⁰. Suç şüphesi ile başlamış olan cezai süreç, delillerin ortaya koyduğu tabloya göre, başlangıçtaki şüpheyi ortadan kaldırarak suçun varlığının ispat edildiği

⁵⁴ Centel/Zafer, **a.g.e.**, s. 197.

⁵⁵ Toroslu/Feyzioğlu, **a.g.e.**, s. 169.

⁵⁶ Yener Ünver/Hakan Hakeri, **Ceza Muhakemesi Hukuku**, 2. Cilt, 6. Baskı, Ankara: Adalet Yayınevi, 2012, s. 98.

⁵⁷ Baki Kuru, **Hukuk Muhakemeleri Usulü**, Cilt II, 6. Baskı, İstanbul: Demir – Demir Yayıncılık, 2001, s. 1966.

⁵⁸ Alangoya/Yıldırım/Deren-Yıldırım, **a.g.e.**, s. 330.

⁵⁹ Bkz. s. 17 vd.

⁶⁰ Öztürk/Erdem/Özbek, **a.g.e.**, s. 411.

ya da edilemediği bir noktaya varacaktır. Yani görüldüğü gibi ispat kurumu delillerin varlığına bağlıdır⁶¹.

B. İspat kavramı

Bu noktada delilin ispata sıkı sıkıya bağlı bir kavram olduğu daha net görüldüğü için biraz da ispat kavramının içeriğine girmek yerinde olacaktır. TDK Güncel Sözlük'te ispat, “*Tanıt ve kanıt göstererek bir şeyin gerçek yönünü ortaya çıkarma, kanıtlama, tanıtlama, tanıt.*” olarak tanımlanırken⁶²; Türk Hukuk Lûgatı'na göre ise (*lat. probatio, alm. Beweelsführung, Bewels, fr. administration de la preuve, ing. probation*), “*İhtilaf mevzuu olan maddi veya hukuki vakıanın olduğu veya olmadığı hususunda hâkime kanaat verecek delil ve karineleri arz etmek, hakimin kanaatini bu noktaya çekmek.*” olarak tanımlanmıştır⁶³. Bu tanımlardan da anlaşılacağı üzere ispat özet olarak, bir olayın gerçeğinin ortaya çıkarılmasıdır. Hukuk açısından ise bu gerçeğin ortaya çıkarılmasında ve hâkimin kanaatinin oluşmasında araç olarak karine ve deliller kullanılacaktır.

Normda ilk olarak Anayasa'nın 39. maddesinde ispat hakkı başlıklı bir madde bulunmaktadır. Ancak bu madde yalnızca hakaret suçu açısından isnadın doğruluğunun ispatı ile maddede bulunan şartlara istinaden sanığın beraat edebileceğine yönelik özel bir düzenlemedir.

CMK ve HMK'de ise ispat kelimesi sıklıkla geçmekle birlikte, kanunların vermiş olduğu bir ispat tanımı bulunmamaktadır.

Doktrindeki tanıma göre ceza muhakemesinde ispat, hukuk düzeni tarafından kabul edilen vasıtalar yoluyla, fiilin fail tarafından işlendiği veya işlenmediği konusunda yargılama makamının tam bir kanaate ulaşmasını temin uygulamasıdır⁶⁴. Yani ispat etmek, hâkimi bir vakıanın varlığına ikna etmeyi başarmak demektir⁶⁵.

⁶¹ Yurtcan, s. 167.

⁶² TDK Güncel Sözlük.

⁶³ Türk Hukuk Lûgatı, s. 168.

⁶⁴ Öztürk/Erdem/Özbek, **a.g.e.**, s. 410.

⁶⁵ Claus Roxin, “**İspat Hukukunun Esasları**”, Çev. Yener Ünver, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl: 4, Sayı: 8, Güz 2005/2, s. 266.

Bu tanımlardan da yola çıkarak ispatın bir vakıanın gerçekliği konusunda hâkimin kanaatini oluşturacak yol olduğu görülmektedir. Bu yolu aydınlatacak ışıklardan biri ise delillerdir. Buna ek olarak yukarıdaki Türk Hukuk Lûgatı tanımından da yola çıkılarak, karinelerin de hâkime kanaat vermede etkili olacağı ortaya kinsa da, bu hususun daha çok medeni usul hukuku bakımından geçerli olacağı da belirtilmelidir. Ancak ceza muhakemesi açısından da karinelerin varlığı yadsınamaz bir gerçektir.

Karine ihtimale dayanan bir kavramdır. Bir olayın doğruluğunun önceden ve soyut bir şekilde kabul edilmesi olarak tanımlanmıştır⁶⁶. Günümüzdeki temel hak ve özgürlükleri de göz önünde bulundurursak, ceza muhakemesinde mevcut olabilecek tek karinenin masumiyet karinesi olacağı söylenebilir⁶⁷.

Ceza muhakemesinde tek karine olarak masumiyet karinesini kabul etmek ise deliller açısından problem yaratacaktır. Bu durumda delillerin sağlamlığının kontrolü imkânsız hale gelecektir. Her delil doğruluk açısından bir karine gerektirecektir⁶⁸. Ancak bu karinenin aksini ispatlamaya (karineyi çürütmeye) yardımcı olacak haklar verilmesi durumunda hukuka uygunluk sağlanmış olur⁶⁹. Karinenin çürütülmesi imkânı bir hukuk düzenince kabul edilmiyorsa, bu hukuk düzenine hâkim olan ispat sistemi vicdani değil, kanuni olacaktır. Tüm bu nedenlerle ceza hukuku açısından kabul edilecek karineler çok dikkatli bir şekilde süzgeçten geçirilmelidir.

Aslında yukarıdaki açıklamalardan da görüldüğü gibi karineler de doğrudan doğruya deliller ile ilgilidir. Bu hususu temel alırsak, ceza muhakemesinde hükmün neredeyse tamamen delillere dayalı bir şekilde verilmekte olduğu da ortaya çıkacaktır. Böylece delil kavramının doğrudan doğruya hâkim kararlarının kaynağı olarak nitelenmesi de mümkün olacaktır⁷⁰.

⁶⁶ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1495.

⁶⁷ Erem, **a.g.e.** , s. 366.

⁶⁸ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1497.

⁶⁹ Örneğin bir fotoğrafın veya videodaki görüntülerin ilk planda doğruluğu kabul edilecektir. Ancak fotomontaj ya da videoda oynama yapma yoluyla değişiklik yapıldığının ileri sürülmesi hukuken mümkün olmalıdır. Belgeler açısından da mahkemede bir belgenin sahteliğinin ileri sürülebilmesi gerekir.

⁷⁰ Erem, **a.g.e.** , s. 355.

İspat açısından karineler ile ilgili yukarıdaki çözümlemeler yapıldıktan sonra, ispatın konusunu neyin oluşturduğu ve ispat külfetinin kimde olduğu meselelerinden bahsedilebilir.

1. İspatın konusu

Medeni usul hukukunda ispatın konusu, tarafların üzerinde anlaşılmadıkları ve uyuşmazlığın çözümünde etkili olabilecek çekişmeli vakılardan oluşur ve bu vakıaların ispatı için delil gösterilir (HMK 187 ve ayrıca HUMK 238). Herkesçe bilinen (aşikâr) vakıalar ile ikrar edilmiş vakıalar çekişmeli sayılmamaktadır⁷¹. Ayrıca kanunda aksine bir hüküm bulunmadıkça, taraflardan her biri, hakkını dayandığı olguların varlığını ispatla yükümlüdür⁷². Yani medeni usul hukuku açısından temel kural, ispat külfetini uygulanacak hukuk kuralından lehine sonuç çıkaracak bir iddia sahibi olan kişiye yüklemektedir⁷³.

Ceza muhakemesinde ispata konu olacak mesele ise, muhakemenin maddi yönü olarak da görebileceğimiz vakıadır. Deliller ise vakıanın gerçekliğinin ispatına yönelik olarak ortaya konulacaktır. Bu vakıanın gerçekliğinin ispatına yönelik olarak bilirkişilik müessesinin de hâkime yardımcı olacağı durumlar olacaktır⁷⁴. Olayın maddi yönünü aydınlatılması ile hâkim, kişinin suçlu olup olmadığına yönelik bir kanaat sahibi olacaktır. İspatın gerçekleşmesi için suçluluğa inandırmak yetmez, bu konuda tam bir kanaat oluşmalıdır⁷⁵. Aksi durum masumiyet karinesini zedeleyecek bir sonuç yaratacaktır. Şüphenin tamamen ortadan kalkmadığı durumlarda, şüpheden sanık yararlanır (*in dubio pro reo*)⁷⁶. Türkiye'nin ceza muhakemesi hukuku sisteminin tahkike dayalı işbirliği sistemi özelliği taşıdığından delilin ve ispat sistemlerinin tarihçesi başlığı altında bahsedilmiştir⁷⁷. Bu nedenle, ispat için yenilmesi gereken şüphe de tahkik sistemindeki gibi olacaktır. Yani, yargılama sonunda yenilmesi gereken şüphe, her türlü şüphe olmayıp akla ve mantığa uygun gerekçelere dayanan şüphedir. Bunun aksine her türlü şüphenin yenilmesini beklemek, mutlak gerçeğe ulaşılmasını umut etmek olur ki, bu da imkânsızdır.

⁷¹ Alangoya/Yıldırım/Deren-Yıldırım, **a.g.e.**, s. 347.

⁷² 4721 sayılı Medeni Kanun, madde 6.

⁷³ Alangoya/Yıldırım/Deren-Yıldırım, **a.g.e.**, s. 338.

⁷⁴ Bkz. ss. 51-52.

⁷⁵ Öztürk/Erdem/Özbek, **a.g.e.**, s. 410; Yurtcan, **a.g.e.**, s. 168.

⁷⁶ Detaylı bilgi için bkz. Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, ss. 1334-1338.

⁷⁷ Bkz. s. 11.

“Şüpheden sanık yararlanır” kuralını sanık lehine uç noktalara götürmek, gerekçeye dayanan şüphenin yenilmesi zorunluluğunu, her türlü şüphenin yenilmesi seviyesine taşıyacaktır ki; bu da ceza muhakemesinin etkinliğini kabul edilemez oranda zayıflatacaktır⁷⁸.

Hukuksal meseleler ise ispat konusu olamazlar. Buna hâkimin hukuku kendiliğinden uygulaması kuralı (*iura novit curia*) denir⁷⁹. Hukuk fakültesi mezunu herkesin bilebileceği genel bilgileri ve hâkimlik stajını başararak mesleğe atanmış her hâkimin bilmesi gereken hukuk bilgisi ile çözümlenebilecek konularda, bilirkişiye başvurulamayacaktır⁸⁰. Nitekim CMK 63. maddesinde “...Ancak hâkimlik mesleğinin gerektirdiği genel ve hukuki bilgi ile çözülmesi olanaklı konularda bilirkişi dinlenemez.” denilerek, bu husus kanun tarafından da belirtilmektedir.

Bunlara ek olarak aşikâr vakıaların ispatlanmasına gerek duyulmaz⁸¹. Herkesçe bilinen (maruf) ve meşhur vakıalar aşikârdır. Örneğin yolda yürüyen bir insanın canlı olduğuna dair ispat için her hangi bir delil gerekmez. Bu durum ilgili bilginin belirli bir insan çevresiyle sınırlı olduğu durumlarda da geçerlidir⁸².

Ayrıca ceza muhakemesi hukukunda ikrarın ispat açısından sahip olduğu konumun, medeni usul hukukundaki ikrarın ispat açısından sahip olduğu konumla aynı olmaması gerekir. Nitekim hükmün verilmesinde hâkimin vicdani kanaatini ön plana çıkaran ceza muhakemesi sisteminde ikrarın, her delil gibi, hâkimi bağlamaması gerekir⁸³. Bu nedenle ikrarın ispata etkisi de medeni usul hukukundaki ikrar müessesesinin aksine daha zayıftır.

2. İspat külfeti

Bu noktada bir diğer önemli olan husus ceza muhakemesinde ispat külfetinin kimde olacağı meselesidir. Medeni usul hukuku mantığıyla düşünülürse, ispat

⁷⁸ Metin Feyzioğlu, **Ceza Muhakemesinde Vicdani Kanaat**, Ankara: Yetkin Yayınları, 2002, s. 197.

⁷⁹ Ancak eski veya yabancı hukuk gibi hâkimin hukuku bilmemesinin mazur görüleceği durumlar olabilir. Bkz. Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1399, dn. 11.

⁸⁰ Ali Parlar/Muzaffer Hatipoğlu/Erol Güngör Yüksel, **Açıklamalı-İçtihatlı Ceza Muhakemesi Hukukunda Deliller, Çapraz Sorgu ve İspat**, Ankara: Yayın Matbaacılık, 2008, s. 9.

⁸¹ Detaylı bilgi için bkz. Erem, **a.g.e.**, s. 365.

⁸² Roxin, **a.g.e.**, s. 268.

⁸³ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1379.

k lfetinin kiři i itham edenlerden iddia makamı olan savcıya ve bizzat iddia sahibi davacıya kalacağı   ylenecektir. Nitekim soruřturma sırasında davacı, iddiasını ortaya koyan delilleri savcıya sunar. Savcının soruřturma sırasında topladıđı delillerin su un iřlendiđi hususunda yeterli bir ř phe oluřturması halinde; savcı, ilgili mahkemeye kovuřturmaya ge ilmesi talebiyle bir iddianame d zenler (CMK 170). Ancak savcının g revi, sadece ř pheli aleyhine olan delilleri toplamak deđildir. Savcı ř phelinin lehine olan delilleri de toplayarak muhafaza altına almakla ve ř phelinin haklarını korumakla y k ml d r (CMK 160/2). Ayrıca ceza muhakemesi hukukunda h kimlerin resen delil arařtırması⁸⁴, delilleri tartıřması ve sistem olarak da delil serbestisi esasına g re hareket etmeleri de ispat k lfeti meselesine etki etmektedir⁸⁵. Bu nedenlerle ceza muhakemesi a ısından medeni usul hukukunda bulunan gibi bir ispat k lfeti sorunu yoktur. Zaten kiřinin kendisi ve yakınları aleyhine delil vermeye zorlanması yasađını i eren ve masumiyet karinesinin h kim olduđu bir sistem ile ispat k lfetinin varlıđı  eliřecektir⁸⁶.

III. Dijital delil kavramı

Ceza muhakemesi a ısından delil ve ispat kavramlarını yerine oturtttuktan sonra bu  alıřmanın asıl i eriđinin bulunduđu dijital delillere ge ilebilir. Nitekim dijital delilleri incelemeyen  nce, ceza muhakemesi a ısından delili ortaya koyarak dijital delilleri bu delil kavramının i erisine yerleřtirmek ve bu kavramın i eriđine g re yorumlamak gerekir.

Delil serbestisinin hakim olduđu bir ceza muhakemesi sisteminde her t r delil hakime vicdani kanaat vermede yardımcı olabilecektir⁸⁷. Bu nedenle iřbu ilkeden yola  ıkılarak dijital delillerin de delil deđerini haiz olduđunu   ylemek m mk nd r. Dijital delillerin kullanılması son zamanlarda artan teknolojik geliřmelerle,  zellikle de bilgisayar teknolojilerinin geliřimi ile birlikte, ortaya  ıkmıřtır. G n m zde iřlenen su ların da bu teknolojik geliřmeler ıřıđında bir evrim ge irdiđi ger eđi de g z  n ne alındıđında, dijital delillerin, her ge en g n, hukuk g ndeminde

⁸⁴ Centel/Zafer, **a.g.e.** , s. 651. Ayrıca h kimin resen delil arařtırmasının soruřturma evresinde bulunduđu ama CMUK 237/son'da d zenlenen fıkranın CMK'de yer almaması nedeniyle kovuřturma evresinde bulunmadıđına y nelik g r ř i in bkz. Kunter/Yenisey/Nuhođlu (2010), **a.g.e.** , s. 1342.

⁸⁵ Erem, **a.g.e.** , s. 362.

⁸⁶  zt rk/Erdem/ zbek, **a.g.e.** , s. 410.

⁸⁷ Daha  nce de belirtildiđi  zere, delillerin kabul edilebilirliđi a ısından delil serbestisine getirilen bazı sınırlamalar da mevcuttur. Bkz. s. 10 vd.

kendilerine daha fazla yer bulmaları da kaçınılmaz bir gelişme olacaktır. Özellikle “bilişim suçları”nın⁸⁸ sayıca artması ve çeşitlenmesinin yanı sıra, klasik suçların bilişim yöntemleri kullanılarak işlenmeye başladığı bir dönem içerisinde bulunmaktadır. Yani her tür suç açısından dijital delillere ulaşmak mümkün olabilmektedir. Aynı zamanda dijital deliller yoluyla canlandırılan olaylarda hâkimin suç bulmacasını çözmesi de kolaylaşmaktadır. Hatta mevcut şartlar altında kimi olayların dijital delillere başvurulmadan çözülmesi mümkün olmamaktadır. Bu yüzden dijital deliller zamanla klasik delillere göre tercih edilir hale gelmişlerdir. Günler ilerledikçe ceza muhakemesi alanındaki kolluk, savcı ve hâkimlerin de dijital delil içeren olaylarla karşılaşma sıklığı da artmaktadır⁸⁹. Teknolojinin yoluna durmaksızın, hatta bir ivme ile devam etmesi kuşkusuz ki dijital delillerin daha çok önem kazanmasına öncülük eden bir faktör olacaktır. Peki dijital deliller nelerden oluşmaktadır? Bu soruya cevap verebilmenin yolu da kuşkusuz olarak dijital delil kavramının detaylı olarak incelenmesinden geçmektedir.

Dijital delil (*fr. preuves numériques, ing. digital evidence*) ortaya yeni çıkan bir kavram olduğu için normların içerisinde hiçbir şekilde tanımlanmamakla birlikte, doktrinde ise pek çok farklı şekilde tanımlanmış bulunmaktadır.

⁸⁸ Bilişim suçu kavramı konusunda doktrinde bir tartışma mevcuttur. Doktrinde Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, İstanbul: Alfa Yayınevi, 1997, “bilgisayar suçları” terimini kullanırken; Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul: Beta Yayınevi, 2001 ve İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye’de Durum**, Ankara: Adalet Yayınevi, 2008 “siber suç” terimini kullanmaktadır. Caner Yenidünya/Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003; Hatice Akıncı/A. Emre Alıç/Cüneyd Er, “**Türk Ceza Kanunu ve Bilişim Suçları**”, İnternet ve Hukuk, Yeşim Atamer (der.), İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004; Muammer Ketizmen, **Türk Ceza Hukuku’nda Bilişim Suçları**, Ankara: Adalet Yayınevi, 2008; Zakir Avşar/Gürsel Öngören, **Bilişim Hukuku**, İstanbul: Pasifik Ofset, 2010; Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 4. Baskı, Ankara: Seçkin Yayıncılık, 2012 ve Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014 “bilişim suçları” terimini tercih edenlerdir. Bu çalışmada da bilişim suçu terimi kullanılacaktır.

Bu konudaki tartışmayla ilgili bir sonuç çıkarılması için öncelikle tüm bu kavramların daha iyi anlaşılması gerekmektedir. TCK 243.-245. maddeleri arasındaki suçları bilişim alanında suçlar olarak adlandırmıştır. Bunun yanı sıra klasik nitelikteki bazı suçların (hırsızlık ve dolandırıcılık) bilişim sistemleri kullanılarak işlenmesinden de bahsedilmiştir. Türk ceza hukuku doktrininde de “bilişim suçu” teriminin yaygın olarak kullanılmaktadır. Ancak bu konuda bir uzlaşma bulunmamaktadır. Avrupa’da Avrupa Konseyi’nin bu konuda en geçerli metni olan Siber Suçlar Sözleşmesi (*Convention on Cybercrime*)’nin de etkisiyle “siber suç” terimi yaygınlaşsa da bu konuda da net bir uzlaşının bulunduğunu söylemek zordur. Özellikle Türkiye’deki resmi çeviride bu sözleşmenin isminin “Sanal Ortamda İşlenen Suçlar Sözleşmesi” olduğuna da dikkat çekmek gereklidir. ABD’de ise bilgisayar suçları anlamına gelen “*computer crimes*” terimi hala yaygınlığını korumaktadır.

⁸⁹ Eoghan Casey, **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**, 3. Edition, Londra: Academic Press, 2011, s. 9.

Bunlardan birine göre dijital deliller, “*Adli bilişimle ilgili bir çalışma esnasında, bilişim sistemleri (bilgisayarlar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli deliller*” olarak tanımlanmışlardır⁹⁰.

Dijital delil kavramının tercih edilmediği bir başka eserde bu deliller elektronik deliller olarak şu şekilde tanımlanmışlardır: “*Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir.*”⁹¹. Yine elektronik delil kavramı bazı diğer eserlerde de tercih edilmektedir⁹².

Yine yabancı doktrinde de gerek elektronik deliller gerekse dijital deliller kavramının pek çok farklı kişi tarafından değişken biçimde kullanıldığı da görülmektedir⁹³.

Tüm bu incelemelerden görüldüğü üzere daha henüz dijital delil kavramının kullanımı üzerinde bile uzlaşa sağlanamamıştır. Hatta bu kavramın yerine elektronik delil kavramının kullanıldığı görülmektedir. Ancak bu çalışma boyunca tercih edilecek olan kavram dijital delil olacaktır. Bunun da nedenleri dijital delil-elektronik delil kavramlarının benzerlikleri ve farklarının değerlendirileceği başlık içerisinde detaylı olarak açıklanacaktır⁹⁴.

Bunun yanı sıra yukarıdaki tanımlarda görüldüğü üzere, belli kavramların detaylı bir şekilde incelemesi yapılmadan, dijital delillerin niteliklerini de anlamının pek mümkün olmayacağı söylenebilecektir. Bu yüzden bu konuda yer alan diğer kavramların da detaylı bir şekilde incelenmesi gerekecektir.

⁹⁰ Türkay Henkoğlu, **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, 2. Baskı, İstanbul: Pusula Yayıncılık, 2014, s. 5.

⁹¹ Leyla Keser Berber, **Adli Bilişim**, Ankara: Yetkin Yayınları, 2004, s. 46.

⁹² Ergün, **a.g.e.**, s. 49; Karagülmez, **a.g.e.**, s. 443 vd.

⁹³ Örneğin Casey ve Orin S. Kerr, “**Digital Evidence and the New Criminal Procedure**”, Columbia Law Review, Ocak 2005, s. 279 vd. içerisinde dijital delil kavramını tercih etmekte iken Stephen Mason, “**Introduction**”, Stephen Mason (ed.), International Electronic Evidence, Londra: British Institute of International and Comparative Law, 2008 içerisinde elektronik delil ile dijital delil kavramlarının ikisini birden kullanmakta, ancak bu kavramların içerikleri açısından farklılık gösterdiklerini ifade etmektedir.

⁹⁴ Bkz. s. 24.

A. Dijital delil – elektronik delil kavramlarının benzerlikleri ve farkları

Dijital delil ile elektronik delil kavramlarının benzerlikleri ve farklarının görülebilmesi için dijital ve elektronik kavramlarının detaylı olarak açıklanması gereklidir. Böylece kullanılacak kavramın seçimini sağlayan hususlar da ortaya çıkacaktır. Bu noktada öncelikle elektronik kavramı incelenecektir.

1. Elektronik kavramı

Elektronik, maddenin eksi yüklü elektronlarının serbest hareketlerini ve bu hareketi denetleyerek oluşturulan yapıları konu edinir⁹⁵. Yani temel olarak, maddenin elektriksel özelliklerini kullanarak güç iletimiyle, bunu oluşturan sistemlerle ilgilenir. Dolayısıyla maddenin elektriksel özelliklerini kullanan tüm aygıtlar için geçerli bir üst terimdir. Bu durumda elektronik deliller de elektronik bir aygıt aracılığıyla üretilen, işlenen, depolanan veya iletilebilen, hükmün verilmesine etki eden verilerdir⁹⁶.

Tüm bu elektronik hareketlerin matematiksel fonksiyon olarak gösterilmesine sinyal denilmektedir. Dolayısıyla sinyaller, elektronik açısından veri hareketini sembolize etmektedirler. Bu veriler ise, analog ve dijital olmak üzere ikiye ayrılmaktadırlar⁹⁷. Yani dijital veriler elektronik içerisinde kullanılan bir tür sinyal çeşidi olmaktadır.

Tüm bu tanımlardan görüleceği üzere elektronik kelimesi, dijital kelimesine göre daha geniş bir alanı kapsamaktadır. Bu noktada dijital kelimesini daha iyi anlayabilmek için, elektronik alanında elektrik sinyallerinin iki farklı çeşidini oluşturan analog ile dijital kavramlarının da ayrımının yapılması gereklidir.

⁹⁵ Karagülmez, **a.g.e.** , s. 41.

⁹⁶ **Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk**, Ankara: Ankara Barosu Yayınları, 2009, s. 173.

⁹⁷ Mason, **a.g.e.** , s. xxxv.

2. Analog kavramı

Analog sözcüğü köken olarak Fransızca'daki “*analogue*” kelimesinden türemiştir ve “*Benzer, eş*” anlamlarına gelmektedir⁹⁸. Yani değişik yapılarda olmasına rağmen aynı görevi yapanlar analog olarak adlandırılmaktadır. Analog sinyaller ise, giriş sinyalinin bazı başka sinyaller ile elektriksel işlemler geçirilerek değiştirilmesi ile elde edilir. Dolayısıyla, giriş sinyali ve çıkış sinyali arasındaki bu süreklilik bir matematiksel formül ile gösterilebilir. Ancak bu iki nokta arasındaki sinyallerin değerleri çok çabuk değişmekle birlikte, her an farklıdır ki bu nedenle sonsuz sayıda ara değer söz konusudur⁹⁹. Bu nedenle analog verilerin değiştirilmesi imkânsız olmasa da ustalık ister ve zordur¹⁰⁰.

3. Dijital kavramı

TDK Güncel Sözlük'e göre dijital kelimesi de Fransızca'dan Türkçe'ye geçmiş olup “*Sayısal*” anlamına gelmektedir¹⁰¹. Dijital kelimesi içerisinde Latince *digit* kökünü barındırmakta ve bir şeyin sayılarla doğrudan olan bağlantısı ortaya koymaktadır.

Dijital sinyal, içerik olarak 0 ve 1'lerden oluşan ikili kod sisteminin kullanılmasıyla oluşturulur. Burada 1 ile akımın geçme anı, 0 ile ise geçmeme anı gösterilmektedir¹⁰². Bu kod sisteminde veriler rakamların arka arkaya dizilmesi ile elde edildiği için üzerinde kolaylıkla değişiklik yapılabilir. Buna ek olarak, bir dijital veriye hata düzeltme kodları eklenerek, söz konusu verinin bozulsa bile tamir edilebilmesi sağlanabilir. Ayrıca, bir dijital veri gönderilirken başka bir dijital veri ile aynı ortama konulup gönderilebilir. Yine bu tür veriler rahatlıkla şifrelenebilir.

4. Değerlendirme

Görüldüğü gibi, dijital veriler ile analog veriler arasındaki en büyük fark, analog verilerin sürekli olan bir ölçekte ve iki nokta arasında tüm değerleri alabilecek

⁹⁸ TDK Güncel Sözlük.

⁹⁹ Karagülmez, **a.g.e.** , s. 41.

¹⁰⁰ Mason, **a.g.e.** , s. xxxv.

¹⁰¹ TDK Güncel Sözlük.

¹⁰² Karagülmez, **a.g.e.** , s. 41.

şekilde var olmaları iken, dijital verilerin ise yalnızca belli değerlerden oluşan rakamlarla sınırlı olan, sürekli olmayan bir ölçekte ve kesikli olarak var olmalarıdır¹⁰³. Bu arada unutulmadan belirtilmelidir ki günümüzde gerek analog veri dijitalle, gerekse dijital veri analoga rahatça çevrilebilmektedir¹⁰⁴.

Yaşadığımız süreç içerisinde bilgi çağında bulunduğumuz ileri sürülmekte ve bu çağı başlatan sürecin bilgisayar teknolojilerinin gelişmesiyle oluştuğu belirtilmektedir¹⁰⁵. Tarım ve endüstri devrimleri ile başlayan bilginin en güçlü ekonomik değer haline gelmesi süreci, bilginin depolanması ve iletilmesi kaynaklarının gerek kapasiteleri gerek olanakları nedeniyle dijital teknolojiye sahip aygıtlara kayması sonucunda bir anlamda dijital devrim olarak adlandırılabilir bir değişim meydana getirmiştir. Bu değişimin sonucu olarak ise bilgi iletimi ve depolama ile ilgili olarak kullanılan klasik yöntemlerin yanı sıra analog teknolojiler de yerlerini dijital teknolojiye sahip aygıtlara bırakmaktadır¹⁰⁶.

Az önce verilen dijital devrim örneklerinde de görüldüğü gibi elektronik yapıya sahip her aygıt dijital veri içermemektedir¹⁰⁷.

Sonuç olarak, dijital delillerin elektronik yapıda bulunması inkâr edilmemekte, ancak sadece dijital halde bulundukları durumlarda dijital delil olarak değer ihtiva edecekleri belirtilmektedir. Yani dijital teriminin teknik anlamı açısından bu tür delillerin de elektronik delil olarak değil, dijital delil olarak adlandırılmaları da daha doğru olacaktır. Böylece elektronik delil-dijital delil arasındaki kavram kargaşası da çözülmüş olacaktır. Zaten doktrinde elektronik delil kavramı kullanılsa da, bunun içerisinde bahsedilen hususlar dijital teknolojiye yöneliktir.

¹⁰³ Fatoş Tünay Yarman-Vural/Yusuf Murat Erten, **Bilgisayar Sistemleri**, 5. Baskı, Ankara: Akademi Yayıncılık, 2000, s. 19.

¹⁰⁴ Bu işleme modülasyon denmektedir. Bilgi için bkz. Yarman-Vural/Erten, **a.g.e.**, s. 281; Hatta bu teknolojiler artık bir bütün içerisinde kullanılmaktadır. Örneğin, dijital veri kullanan modem ve ekran kartı gibi aygıtlar analog veriler de kullanır. Ancak sabit hatlı telefon ve antenli televizyon gibi aygıtlarda ise tamamen analog veri alışverişi vardır.

¹⁰⁵ Donald H. Sanders, **Computers Today**, 2. Edition, Singapur: McGraw – Hill Book Company, 1986, s. 78.

¹⁰⁶ Klasik ve analog teknolojiden dijitalle evrilen teknolojilere bazı örnekler olarak; plakların CD ve MP3'e, daktilonun yazıcıya, analog fotoğrafların (negatif filminden oluşturulan) dijital fotoğraflara, analog televizyon yayınının (doğrudan anten ile alınan) dijital televizyon yayınına, VHS kasetlerinin VCD, DVD VE Blu-Ray'a, ankesörlü ve sabit hatlı telefonların cep telefonlarına, mektubun e-mail, SMS, MMS ve sosyal ağlar yoluyla iletişime ve kitapların e-kitaplara dönüşmesi verilebilir.

¹⁰⁷ Karagülmez, **a.g.e.**, s. 41.

Bunlara ek olarak hukuki düzenlemelerin hayatın gerisinde kalmaya mahkûm oldukları da belirtilmelidir. Zaten mevcut durumda var olmayan ve gelecekte var olacağı düşünülen bir şey hakkında doğrudan düzenleme yapmak mantıklı olmayacaktır. Bu durumda önemli olan husus, günümüzdeki mevcut durumu düzenlemektir. Bu yüzden gelecekte dijital teknoloji yerini yeni bir teknolojiye bırakırsa diye de elektronik kavramını kullanmak doğru görünmemektedir.

Tüm bunlar bir kenara bırakılırsa, elbette elektronik delil kavramı daha kapsayıcıdır. Ancak bu kapsayıcılık analog deliller açısından sıkıntı yaratabilir. Her ne kadar kullanım alanları daralsa da farklı yapıları nedeniyle, analog deliller için dijital delillerden farklı hukuki düzenlemeler yapmak gereklidir¹⁰⁸.

Türkiye’de elektronik, analog ve dijital kavramlarının hukuk düzenlemeleri içerisinde ne şekilde yer bulduğuna bakıldığında ise gerek elektronik gerekse dijital kelimelerin kullanıldığı düzenlemeler bulunmaktadır.

CMK’de kullanım açısından “elektronik” kavramı tercih edilmiştir. CMK 43/2’de tanıkların çağrı usullerinde elektronik postanın kullanımından bahsedilmektedir. Yine 2012 yılında getirilen CMK 38/A maddesi ile UYAP üzerinden yapılacak elektronik işlemler düzenlenmiştir. “Analog” ve “dijital” kelimelerine ise CMK’de yer verilmemiştir. TCK’de de 6/1-g ve 297/1 maddelerinde “elektronik” kelimesinin kullanıldığı görülmektedir. Yine ne “analog” kelimesi ne de “dijital” kelimesi TCK kapsamında hiç kullanılmamaktadır.

Yine 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun’un 3/3, 6/A-5 ve ek madde 1 içerisinde “elektronik” teriminin kullanımı dikkat çekmektedir. Yine ne “analog” kelimesi ne de “dijital” kelimesi bu kanunda da bulunmamaktadır.

¹⁰⁸ **Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk**, s. 173; bu nedenle dijital teknolojiye uyarlanmamış bu gibi eşyadan elde edilen veriler de dijital delil kapsamında kabul edilemez. Bunlar ancak elektronik delilin diğer türü olacak olan analog delil olabilirler. Bu nedenle bu tür eşyayı da dijital delil kapsamından farklı bir yere ayırmak gerekir.

5070 sayılı Elektronik İmza Kanunu'nda da “elektronik” kelimesi hem kanunun adında hem de içeriğinde kullanılmış, “analog” ve “dijital” kelimeleri ise kendilerine yer bulamamışlardır.

6502 sayılı Tüketicinin Korunması Hakkındaki Kanun'un 3/f, 3/h, 6/1, 49/2, 77/17 ve 80 maddelerinde de “elektronik” kelimesi bulunmakta, “analog” ve “dijital” kelimeleri yine kendilerine yer bulamamaktadırlar.

4630 sayılı Kanun ile getirilen değişiklikler sonrası 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 5. maddesinde “elektronik” kelimesi kendisine yer bulurken, 25 ve 72/1 maddelerinde “dijital” kelimesi kullanılmaktadır. “Analog” kelimesi bu kanunda da bulunmamaktadır.

5809 sayılı Elektronik Haberleşme Kanunu ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da da “elektronik” kavramı temel alınmıştır.

Sonuç olarak Türkiye’de kanun düzenlemelerinde elektronik kavramının daha geçerli olduğu görülmektedir. Hatta görüldüğü kadarıyla düzenlemeler içerisinde “dijital” kelimesinin neredeyse tesadüfen yer aldığı söylenebilir.

B. Veri kavramı

Bu noktada yukarıdaki bahsedilen hususlardan da açıkça anlaşılabileceği üzere dijital delil ve veri kavramları arasında da sıkı bir ilişki bulunmaktadır. Nitekim dijital delil kavramını oluşturan ana ve temel unsura bakıldığında veri kavramı öncelikli olarak dikkat çekmektedir. Bunun nedenleri ise veri kavramının, hem dijital delili oluşturan çekirdek olması, hem de hukuk düzenince kabul edilen uluslararası ve yerleşmiş bir kavram olmasıdır. Dolayısıyla veri kavramının tanımının yapılmasıyla, dijital delil kavramının içeriği de biraz daha netleşecektir.

TDK Güncel Sözlük’e göre verinin pek çok anlamı vardır. Ancak konumuzu ilgilendiren anlamlarına bakacak olursak veri (*ing. data, fr. donnée*); “Bilgi, data” ve bilişim bilimi açısından ise “Olgu, kavram veya komutların, iletişim, yorum ve işlem

için elverişli biçimli gösterimi” olarak tanımlanmıştır¹⁰⁹. Kriminal Terimleri Sözlüğü’ne göre veri; adli bilişim incelemeleri açısından işlenebilir duruma getirilmiş sayısal niceliktir¹¹⁰. Bilişim Terimleri Sözlüğü’ne göre ise veri; “*Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi. Elverişlilik, kişiler ya da özdevimli makinelerle iletişim, yorum ya da işleme uygunluk biçiminde düşünülür.*” şeklinde tanımlanmıştır¹¹¹. Ayrıca yine bu son tanımın sonunda veri ile bilgi arasındaki anlamsal ilişkiye de değinilmiştir.

Tüm bu veri tanımlarından ve açıklamalardan da görüldüğü üzere veri ile bilgi arasında önemli bir bağlantı bulunmaktadır. Bu nedenle bilginin de tanımının yapılması konunun açıklığa kavuşması açısından yararlı olacaktır. TDK Güncel Sözlük’e göre bilginin de veri gibi pek çok anlamı vardır. Bu tanımlara göre bilgi (*ing. information, fr. information*); “*İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat*”, “*Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf*”, “*İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf*” ve bilişim bilimi açısından ise, “*Kurallardan yararlanarak kişinin veriye yönelttiği anlam*” olarak tanımlanmıştır¹¹². Bilgisayar Terimleri Karşılıklar Kılavuzu’na göre ise bilgi; işlemde kullanılan uzlaşımsal kurallardan yararlanarak kişinin veriye yönelttiği anlam olarak tanımlanmıştır¹¹³. Yani görüldüğü gibi bilgi insan tarafından ulaşılabilecek gerçeği temsil etmektedir. Kısacası veri, bilgilerin belirli bir formata dönüştürülmüş halidir¹¹⁴. Konuyla ilgisi açısından bakıldığında ise bilgiye erişimin verilerin değerlendirilmesi yoluyla olacağı görülmektedir. Yani değerlendirme açısından temel unsur yine veri olmaktadır.

Tüm bu parçalar bir araya getirildiğinde veri ile bilgi kavramlarının TDK Güncel Sözlük’te eş anlamlı gibi verilmesinin doğruluğu tartışılabilir¹¹⁵.

¹⁰⁹ TDK Güncel Sözlük.

¹¹⁰ TDK BSTS Kriminal Terimleri Sözlüğü, http://www.tdk.gov.tr/index.php?option=com_bilimsanat. (Erişim tarihi: 11.04.2014)

¹¹¹ TDK BSTS Bilişim Terimleri Sözlüğü, http://www.tdk.gov.tr/index.php?option=com_bilimsanat. (Erişim tarihi: 11.04.2014)

¹¹² TDK Güncel Sözlük.

¹¹³ TDK BSTS Bilgisayar Terimleri Karşılıklar Kılavuzu, http://www.tdk.gov.tr/index.php?option=com_bilimsanat. (Erişim tarihi: 11.04.2014)

¹¹⁴ Sanders, **a.g.e.**, s. 10; Yazıcıoğlu, **a.g.e.**, s. 29.

¹¹⁵ Nitekim veri, *data* kelimesinin karşılığı iken; bilgi ise, *information* kelimesine karşılık gelmektedir. Bu konudaki tartışma için bkz. Dülger, **a.g.e.**, s. 79, dn. 103.

Konuyla ilgili olarak mevzuata bakıldığında veri ile ilgili olarak bazı tanımların yapıldığı görülmektedir.

Örneğin, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile getirilen veri ve bilgi tanımları mevcuttur. İşbu kanunun tanımlar başlıklı 2. maddesinde veri, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer; bilgi ise, verilerin anlam kazanmış biçimi olarak tanımlanmaktadır.

Ayrıca 5070 sayılı Elektronik İmza Kanunu 3. maddesinde elektronik verinin tanımı, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar olarak yapılmıştır.

Yine henüz yasalaşmasa da Kişisel Verilerin Korunması Kanunu Tasarısı'nın 3. maddesinde kişisel veri, belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler olarak tanımlanmaktadır.

Veri kavramı, tüm bu tanımlarda farklı şekillerde ele alınmış olsa da, tüm tanımlar açısından ortak kabul edilen bir husus vardır ki, o da verinin bir kayıt ya da bilgiyi ifade etmesinin yanında daha çok, hukuki bir kavram ve çekirdek değer olmasıdır. Çekirdek değer olan veriler gerek dijital deliller gerekse elektronik deliller açısından temel unsuru oluşturmaktadırlar. Bu ortak çekirdek değer hukuki düzenlemeler açısından kullanılacak ana kavram olmalıdır.

C. Bilişim kavramı

Yukarıdaki veri tanımlarından da yola çıkılarak, verilerin her ne kadar elverişli bir gösterimi içerdikleri kabul edilse de bu elverişliliğin sadece belli yöntemler aracılığıyla gerçekleşmesi mümkündür.

Örneğin veri ile bilgi kavramlarının karşılaştırılması sonucunda bilgiye erişimin, verilerin değerlendirilmesi yoluyla yapılacağı ortaya konulmuştu. Bu durumda verilerin değerlendirilmesi ile ortaya çıkan bu bilgileri, hâkimlerin beş duyusuyla algılayabileceği, yani değerlendirebileceği hale kim getirecektir? Hâkim

bu işi kendiliğinden mi yapacaktır yoksa bu iş taraflar tarafından mı yapılacaktır? Yani bilgi haline dönüşen veriler dijital delil olarak hukuk alanına nasıl dâhil olacaklardır? Tüm bu soruların cevabını verecek olan bir alan mevcuttur. Bu alan ise bir bilim dalı olan bilişimdir.

TDK Güncel Sözlük’e göre bilişim, “*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*” olarak tanımlanmaktadır¹¹⁶. Bilişim Terimleri Sözlüğü’ne göre bilişim (İng. *informatics*, fr. *informatique*) ise; “*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevim alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır.*” olarak tanımlanmıştır¹¹⁷. Bu son tanımda aynı zamanda bilişim kelimesi ile enformatik kelimesinin eş anlamlı olduğu belirtilmiştir.

Bilişim kelimesi bir endüstrinin tümünü karşılayan bir üst kavram olmakla birlikte, kelimenin oluşumunda bilgi-işlem ve iletişim kavramlarının bir araya geldiği görülmektedir. Dolayısıyla bilişim, bilgi-işlem¹¹⁸ ve iletişime yönelik fonksiyonların bir arada bulunduğu elektroniğin ifade edilme şekli de olmaktadır¹¹⁹.

Yukarıdaki açıklamalardan görüldüğü üzere hukukun dijital delilleri anlamlandırabilmesi için gerekli yardım bilişim bilimi tarafından verilecektir. Bilişim

¹¹⁶ TDK Güncel Sözlük.

¹¹⁷ TDK BSTS Bilişim Terimleri Sözlüğü.

¹¹⁸ Bilişim kavramının bilgiyi değil, veri-işlem ve veri iletişimi kapsadığı hakkındaki görüş için bkz. Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin Yayıncılık, 2014, s. 53.

¹¹⁹ Akıncı/Alıç/Er, **a.g.e.**, s. 170.

bilimi yardımıyla elektronik aygıtlardan alınan bilgiler, beş duyuyla algılanabilir ve akılcı olarak düzenlenerek insanlar tarafından anlamlandırılabilir hale getirilecek, böylece hâkimler bilgilerden oluşan dijital delilleri değerlendirebilir hale geleceklerdir. Bu noktada nasıl ki tıp biliminin hukuka yardım ettiği tıbbi uzmanlık gerektiren alan adli tıp olarak adlandırılmışsa, dijital delillerin elde edilmeleri açısından kullanılan yöntemler konusunda yardım alınan bilim dalının adının bilişim olmasından dolayı, işbu alana da adli bilişim adı verilmiştir¹²⁰. Böylece adli bilişimin adli bilimler içerisinde bir alt dal olduğunun söylenmesi de sakınca yaratmayacaktır¹²¹. Adli bilişim konusuna dijital delillerin elde edilmesi ve ispat gücü başlığı altında daha detaylı bir biçimde değinilecektir¹²².

IV. Dijital delillerin özellikleri

Tüm bu tanımlardan ve açıklamalardan da açıkça anlaşılacağı üzere dijital deliller, ceza muhakemesindeki klasik delillerden farklıdırlar. Dolayısıyla dijital delil kavramını ele aldıktan sonra dijital delillerin çeşitleri ve elde edilmesinden bahsetmeden önce, dijital delillerin sahip oldukları özellikleri ortaya koymak mantıklı olacaktır. Nitekim dijital deliller, özellikleri açısından da klasik delillere göre farklılık taşıyacaklardır. Kendilerine has bu özellikleri açıklamak, hem dijital delil çeşitlerinin belirlenmesi hem de dijital delil elde etme sürecinde uygulanacak farklı yaklaşımların kaynağına inmek açısından yararlı olacaktır.

Dijital delillerin özelliklerini iki farklı kategori altında incelemek doğru olacaktır. Bunlardan birinci olan kategorinin içerdiği özelliklerin, aynı zamanda ceza muhakemesi sisteminin bütünlüğü açısından da dijital delillerde mutlaka bulunması gerekir. Buna göre, dijital delillerin genel özellikleri başlığı altında az sonra bahsedilecek olan gerçekçilik hariç tüm özelliklere¹²³ sahip olmaları gereği bulunmaktadır. Bu özellikleri hızlıca sayacak olursak dijital delil; hukuka uygun, akla uygun, olayı temsil edici, ispat bakımından önemli, müşterek, sağlam, güvenilir ve elde edilebilir olmalıdır. Zaten bu özellikler ceza muhakemesinde delilin sahip olması gereken temel özelliklerdir. Dijital deliller de ceza muhakemesindeki diğer

¹²⁰ Keser Berber, **a.g.e.** , s. 39.

¹²¹ Değirmenci, **a.g.e.** , s. 65.

¹²² Bkz. s. 46 vd.

¹²³ Gerçekçilik konusundaki problem için bkz. s. 35.

tüm deliller gibi bu özelliklere uygun olmalıdırlar. Uygulamada özellikle dijital delillerin elde edilmeleri açısından hukuka uygunluk ile sağlamlık ve güvenilirlik üzerine pek çok problem çıkmaktadır.

A. Delillerin genel özellikleri açısından

Delil ve ispat sistemlerinin tarihi süreç içerisinde hukuk sistemleri içerisinde nasıl kabul edildikleri, delil ve ispat kavramlarının ceza muhakemesi açısından neyi ifade ettiği açıklanırken delil serbestisinden bahsedilmiştir. Böylece sanki her ispat aracının delil sayılabileceği sınırsız bir delil algısı yaratılmıştır. Ancak delillerin, ceza muhakemesi hukuku çerçevesinde kullanılabilmesi için, belli özelliklere sahip olmaları gerekir. Her ispat vasıtasına delil denemez¹²⁴. Nitekim daha önce de belirtildiği gibi delil serbestisinin getirdiği özgürlük, bu serbestinin sınırsız bir serbesti içerdiği şeklinde algılanmamalıdır. Aşağıda sayılan özelliklere sahip olmayan ispat vasıtalarının, ya hâkim tarafından duruşmada ortaya konulmaları reddedilecek, ya da ortaya konulmaları halinde hükme dayanak olmaları mümkün olmayacaktır. Aksi durumun verilen hükmün hukuka aykırı olması sonucunu doğuracağı söylenmektedir¹²⁵. Dijital delillerin de kabul edilebilirlikleri açısından delillerin genel olarak sahip olması gereken bu özelliklere uygunluk göstermeleri beklenecektir.

1. Hukuka uygunluk

Bir delil her şeyden önce hukuka uygun olmalıdır¹²⁶. Bu husus Anayasa'nın 38. maddesinin 6. fıkrası ile güvence altına alınmıştır. Ancak Anayasa'nın 38. maddesinde; “*Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez.*” denilmesi ile kanuna aykırı şekilde elde edilen bulguların delil olarak değerlendirilemeyeceği ortaya konmuştur. Aynı husus delillerin elde edilmesi konusundaki kuralları belirleyen CMK'de de kendine yer bulmuş, bu tür delillerin hâkim tarafından reddedilmesi gereği belirtilmiştir (CMK 206/2-a ve ayrıca CMUK 238/2-a). Kanunda ispat açısından, sadece hukuka uygun delillerin kullanılabilceği

¹²⁴ Öztürk/Erdem/Özbek, **a.g.e.** , ss. 411-412.

¹²⁵ Centel/Zafer, **a.g.e.** , s. 199.

¹²⁶ Centel/Zafer, **a.g.e.** , s. 199; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1331; Öztürk/Erdem/Özbek, **a.g.e.** , s. 412.

de ayrıca belirtilmiştir (CMK 217/2). Tüm bu tanımlamalar sebebiyle hukuka uygunluğun tersi olarak hukuka aykırılık ve kanuna aykırılık ikilemi ortaya çıkmıştır. Ancak hukuka aykırılık, kanuna aykırılıktan daha geniş bir anlama sahiptir. Nitekim Anayasa'ya, 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. Kanuna aykırılık ise sadece kanunla sınırlı olacaktır. Çünkü kanunda yer almayan bir husus, başka bir norm içerisinde bulunuyor olabilir. Bu durumda kanuna göre uygun gözüken bir hal, bütünlük arz eden bir kavram olan hukuka aykırı olabilir. Tüm bu açıklamalardan da anlaşılacağı üzere, ulusal normlar aracılığıyla açıkça yasaklanmış yöntemlerle elde edilen deliller ve herhangi bir yasaklama bulunmasa da diğer normlara aykırı biçimde elde edilen deliller tartışmasız biçimde hukuka aykırıdır.

Yukarıda bahsedilenlerin dışında ulusal normların sessiz kaldığı ve evrensel kurallara aykırılık oluşturan yöntemlerle elde edilen delilleri de hukuka aykırı kabul etmek bir hukuk devleti açısından zorunludur¹²⁷. Bu yüzden hukuka aykırılık denildiğinde; *“gerek pozitif hukuk metinlerine gerekse kişilerin temel hak ve hürriyetlerine ilişkin evrensel hukuk ilkelerine aykırılık bulunup bulunmadığı da gözetilmeli ve aykırılığın varlığı halinde hukuka aykırılığın mevcudiyeti kabul edilmelidir”*¹²⁸. Bu kurallara uymadan elde edilen ispat vasıtaları hukuka aykırılık nedeniyle delil değeri kazanamayacağından, hâkim tarafından da herhangi bir şekilde değerlendirmeleri yapılmamalıdır¹²⁹.

¹²⁷ Güçlü Akyürek, **“Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu”**, Türkiye Barolar Birliği Dergisi, Sayı: 101, Temmuz 2012, s. 63.

¹²⁸ AYM 22.06.2001-2/2, Resmi Gazete, Tarih: 05.01.2002, No:24631 (Mükerrer); Centel/Zafer, **a.g.e.**, s. 653; Ünver/Hakeri, **a.g.e.**, s. 157.

¹²⁹ Hukuka aykırı elde edilen delillerin değerlendirilmesi üzerine görüşler için Centel/Zafer, **a.g.e.**, ss. 658-666.

Anglosakson ceza hukuk sisteminde, hukuka aykırı delillerin ve hatta bu deliller yoluyla ulaşılan delillerin (zehirli ağacın meyvesi de zehirlidir ilkesi) de hukuka aykırı olduğu ve yargılamada kullanılamayacağı kabul edilmekte iken; Kıta Avrupası ceza hukuku sisteminde ise, zedelenen hakkın önemli bir hak ihlal oluşturup oluşturmadığı veya zedelenen hakların yarıştırılması gibi yöntemler de kullanılarak değerlendirme yapılmaktadır.

Kanunun hem eski (CMUK 254/2), hem de mevcut (CMK 217/2) halinde ve yine Yargıtay'ın verdiği kararlarda (her ne kadar bu konuda verilen değişik nitelikte kararlar bulunsun da) Türk Ceza Hukuku sisteminde de aynı Anglosakson hukuk sistemindeki gibi hukuka aykırı delillerin mutlak değerlendirme yasağına tabi olduğu görüşü kabul edilmiştir.

2. Gerçekçilik

İkinci olarak deliller, gerçekçi olmalıdırlar¹³⁰. Gerçekçi olmak demek delillerin soyut değil somut olması, dolayısıyla gerçeğin bir parçasını oluşturmaları gereğidir. Yani insanların sahip olduğu beş duyuyla algılanabilecek bir niteliğe sahip olmalıdırlar. Bu husus dijital deliller açısından tartışılabilir. Nitekim dijital delillerin kendilerine has özelliklerinde de görüleceği üzere dijital deliller gayrı maddi olarak gizli bir yapıya sahiptirler¹³¹. Dolayısıyla bazı araçlar veya yöntemlerle somut, yani insanların duyu organlarıyla algılayabilecekleri, bir hale getirilmeye ihtiyaç duyarlar. Bu nedenle gerçekçilik özelliğinin dijital delillerin bulunduğu bir ceza muhakemesi sisteminde bulunması çelişkiye yol açabilir.

3. Akla uygunluk (Rasyonellik)

Üçüncü olarak ise deliller, akılcı olmalıdırlar¹³². Delil sistemleri tarihçesinde de bahsedildiği üzere, inanca dayalı delil sistemi ile son bulan akıl dışı delillerin, günümüz modern hukuk sistemlerinde kabul edilmesi mümkün değildir. Hâkimi hükmü verme konusunda ikna edecek delillerin, maddi gerçeği de akla uygun (rasyonel) ve mantık kuralları çerçevesinde yansıtabilmesi gereklidir. Bu nedenle delil olarak kabul edilecek ispat vasıtalarının, bilim tarafından da kabul edilebilir olmaları aranmalıdır. Bu duruma örnek olarak, hâkimin kararını herhangi bir şekilde batıl inanca ya da fala bağlayamaması gösterilebilir. Bu noktada ayrıca yeminin delil olarak değeri tartışma konusu yapılabilir. Nitekim akılcı bir delil sisteminde yeminin delil olması mümkün olmayacaktır¹³³.

4. Olayı temsil edicilik (Maksada elverişlilik)

Bunlara ek olarak deliller, olayı temsil edici olmalıdırlar¹³⁴. Ceza muhakemesinde amaç, daha önce de bahsedildiği gibi, geçmişteki suça konu olabilecek olayı aydınlatmaktır. Bu nedenle delilin de olayın tamamını ya da bir

¹³⁰ Centel/Zafer, **a.g.e.** , s. 199; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1328; Öztürk/Erdem/Özbek, **a.g.e.** , s. 412.

¹³¹ Bkz. s. 37.

¹³² Centel/Zafer, **a.g.e.** , s. 200; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1329; Öztürk/Erdem/Özbek, **a.g.e.** , s. 412.

¹³³ Erem, **a.g.e.** , s. 349; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1330, dn. 16.

¹³⁴ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1330; Öztürk/Erdem/Özbek, **a.g.e.** , s. 411.

kısmını yansıtıcı bir niteliği olmalıdır. CMUK'ta bu husus “maksada elverişlilik” olarak adlandırılmaktaydı (CMUK 239/2-d). Olayı temsil edici olmayan delillerin sahip olmaları gereken bir diğer özellik olan ispat bakımından önemli olma gereğini de yerine getiremeyecekleri açıktır.

5. İspat bakımından önemli olmak

Delillerin sahip olması gereken bir diğer özellik, ispat bakımından önemli olmaları gereğidir¹³⁵. Sadece karara etkili olacak ve gerçeğin ortaya çıkması açısından ispat edilmesine gerek duyulan bir husus ile ilgili deliller önemlidir. Bunlar, yani önemli olanlar, dışındaki deliller ile uğraşılmaz. Çünkü delil ile ispat edilmek istenen olay, karara etkili bir olay olmalıdır (CMK 206/2-b ve ayrıca CMUK 239/2-c). Aksi halde hâkimin bu delili reddetmesi gerekecektir.

6. Müstereklik

Deliller açısından bulunması gereken bir başka özellik ise müsterek olmaları gereğidir¹³⁶. Delil müsterekliğinin sağlanması için, deliller duruşmada tartışmaya açılmalıdırlar (CMK 217). Böylece hem tarafların hem de hâkimin delillere doğrudan ulaşımı (vasıtasızlık ilkesi) sağlanacaktır. Bunun için ise delillerin önceden karşı tarafa da bildirilmesi gerekecektir (CMK 179, 181). Ayrıca CMK 217. maddesi içeriğine bakıldığında, hâkime yönelik bağlayıcılığın delillerin duruşmada tartışılmış olması gereği açısından bulunduğu görülmektedir. Duruşmada tartışılmayan bir husus delil olarak ileri sürülemeyecektir. Delillerin mahkemeye getirilmiş ve hâkimin huzurunda tartışılmış olması gereği hâkimin delillerle doğrudan doğruya temasa geçmesi gereğini de ortaya koymaktadır¹³⁷. Sadece bir tarafın ya da hâkimin bilgisi dâhilinde kalarak tartışmaya açılmamış ispat vasıtaları da delil değeri kazanamayacaklardır. Aksi halde adil yargılanma hakkı zedelenmiş olacaktır.

¹³⁵ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1331.

¹³⁶ Centel/Zafer, **a.g.e.** , s. 199; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1332.

¹³⁷ Öztürk/Erdem/Özbek, **a.g.e.** , s. 409.

7. Sağlamlık ve güvenilirlik

Bahsedilenlere ek olarak, delillerin sağlam ve güvenilir olmaları gerekir¹³⁸. Uydurulmuş veya değiştirilmiş bir delilin hükme etki ediyor olması ceza yargılamasına olan güvenin ve kamusal adalet duygusunun sarsılmasına neden olacaktır. Bu özellik dijital deliller açısından en sorunlu alandır. Bu sorunların neler olduğu dijital delillerin elde edilmesi içerisinde bulunan adli bilişimin evreleri konusunda detaylı olarak ele alınacaktır¹³⁹.

8. Elde edilebilirlik

Tüm bu özellikler dışında delil ayrıca elde edilebilir olmalıdır¹⁴⁰ (CMUK 239/2-e). Elde edilmesi imkânsız olan bir şeyin, delillerin sahip olmaları gereken bir diğer özellik olan olayı temsil ediciliğinden de bahsedilemeyecektir.

B. Dijital delillerin kendilerine has özellikleri

Dijital delillerin özellikleri açısından ikinci kategori ise onları klasik delillerden ayıran, kendilerine has olan özellikleridir. Bunlar ise daha çok dijital delilin bilişim bilimi açısından sahip olduğu teknik özelliklerin getirdiği sonuçlardan oluşmaktadırlar.

1. Gizli yapıda bulunma

Bu özelliklerden ilki ve en önemli olanı, dijital delillerin aynı DNA veya parmak izi delillerinde olduğu gibi ilk bakışta soyut olmaları yani gizli bir yapıda bulunmalarıdır¹⁴¹. Ancak olay yerinde bulunan DNA veya parmak izi gibi ilk halde

¹³⁸ Centel/Zafer, **a.g.e.** , s. 199.

¹³⁹ Bkz. s. 54 vd.

¹⁴⁰ Centel/Zafer, **a.g.e.** , s. 199.

¹⁴¹ **CoE Electronic Evidence Guide**, 2013, s. 11, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/2467_EEG_v18protected.pdf (Erişim tarihi: 30.12.2014); Technical Working Group for Electronic Crime Scene Investigation, **Electronic Crime Scene Investigation: A Guide for First Responders**, Temmuz 2001, <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf> (Erişim tarihi: 25.05.2014), s. 6; Kubilay Say, “**Data İncelemeleri**”, Oğuz Karakuş (ed.), Kriminallistik, Ankara: Adalet Yayınevi, 2. Baskı, 2013, s. 521;

soyut olan delillerin somutlaştırılması ve tespiti o anda yapılabilir. Dijital delillerin ise bunlardan farklı olarak niteliklerinin tespitinin ilk anda yapılamaması olasılığı vardır. Dijital delillerin bu özelliği ceza muhakemesi açısından ön plana çıkartılmakta, maddi deliller ile somutluk ve soyutluk açısından oluşan bu temel farklılığa göre düşünülmüş araştırma yöntemlerine ihtiyaç duyulduğu belirtilmektedir¹⁴².

Bu nedenle dijital delillerin bazı araçlar veya yöntemlerle somut, yani insanların duyu organlarıyla algılayabilecekleri, bir hale getirilmelerine ihtiyaç olacaktır¹⁴³. Bunu yapacak araçlar elektronik aygıtlardır. Elektronik aygıtların somut yapıda olması nedeniyle olay yerinde dijital delil araştırması yapılırken öncelikle bu aygıtlar dikkate alınacaktır. Ancak aygıtların yanı sıra aygıtların kullandığı dijital uygulamalar ve veriler de bu somutlaştırmada rol oynamaktadırlar. Dolayısıyla bazen aygıt yapısından dolayı bazen de veri niteliği nedeniyle dijital delillerin olay incelemesi anında ortaya çıkarılması mümkün olmamakta, yapılacak işin belli bir süre veya özel bir yöntem gerektireceği haller ortaya çıkmaktadır. Dijital delil elde etme açısından karşılaşılan sorunların en temelleri bu haller olmaktadır.

Ayrıca işin uygulama yönü göz önüne alındığında, bu gizli yapıyı ortaya çıkaracak belli kişilere ihtiyaç vardır. Bu kişiler ise ilgili kanunlarda delil toplama konusunda yetkilendirilmiş adli kolluk ve onlara teknik uzmanlık anlamında yardımcı olacak adli bilişim uzmanları olacaktır¹⁴⁴. Gizli yapının açığa çıkarılmasında adli bilişim uzmanlarınca yapılan incelemeler sonucunda oluşturulacak raporlar önem kazanacak, hâkimler de raporlara istinaden bu delilleri vicdani kanaatleri ile değerlendirebilecek hale geleceklerdir.

Keser Berber, s. 44; Mustafa Göksu, **Hukuk Yargılamasında Elektronik Delil**, Ankara: Adalet Yayınevi, 2011, s. 30.

¹⁴² Orin S. Kerr, **“Digital Evidence...”** içerisinde tamamen bu problematiğin üzerinde durmuş, hukukçuların var olan düzenlemeleri de göz önüne alarak buna yönelik fikir geliştirmeleri gereğinden bahsetmiştir.

¹⁴³ Dülger, **a.g.e.**, s. 751; Göksu, **a.g.e.**, s. 30.

¹⁴⁴ Adli bilişim sürecinin nasıl işleyeceği hususu üzerinde dijital delillerin elde edilmesi başlığı altında durulacaktır. Bkz. s. 52 vd.

2. Kopyalanabilir olma

Dijital delilleri klasik delillere göre ayıran belki de en önemli özellik kopyalanabilir olmalarıdır¹⁴⁵. Dijital veriler daha önce de bahsedildiği gibi içerik olarak 0 ve 1'lerden oluşan ikili kod sisteminin kullanılmasıyla oluşturulmaktadır. Dijital veri içeren aygıtlarda veriyi oluşturan kod diziliminin aygıt içerisine veya dışarısına aynen aktarabilmek için bir komut sistemi bulunmaktadır. Dolayısıyla dijital veriler sınırsız bir şekilde kopyalanabilirler. Üstelik bazı aygıtlar yedekleme adı altında kullanıcı komutu dışında kendiliğinden de bir kopyalama mekanizmasına sahip olabilirler.

İşbu özellik dijital delillerin incelenmesini hızlandırabilecek bir husustur. Böylelikle örneğin, uygulamada pek çok farklı bilişim uzmanı aynı anda orijinal verinin içeriğinin aynısına sahip olan kopya veriyi inceleyebilirler. Bunun yanı sıra bu özellik sayesinde dijital deliller mahkemeye de kolaylıkla sunulabilirler.

3. Kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olma

Dijital delillerin bir başka özelliği ise, yapılarından kaynaklanan nedenlerle, kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olmalarıdır¹⁴⁶. Bazı elektronik aygıtlar yapılan işlemleri dijital veri olarak bir önceki dijital verinin üzerine yazabilmektedirler. Bu durum elektrik gücünün kesildiği anlarda gerçekleşebildiği gibi, aygıtın özelliğinden de kaynaklanabilmektedir¹⁴⁷.

Yine bu tür veriler uzman olmayan kişiler tarafından da rahatlıkla değiştirilebilir, bozulabilir ve yok edilebilirler. Aygıtın normal bir kullanıcısı bile bu tür komutları yerine getirmeye ehil olabilmektedir. Bu durum bir yandan dijital delillere daha özenli yaklaşılmasını gerektiren bir husus olsa da, değiştirme, bozma ve yok etmeye yönelik hareketlerin tespitinin uzmanlar aracılığıyla kolaylıkla yapılabildiği de söylenmelidir.

¹⁴⁵ CoE Electronic Evidence Guide, s. 12.

¹⁴⁶ CoE Electronic Evidence Guide, s. 11; Technical Working Group for Electronic Crime Scene Investigation, a.g.e. , s. 6; Say, “Data İncelemeleri”, s. 521; Keser Berber, a.g.e. , s. 46.

¹⁴⁷ Örneğin aygıtta, yeni verilere yer açabilmek için bazı eski verilerin üst üste depolanması gibi özellik bulunması.

Ayrıca örneğin bir veri içerik olarak aynı bile olsa, farklı elektronik aygıtlardan veya dijital yöntemlerle somutlaştırıldığında, insanın karşısına çok farklı şekillerde çıkabilmektedir¹⁴⁸.

4. Yaygın ve uluslararası nitelikte olma

Dijital delillerin bir diğer önemli özelliği ise bu delillerin dünya çapında bir alana dağılmış olabilecekleri gerçeğidir¹⁴⁹. Özellikle elektronik aygıtların birbirleriyle olan bağlantıları düşünülünce, dijital delillerin bulunduğu alanın ne kadar geniş bir yaygınlığa sahip olabileceği de görülebilir. Bu durum uygulamada dijital delilin elde edileceği kaynağı belirlemek konusunda büyük sıkıntılar doğurmaktadır. Ayrıca kaynağın yeri bulunsa da, bu yerin ülke yetki alanı dışında bulunması durumu da problem doğurmaktadır. Örneğin, gerek internet ağı gerekse bulut teknolojisi gibi uluslararası özelliği olan teknolojilerin içerisinde bulunan verilerin kayıtlı olduğu aygıtlar bir başka ülkede bulunuyor olabilir.

Bu durumlarda delillerin elde edilmesi meselesi de uluslararası bir nitelik kazanmaktadır. Böylece adli makamların, ulusal makamlardan farklı olarak gerek yabancı gerek uluslararası nitelikte olan ve dijital verileri bünyelerinde içeren ya da bu konuda hizmet sunan kurumlarla bir bilgi alışverişi işbirliğine gitme zorunluluğu ortaya çıkmaktadır. Bu gibi hallerde uluslararası adli yardımlaşmanın yetersizliği dijital delillerin elde etme konusunda da olumsuz sonuçlar doğurmaktadır.

5. Aidiyet tespiti zorluğu

Dijital delillerin dünya çapında bir alana dağılmış olabilecekleri gerçeğini doğuran neden, herkes tarafından kolayca üretilebilmeleridir. Ancak bu üreticinin tespiti hiç de kolay olmamaktadır. Nitekim dijital verilerin özellikle internet ağı gibi geniş bir mecrada anonimlik temel alınarak günümüzdeki büyümeyi gerçekleştirdiği yadsınamaz. Bilgi kaynağındaki bu anonimlik anlayışı ile dijital verilerin aidiyetinin belirlenmesini zorlaştırmaktadır¹⁵⁰. Nitekim bilginin üretildiği kaynağa varılsa bile

¹⁴⁸ Göksu, **a.g.e.** , s. 33.

¹⁴⁹ Technical Working Group for Electronic Crime Scene Investigation, **a.g.e.** , s. 6; Say, “**Data İncelemeleri**”, s. 521.

¹⁵⁰ Göksu, **a.g.e.** , ss. 31-32.

bilgiyi üreten kişinin kaynağın sahibi olduğunu kanıtlamak da kolay değildir. Bu nedenle bu konu ile ilgili ceza muhakemesi açısından bazı karineler yaratma gereği oluşacaktır. Bu nedenle hukuk alanında aidiyetin ispatı açısından, güvenli elektronik imza gibi yeni kurumlar ortaya çıkmaktadır¹⁵¹.

6. Gelişim ve değişim gösterebilir olma

Dijital delillerin bir başka özelliği ise gelişim ve değişim gösterebilir olmalarıdır¹⁵². Her alanda yeni teknolojilerin çok büyük bir hızla gelişim göstermesi, bu teknolojiyi sadece kullanma bakımından değil inceleme bakımından sıkıntılar doğurmaktadır. Yalnızca cep telefonlarının son on yılda yaşadığı değişim göz önüne alınırsa, bu konunun önemi daha iyi anlaşılabilecektir. On yıl önce telefon niteliğine denk gelen özellikleri gözetilerek üretilmekte olan bu aygıtların her biri, günümüzde adeta birer küçük bilgisayar halini almıştır.

V. Dijital delil çeşitleri

Dijital delillerin, bir önceki başlıkta bulunan özelliklerinde de açıklandığı üzere, ilk bakışta görünmeyecek bir yapıya sahip olmaları nedeniyle, gerek elde edilmeleri gerek incelenmeleri açısından ancak belli aygıtlar kullanılabilecektir. Bu da daha önce de bahsedildiği üzere dijital delillerin elektronik yapıda bulunmasından ileri gelmektedir. Dijital delilleri ceza muhakemesindeki klasik delillerden ayıran en önemli özelliklerden biri budur. Yazı dosyaları, şekil dosyaları, ses dosyaları, fotoğraf dosyaları, video dosyaları, bilgisayar programları, bu programların işlevlerine özgü dosyalar, bilgisayar kütükleri, iletişim kayıtları, siber ağ gezinti kayıtları, siber ağda kayıtlı dosyalar ve sayılan tüm bu dosyalar ve kayıtların oluşturulma, değiştirilme ve erişim tarihleri gibi pek çok veriyi dijital delil olarak belirtebiliriz.

Görüldüğü gibi dijital deliller, tarihi süreç açısından henüz çok yeni de olsalar pek çok farklı formatta bulunmaktadırlar. Bu anlamda, elektronik aygıtlardan elde edilebilecek ve delil oluşturabilecek nitelikteki dijital delilleri sınırlandırarak saymaya çalışmak pek de kolay değildir. Bu yüzden dijital delilleri sınıflandırırken

¹⁵¹ Göksu, **a.g.e.** , s. 32.

¹⁵² **CoE Electronic Evidence Guide**, s. 12.

normal bir çeşit sayımı yapmaktansa, öncelikli olarak dijital delillere aracılık eden aygıtları sayarak, bu aygıtları ve bulundurabilecekleri delil içeriğini ortaya koymak daha yararlı ve açıklayıcı olacaktır.

Günümüzde dijital delil içeren aygıtların hepsini sınırlı sayıda sayabilmek pek mümkün görünmemektedir. Her yeni gün dijital veri içeren bir başka tür elektronik aygıt piyasaya sürülebilmektedir. Ancak bu aygıtları kısaca fakat tüketici olmayacak şekilde sayarsak; bilgisayarlar, el bilgisayarları, cep telefonları, dijital kamera ve fotoğraf makineleri, mp3 çalar/ipod, faks ve fotokopi makineleri, küresel konumlama cihazları (GPS), kredi kartı kopyalama aletleri gibileri ceza yargılaması açısından önemli dijital deliller içerebilmesi mümkün olan elektronik aygıtlardır.

Ayrıca elektronik aygıt olmayan internet, siber ağ, bulut teknolojisi gibi veri depolama ve iletme işlevlerine sahip ortamlara da ancak bir elektronik aygıt aracılığıyla ulaşılabileceği unutulmamalıdır.

Bu aygıtların sınırlayıcı bir biçimde veya sınıflandırılarak ayrılması dijital teknolojinin gelişim ve değişim hızına da bakılacak olursa pek kolay olmamaktadır. Hatta dijital delillerin gelişen ve değişen yapısı düşünüldüğünde bu deliller bakımından sınırlayıcı bir tasnif yapmak zaten imkânsızdır. Ayrıca dijital sistemler zaman içerisinde birbirleriyle o kadar uyumlu bir hale gelmişlerdir ki neredeyse her çeşit dijital veri, dijital teknolojiyi destekleyen her aygıtta bulunabilir hale gelmiştir. Yalnız bazı aygıtların kendilerine münhasır veri kayıtları da bulunmaktadır¹⁵³. Yine de bu aygıtlar teknolojik özelliklerine göre birçok farklı çalışma içerisinde çeşitli şekillerde sayılmaktadırlar¹⁵⁴.

VI. Dijital delillerin delil teorisine göre yeri

Dijital delillerin delil teorisine göre yerinin belirlenmesini yapabilmek için öncelikle ceza muhakemesindeki delil çeşitlerinin incelenmesi gerekecektir. Bu belirleme süreci sadece teorik bir tartışma olarak görülmemelidir. Nitekim bu

¹⁵³ Örneğin cep telefonlarındaki kısa mesaj kayıtları, telefon rehberi kayıtları, son aramalar listesi gibi kayıtlar.

¹⁵⁴ Konuyla ilgili bkz. Değirmenci, **a.g.e.** , ss. 140- 159; Dülger, **a.g.e.** , ss. 740-746; Technical Working Group for Electronic Crime Scene Investigation, **a.g.e.** , ss. 9-23.

tartışma sonucunda varılacak nokta, işin uygulama sürecini içeren dijital delillerin elde edilmesine doğrudan etki edecektir.

Daha önce delil ile ilgili olarak norm incelemesi yapıldığında, Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik'in delilin ne olduğuna dair bir tanımda bulunan tek normatif düzenleme olduğu görülmüştü. Dolayısıyla delil çeşitlerinin de açıkça belirtildiği normatif kaynak incelemesi yapıldığında ortaya çıkan sonuç yine çok kısıtlıdır. Bu konuda yine sadece aynı yönetmeliğin 3. maddesinde maddi delil adı altında bir delil çeşidi tanımlanmaktadır. İşbu tanıma göre maddi delil; itiraf ve şahadet dışında kalan, suç veya suç sanıklarıyla ilgili maddi (fiziki) bir yapıya sahip, canlı veya cansız, dokunulabilen şeyleri ifade etmektedir¹⁵⁵.

Ancak bu belirleme dışında yapılmış başkaca ayrımlar normlarda net olarak bulunmamakla birlikte, doktrinde normlardan ve delillerin niteliklerinden yola çıkılarak yapılmış pek çok farklı sınıflandırma şekli mevcuttur¹⁵⁶.

Ancak deliller farklı niteliklerine göre pek çok farklı kategoride sınıflandırılmış olsalar da, bu konu neticede delillerin elde edilmesi ve ispat gücü açısından önem arz edecek bir husustur. Öte yandan bu konuda herhangi bir inceleme yapılabilmesi açısından belli bir yol haritasının izlenmesi de gerekecektir. Her ne kadar tartışmalı da olsa bu çalışmada genel olarak kabul edilen delil çeşidi ayrımından yararlanılacak; deliller, üç farklı ana kategoride incelenecektir. Böylece bu konunun tartışmalı kısımları bir kenara koyulursa, delillerin beyan delilleri, belge delilleri ve belirti delilleri olmak üzere üçe ayrıldıkları söylenebilir¹⁵⁷.

¹⁵⁵ Maddi delil-dijital delil ilişkisi ve dijital delillerin maddi olmayan yapılarına dair değerlendirme için bkz. ss. 37-38.

¹⁵⁶ Gerek Anglosakson ceza hukuku doktrininde gerekse Kıta Avrupası ceza hukuku doktrininde delillerin değerleri ve özellikleri açısından pek çok farklı kategori üzerinden değerlendirildiği görülmektedir. Genel olarak yapılan ayrımlardan biri, Centel/Zafer ve Ünver/Hakeri de belirtildiği gibi, hâkimin delilleri elde etme şekline göre doğrudan delil ve dolaylı delil olarak yapılmaktadır.

Türk ceza hukuku doktrininde ise beyan, belge ve belirti delilleri ayrımı dikkat çekmektedir. Ancak bu ayrım yapılırken; Erem şahsi deliller ile maddi deliller ayrımını ortaya koymuştur (s. 426); yine Centel/Zafer delilleri benzer şekilde kaynağı kişi olan deliller (beyan) ve kaynağı nesne olan deliller (belge ve belirti) olarak ikiye ayırmıştır (s. 201); Kunter/Yenisey/Nuhoğlu (2010) ise delilleri somut olaya münhasır temsili deliller (beyan, belge) ve genel mahiyette temsili “tenkidi” deliller (belirti) olarak ikiye ayırmıştır (s. 1345).

¹⁵⁷ Centel/Zafer, **a.g.e.** , s. 201; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1346.

İlk olarak ele alınacak delil çeşidi beyan delilleridir. Beyan kelimesi anlamı gereği delillerin içeriği hakkında bir ön bilgi sağlamaktadır. TDK Güncel Sözlük’e göre beyan; bildirmedir¹⁵⁸. Bildirmeyi yapabilecek olanlar ise doğal olarak kişilerdir. Dolayısıyla beyan delillerinin kaynağı da kişiler olacaktır. Bu nedenle beyan delillerini kendi içerisinde ayırtırken izlenecek yöntem, ceza muhakemesinde hangi kişilerin yer aldığı ile doğrudan ilgili olacaktır. Ancak ceza muhakemesi içerisinde bulunan kişilerin hepsinin beyanı delil olmaz¹⁵⁹.

Dijital delillerin yapıları gereği beyan delilleri olamayacakları açıktır. Nitekim doğrudan kaynakları kişiler değil nesnelerdir. Yani bir diğer deyişle şahsi delil değildirler. Bu durumda geriye sadece dijital delillerin belge delili mi yoksa belirti delili mi olduklarına dair bir soru işareti kalmaktadır.

İkinci olarak ele alınacak delil çeşidi belge delilleridir. TDK Güncel Sözlük’e göre belge, “*Bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb., vesika, doküman.*” olarak tanımlanmıştır¹⁶⁰. Belge delilleri, somut bir olayı temsil eden ve insan yapısı olan ispat vasıtalarıdır¹⁶¹. Belge delilleri, delil olarak sağlam olma ihtimali en yüksek olanlardır. Ancak yine de belge de insan tarafından düzenlendiğine göre, bir belgenin sağlamlığı da onu düzenleyenin güvenilirliğiyle doğru orantılı olacaktır.

Dijital delillerin belge delili olup olmadığı tartışılacak olursa, belge delillerinin yazılı, anlaşılabilir içeriğe sahip ve kişiye izafe edilebilen bir şey olması gereği¹⁶² ile okunabilecek halde bulunan eşyadan oluştuğu¹⁶³ çıkarımı yapılmıştır. Burada her ne kadar belli bilgisayar programları aracılığıyla okunabilir içerikler oluşturulsa ve elde edilen dijital deliller yazılı olarak bir kâğıda aktarılabilse bile; o içerik artık dijital delilin kendisi olmaktan çıkarak, dijital delile aracılık edebilen elektronik aygıtın insanların anlayabilmesi için yaptığı bir tercüme olmaktadır.

¹⁵⁸ TDK Güncel Sözlük.

¹⁵⁹ Ceza muhakemesinde yalnızca tarafların ve tanıkların beyanı delil olur. Örneğin taraf olmayan hâkim, savcı, müdafî, vekil, zabıt kâtibi, bilirkişi vb. tanık sıfatı ile dinlenirse beyanları delil olabilir.

¹⁶⁰ TDK Güncel Sözlük.

¹⁶¹ Kunter/Yenisay/Nuhoğlu (2010), **a.g.e.**, s. 1384; Toroslu/Feyzioğlu, **a.g.e.**, s. 195.

¹⁶² TCK’nin 204. maddesini oluşturan resmi belgede sahtecilik suçuna yönelik gerekçesine göre belgenin sahip olması gereken özellikler bunlardır.

¹⁶³ Bu arada zaten CMK’de de belgenin okunmasından söz edilmektedir (CMK 215). Burada beyanlar üzerinden yapılan yoruma benzer bir şekilde, muhtevası okunabilecek haldeki şeylerin belge oldukları çıkarımı yapılabilir.

Neticede bu tercüme ile okunabilir hale getirilen içerik de elektronik aygıtların aracılığı öncesinde dijital verilerden ibarettir.

Ayrıca dijital delilleri oluşturan veriler sadece okunabilir içeriklerden oluşmamakta, aynı zamanda görülebilir ve dinlenebilir içeriklerin¹⁶⁴ yanı sıra, çeşitli bilişim yöntemleriyle ceza uyumsuzluğunun maddi yönünü oluşturan, olaya yönelik tespitlerin yapılabildiği başka içerikleri de içermektedir. Bu içerikler özellikle bilişim uzmanları tarafından analiz edilebilir halde bulunan içeriklerdir. Dolayısıyla dijital delillerin belge delilleri içerisinde sınıflandırılması da doğru görünmemektedir¹⁶⁵.

Üçüncü ve son olarak ele alınacak delil çeşidi ise belirti delilleridir. Belirti, ispat konusu olaya ilişkin geriye kalan her türlü iz ve eserdir¹⁶⁶. Bu nedenle beyan veya belge delili niteliğine sahip olmayan her delil belirti delili olarak değerlendirilmelidir. Doktrinde belirti ile emarenin aynı anlamı karşıladığı belirtilmektedir¹⁶⁷. Böylece delillerin emareyi kapsamı meselesi de açıklığa kavuşmuş olmaktadır.

Belirtiler tabii belirtiler ve suni belirtiler olmak üzere ikiye ayrılmışlardır. Tabii belirtiler irade dışı veya olayın doğal bir sonucu olarak, olaydan geriye kalan iz ve eserlerdir¹⁶⁸. Suni belirtiler ise iradi olarak veya bir insan tarafından belirli bir amaçla hazırlanmış iz ve eserleri ifade etmektedir¹⁶⁹.

Belirti delillerine olay yerindeki ayak izleri, kan, tükürük, DNA ve parmak izleri gibi örnekler verilebilir. Bu örneklerden de görüldüğü gibi belirti delillerinin

¹⁶⁴ Bu konuda Centel/Zafer ses ve görüntü içeren kayıtların belirti delili olduğunu iddia ederken (ss. 242-243); Kunter/Yenisey/Nuhoğlu (2010) bu kayıtları belge delilleri içerisinde incelemiştir (s. 1385 vd.). Ancak bu noktada irade hususunun önemli olduğunun üzerinde durmuştur. Bu görüşe göre irade dışı yapılan teknik izleme yöntemleri ile oluşturulan ses ve görüntü kayıtları ise belirti delili sayılmalıdır. Ancak bu kayıtların şüpheli veya sanığın kamuya açık ortamlardaki ve işyerindeki faaliyetleri içerecek şekilde yapılabilmesi ile alenilik sağlanmaya çalışılmıştır. Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydetmek suçtur (TCK 133). Bu nedenle telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınması gibi hak ihlallerinin kolaylaşabileceği olağanüstü delil elde etme yöntemlerinin ancak çok ciddi, tutarlı ve kısıtlı hukuki düzenlemeler ile yapılması gerekir.

¹⁶⁵ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1387; dijital delilleri bilişim verisi şeklindeki belge olarak belge delilleri içerisine koymuştur.

¹⁶⁶ Centel/Zafer, **a.g.e.**, s. 245.

¹⁶⁷ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1392.

¹⁶⁸ Centel/Zafer, **a.g.e.**, s. 245; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1392; örneğin olay mahallindeki parmak izleri vb.

¹⁶⁹ Centel/Zafer, **a.g.e.**, s. 245; Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.**, s. 1393; örneğin bir biletin üzerine damga basılmasının kullanıldığına dair işaret olması vb.

kaynağı kişiler ya da nesneler olabilmektedir. Belirti delillerinin bilimsel ve teknik anlamda incelenmesi ise kriminalistik bilimi yoluyla olmaktadır¹⁷⁰. Bu incelemeyi yapacak kişilere ise bilirkişi ya da uzman denilmektedir.

Belirti delillerinin içeriğine ve sayılan özelliklerine bakılacak olursa, dijital delillerin belirti delilleri içerisinde sınıflandırılmasının daha doğru olduğu görülecektir. Dijital delil içeren elektronik aygıtların da bir kan ya da DNA örneği gibi gerek elde edilmesi gerekse incelenmesi sırasında uzmanlık gerekmektedir. Daha önce de bahsedildiği gibi, dijital deliller yapısal özellikleri nedeniyle kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilirler. Bu nedenle dijital delillerin uzmanlarca incelenmeden delil olarak kabulü son derece tehlikelidir. Hatta bu delillerin bilirkişi incelemesi yapılması zorunlu alan içerisine girmesi bile yanlış görünmemektedir.

VII. Dijital delillerin elde edilmesi ve ispat gücü

Sadece dijital delillerin değil genelde tüm delillerin elde edilmesi ve ispat gücü meselesi ceza muhakemesi uygulamalarının en teknik alanlarından ikisini oluşturmaktadır. Üstelik bu iki alan arasında sıkı bir ilişki bulunmaktadır. Genellikle delillerin elde edilmesi sırasında ortaya çıkan problemler delillerin ispat gücünü de doğrudan etkileyebildiği için bu konuyu tek bir başlık altında incelemek daha yerinde olacaktır.

A. Genel olarak delil elde etme süreci ve uygulamaları

Öncelikle ceza muhakemesinde delilin ne zaman elde edilmeye başlanacağı sorusu hala tartışılmaktadır. Bir görüş sadece soruşturma aşamasında delil elde etmenin mümkün olduğunu ve soruşturma aşamasında yapılan işlemlerle hukuka uygun olarak elde edilen ispat vasıtalarının delil niteliğini kazandığını belirtmektedir¹⁷¹. Bir diğer görüşe göre ise, deliller genel kural olarak soruşturma aşamasında toplansa da, kovuşturma aşamasında da delil toplanmasına bir engel

¹⁷⁰ Oğuz Karakuş/Bülent Ünal, “**Olay Yeri İnceleme**”, Oğuz Karakuş (ed.), Kriminalistik, Ankara: Adalet Yayınevi, 2. Baskı, 2013, s. 3.

¹⁷¹ Parlar/Hatipoğlu/Yüksel, **a.g.e.**, s. 512.

yoktur¹⁷². Yine aynı görüşü benimseyen bir diğer esere göre ise, soruşturma aşamasında elde edilen ispat vasıtaları yalnızca şüphe sebepleri olarak adlandırılabilirler. Böylece ispat vasıtalarının delil olarak nitelendirilebilmesi ancak kovuşturma aşamasında mümkün olacaktır¹⁷³.

Ceza muhakemesi hukuku açısından delil elde etmeye yönelik çalışmanın başlayabilmesi için öncelikle kanunda öngörülen bir durum oluşmalıdır. Bu durum savcının, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hali öğrenmesi, yani bir suç şüphesinin oluşmasıdır. Buradaki şüphe basit bir şüphedir. Yani savcının soruşturmayı başlatması için öncelikli olarak önüne gelen olayda basit suç şüphesi bulunduğunu takdir etmesi gerekecektir¹⁷⁴.

Ancak doktrinde suç şüphesinin öğrenilmesiyle soruşturmanın başlaması arasında da delillerin araştırılması bakımından bilgi toplama dönemi adı verilen bir geçiş döneminin de bulunabileceğinden bahsedilmiştir¹⁷⁵.

Soruşturma işlemlerinin başlaması ile savcı kamu davası açmaya yer olup olmadığına karar vermek üzere gerçeğin araştırılması için, emrindeki adli kolluk görevlileri aracılığıyla, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla yükümlüdür (CMK 160). Bu araştırma sonunda toplanan deliller, suçun işlendiği konusunda yeterli şüphe oluşturuyorsa, savcı tarafından iddianame düzenlenir. Yani kamu davası açılabilmesi için suç işlendiği konusundaki basit şüphenin, elde edilen deliller aracılığıyla, yeterli şüpheye yükselmesi gerekmektedir.

Yukarıdaki paragraftaki içerikten görüldüğü üzere savcının emrindeki adli kolluk görevlileri, delillerin elde edilmesi ile ilgili görevleri yerine getirecek kişilerdir. Bu da delil elde etme işlemlerinin kimler tarafından yerine getirileceğini açıklığa kavuşturmaktadır. Adli kolluk görevlileri ilgili kanunlardaki görev ve yetkilerine göre polis, jandarma, sahil güvenlikten oluşmaktadır¹⁷⁶. Ancak delil

¹⁷² Centel/Zafer, **a.g.e.** , s. 75, 597; Ünver/Hakeri, **a.g.e.** , s. 97.

¹⁷³ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , s. 1338.

¹⁷⁴ Centel/Zafer, **a.g.e.** , s. 76.

¹⁷⁵ Centel/Zafer, **a.g.e.** , s. 76.

¹⁷⁶ CMK 164'e göre adli kolluk; 04.06.1937 tarihli ve 3201 sayılı Emniyet Teşkilatı Kanunu'nun 8, 9 ve 12. maddeleri, 10.03.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun

toplanması teknik bir iş olduğu için adli kolluk personeli de işin doğasına uygun şekilde değişik meslek gruplarına mensup kişilerden seçilmelidir¹⁷⁷. Özellikle dijital deliller söz konusu olduğunda bu durum bir ihtiyaç halini almaktadır.

Yeterli şüphe sonucu oluşturulan iddianamenin kabulüyle ve böylece kamu davasının açılması ile girilen kovuşturma aşamasında da delil toplanması mümkündür (CMK 177). Bu aşamada ise delil toplama işleminin yönetimi hâkimde bulunmaktadır.

Ancak gerek soruşturma aşamasında olsun, gerek kovuşturma aşamasında olsun, dijital delillerin elde edilmesine yönelik uygulamaların ceza muhakemesi sistemindeki yerini görebilmek için, öncelikle ceza muhakemesinde delil elde etme yöntemlerinin sayılması yararlı olacaktır. Delil elde etme yöntemleri de aynı dijital delil çeşitleri başlığı içerisinde incelendiği üzere beyan, belge ve belirti delilleri ayrımı üzerinden incelenebilir.

1. Beyan delillerinin elde edilmesi

Beyan delillerinin, kaynağı kişi olan deliller olduğundan bahsedilmişti. İşbu delillerin kişilerden öğrenilecek olması nedeniyle beyana kaynak olacak kişilerin çağrı usulleri yoluyla dinlenmesi sağlanır. Çağrı usullerine uyulmaması halinde zorla getirme gibi başka usuller devreye girecektir.

Şüpheli ve sanık beyanı için ifade alma ve sorgu (CMK 145), şüpheli ve sanık dışındakilerin beyanı için bilgi alma (Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği¹⁷⁸ 4), yer gösterme (CMK 85), teşhis (PVSK ek 6/9) ve doğrudan soru yöneltme (CMK 201) gibi yöntemler aracılığıyla beyan delilleri elde edilebilir.

7. maddesi, 02.07.1993 tarihli ve 485 sayılı Gümrük Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 8. maddesi ile 09.07.1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu'nun 4. maddesinde belirtilen soruşturma işlemlerini yapan güvenlik görevlilerini ifade etmektedir. Ancak CMK 165'e göre gerektiğinde veya savcının talebi halinde, diğer kolluk birimleri de adli kolluk görevini yerine getirmekle yükümlüdür.

¹⁷⁷ Yıldızhan Yayla, **İdare Hukuku**, 2. Basım, İstanbul: Beta Yayınevi, 2010, s. 42.

¹⁷⁸ Resmi Gazete, Tarih: 01.06.2005, Sayı: 25832.

2. Belge ve belirti delillerinin elde edilmesi

Diğer delil çeşitleri olan belge delillerinin kaynağı ise nesnelerdir. Nesneler çağrı usulü ile elde edilemeyeceklerinden, elde edilmeleri bakımından, bu nesnelere erişimin sağlanması gerekmektedir. Belirti delillerinin kaynağı ise gerek kişiler gerekse nesneler olabilmektedir. Ancak belirti delillerinde kaynağını kişilerden alan parçaların kalıntılar olduğu ve herhangi bir şekilde kişiye özgü davranışları gösteremeyecek organizmalar olmaları nedeniyle bunları da aynen nesneler gibi elde etmek gerekecektir. Bu yüzden belge ve belirti delillerini elde edilmeleri bakımından aynı kategori içerisinde incelemek mümkündür.

Belgelerin ve belirtilerin elde edilmesi sadece basit suç şüphesi duyuluyor diye herhangi bir usul kuralına uymadan, doğrudan gidip incelenmeleri yoluyla yapılamaz. Çünkü sadece muhakemenin gerçekleşmesi için keyfi bir şekilde kişilerin mülkiyetinde bulunan eşyalara erişmek ile kişilerin en temel haklarından biri olan özel hayatın gizliliği hakkı¹⁷⁹ ihlal edilmiş olacaktır. Bu nedenle bu türden bir erişimin sağlanmasına yarayan uygulamalara yönelik tedbirler kanunda bulunmaktadır.

Ceza muhakemesi sistemi incelendiğinde belge ve belirti delillerinin elde edilmesinde sıklıkla kullanılan tedbirleri olay yeri incelemesi (Adli ve Önleme Aramaları Yönetmeliği¹⁸⁰ 9), fizik kimliğin tespiti (CMK 81), arama ve elkoyma (CMK 116 ve 127), bilirkişi incelemesi (CMK 63), keşif (CMK 83), bilgi isteme (CMK 332) olarak sıralayabiliriz.

Bu konudaki özel muhakeme tedbirlerine ise, madde içeriklerinde sayılan katalog suçların işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, yani bir son çare olma (*ultima ratio*) ve zorunluluk halinde başvurulabilinecektir. Bunlar bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (CMK 134), iletişimin tespiti, dinlenmesi ve kayda alınması (CMK 135), gizli soruşturmacı görevlendirilmesi (CMK 139) ve teknik araçlarla izleme (CMK 140) olarak sayılabilir.

¹⁷⁹ AİHS 8, Anayasa 20.

¹⁸⁰ Resmi Gazete, Tarih: 24.05.2003, Sayı: 25117.

Tesadüfen elde edilen deliller (CMK 138) ise bu ikili ayrım dışında kalan kendine has bir müessesedir. Bu nedenle yukarıdaki ikili ayırmadan farklı bir konumda bulunmaktadırlar.

B. Dijital delillerin elde edilmesi

Günümüzde her türlü ceza muhakemesi işleminde UYAP kullanılmaktadır. Nitekim bu işlemlerin hepsi UYAP tarafından işlenerek kaydedilebilmekte ve saklanabilmektedirler (CMK 38/A). Dolayısıyla elde edilen delillerin de bu yolla dijitalleştirildiği söylenebilir. Ancak muhakeme işlemlerinde dijital teknolojinin kullanılması ile dijital teknolojinin delil olarak elde edilmesi arasında bir fark bulunmaktadır. Yani örneğin ifade alırken oluşturulan tutanakta ya da arama ve elkoyma işlemlerine yönelik hazırlanan tutanakta bir bilgisayar kullanılması, ilgili tutanağı dijital delil haline getirmemektedir. Burada yalnızca belgenin depolanması açısından kolaylık sağladığı için, dijital teknoloji kullanılmaktadır. Bu nedenle bu gibi uygulamalar dijital delillerin elde edilmesi derken bahsedilen kapsam dışında bulunmaktadırlar.

Bu noktada dijital delil elde edilmesi denildiğinde anlaşılması gereken yöntemler olarak, bir önceki başlıkta sayılan özel muhakeme tedbirleri ile bu özel muhakeme tedbirlerinin kullanılması sırasında ortaya çıkan, kanunun kullanılmasına izin verdiği, tesadüfen elde edilen deliller anlaşılmalıdır. Ancak gizli soruşturmacı görevlendirilmesi bu yöntemlerin dışında tutulmaktadır. Bunun da nedeni gizli soruşturmacının dijital elde edebileceği yöntemler olan hâkim kararı gerektiren tedbirleri kendiliğinden uygulayamayacak olmasıdır. Yani gizli soruşturmacı bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma, iletişimin tespiti, dinlenmesi ve kayda alınması ve teknik araçlarla izleme tedbirlerini kendiliğinden uygulayamaz¹⁸¹. Sonuçta dijital delil elde etme açısından yeni bir tedbir oluşmamıştır. Bu konuda ilgili olan tüm hukuki düzenlemelerden çalışmanın ikinci bölümünde detaylı olarak bahsedilmektedir¹⁸². Bu nedenle bu bölümde dijital delillerin elde edilmesi konusunun teknik yönü ortaya konacaktır.

¹⁸¹ Nurullah Kunter/Feridun Yenisey/Ayşe Nuhoğlu, **Açıklamalı Ceza Muhakemesi Kanunu**, İstanbul: Beta Yayınevi, 2013, s. 1546.

¹⁸² Bkz. s. 108 vd.

Zaten bu bölüme gelmeden önce üzerinde durulan dijital delil çeşitlerinden, özelliklerinden ve bu delillerin delil teorisine göre bulundukları konumdan da açıkça anlaşılacağı üzere, dijital delillerin elde edilmesi süreci klasik delillere göre daha farklı olacaktır.

Dijital delillerin yapıları gereği bir elektronik aygıt içerisinde bulunmaları onları delil elde etme aşamasında klasik delillere göre daha özel bir hale getirmektedir. Nitekim her ne kadar dijital delil içerseler de, somut nitelikteki bu aygıtlar açısından, delil elde etmede bazı klasik yöntemlerin kullanılmasına gerekirken, dijital delil araştırmasını başlatacak noktada başka yöntemlerin kullanılmasına ihtiyaç olacaktır.

Ancak dijital delillerin çok kolay bir şekilde değiştirilebileceği, bozulabileceği ve yok edilebileceği düşünüldüğünde klasik yöntemlerle araştırma yapacak kişilerin de dijital delillere ilişkin bilgili kişiler olmaları gerekecektir¹⁸³.

Nitekim dijital delillerin niteliği hâkim tarafından ilk görüşte anlaşılabilir de bu delillerin sağlamlığının veya hukuki değerlendirmeye konu olacak kısmının teknik uzmanlık gerektiren noktalarının tespiti gerekecektir¹⁸⁴. Bu tespiti yaparak hâkimin değerlendirmesine katkıda bulunacak kurum bilirkişiliktir. Bilirkişi kavramı çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hallerde oy ve görüşü alınacak kişiyi ifade etmektedir. Bilirkişinin oy ve görüşünün alınmasına hâkim veya mahkeme tarafından re'sen veya savcı, katılan, vekil, şüpheli veya sanık, müdafii veya kanuni temsilcinin istemi üzerine karar verilebilir (CMK 63). Soruşturma aşamasında bilirkişi savcı tarafından da görevlendirilebilir (CMK 63/3).

Bilirkişi olarak atanabilecekler, kanunların belirli konularda görevlendirdiği resmi bilirkişiler¹⁸⁵ (CMK 64/3) dışında il adli yargı adalet komisyonları tarafından her yıl düzenlenen bir listede yer alan gerçek veya tüzel kişilerdir (CMK 64). Ancak bu kişiler dışında da bilirkişi seçmek mümkündür (CMK 64/2).

¹⁸³ Bazı durumlarda elektronik aygıtı yapılan en küçük bir müdahalede bile dijital delillerin kaybedilmesi sonucu doğabilir.

¹⁸⁴ Örneğin bir ses veya görüntü dosyasının içeriği hâkim tarafından dinlenerek veya görülerek anlaşılabilir ancak bu içeriklerin üzerinde bir değiştirme yapılmadığının tespiti gerekir.

¹⁸⁵ Buna örnek olarak Adli Tıp Kurumu verilebilir.

Ayrıca kanunun lafzında da görüldüğü üzere bilirkişiye başvurma takdiridir. Ancak bazı konuların çözümü için kanunda bilirkişiye başvuru zorunlu hale getirilmiştir. Bu haller bilirkişiye başvurma mecburiyeti olan haller olarak adlandırılmaktadırlar¹⁸⁶. Bu hallerde bilirkişi raporu olmadan ispat mümkün değildir. Görüldüğü gibi ceza muhakemesinde vicdani ispat sistemi geçerli olsa da, özellikle bu konularda bilimsel ispat sistemine doğru bir kaymanın olduğu da söylenebilir.

Burada mevcut duruma göre oluşacak tek farklılık bilirkişilerin adli bilişim uzmanlarından seçilmesi gereği olacaktır. Nitekim daha sonra da tanımlanacağı üzere bir uygulamalar bütünü olan adli bilişim yöntemlerini uygulamak için bilişim alanında eğitim almış ve teknik uzmanlık gerektiren bilgiye sahip kişilere ihtiyaç duyulmaktadır¹⁸⁷. Bu yöntemlerin başkaca kişiler tarafından uygulandığı bir açıdan bakıldığında ise, adli bilişim uzmanı olarak adlandırılan bu kişilerin yardımıyla, dijital delillerin kendilerine münhasır özellikleri nedeniyle oluşan ve delil elde etme aşamasında klasik delillere göre daha sistematik ve modern metotların uygulanmasının doğruluğu da tartışılacaktır.

Daha önce de bahsedildiği üzere, bu sistematik ve modern metotlar, dijital delillere ilişkin uzmanlıktan sorumlu olan adli bilişim alanı içerisinde bulunacaktır. Bu nedenle dijital delillerin elde edilmesini incelerken, öncelikle adli bilişim ile ilgili temel bilgiler vererek bu metotların nelerden oluştuğunu belirlemek gereklidir. Zaten dijital delillerin elde edilmesi aşaması da aslında kabul edilen adli bilişim evrelerinin adli bilişim uzmanı denetiminde dijital delil üzerinde uygulanmasıdır.

1. Adli bilişim

İngilizce'deki “*computer forensic*” kavramı, Türkçe'de adli bilişim olarak adlandırılmıştır. Her ne kadar bu kavramın gerçek karşılığı bilgisayar kriminalistiği anlamına denk gelse de uygulamada adli bilişim ile bilgisayar kriminalistiği birbirlerinden farklı değildir. Bu noktada daha önce verilmiş olan bilişim tanımları

¹⁸⁶ Para ve benzeri değerlerin sahteliğinin tespiti (CMK 73), şüpheli veya sanığın akıl sağlığının tespiti (CMK 74), şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması (CMK 75), diğer kişilerin beden muayenesi ve vücutlarından örnek alınması (CMK 76), moleküler genetik incelemeler (CMK 78), ölünün adli muayenesi (CMK 86), otopsi (CMK 87), yeni doğanda cesedin adli muayenesi veya otopsi (CMK 88) ve zehirlenmenin tespiti (CMK 89) gibi işlemleri bu haller arasında sayabiliriz.

¹⁸⁷ Keser Berber, **a.g.e.**, s. 46.

da göz önünde bulundurularak, bu alanda yapılan uygulamaların adli bilişim olarak adlandırılması daha doğru olacaktır. Nitekim bilişim kavramı, bilgisayar kavramına göre hem daha geniştir hem de bu uygulamaların tümü göz önüne alındığında daha doğru kullanılan bir anlama sahiptir.

Doktrinde adli bilişimin ne olduğuna dair bazı tanımlar yapılmıştır. Bunlardan birine göre adli bilişim, hukuka uygun şekilde delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan uygulamaları ifade etmektedir¹⁸⁸.

Bir diğer tanım ise şöyledir: “*Soruşturma ve/veya yargılamada, sürecin tarafların iddia ve/veya savunmalarını destekleyecek veya çürütecek gerçeklerin ortaya çıkartılması amacıyla bilişim aygıtlarının kayıtlarının incelenmesidir.*”¹⁸⁹.

Bir başka görüşe göre ise “*Bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığının tespiti amacıyla yapılan çalışmaların tümüdür.*” olarak tanımlanmıştır¹⁹⁰.

Yine başka bir görüş adli bilişimi, potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama olarak benimsemiştir¹⁹¹.

Sonuç olarak tüm tanımlara bakıldığında adli bilişimin, hukukun delil elde etme konusunda bilişimle ilgili meseleler konusunda yardım alacağı bir uygulamalar bütünü olduğu söylenebilir. Bu durum göz önüne alındığında adli bilişimin kaynaklarının da çok çeşitli olduğu söylenebilir. İnternet kullanımları, bilişim suçları, fikri hakların konumu, şirket stratejisi ihlali, internet kullanılarak şeref ve haysiyete karşı fiiller, kurumsal yaşama müdahaleler, sistem suiistimalleri gibi durumlar adli

¹⁸⁸ Dülger, **a.g.e.** , s. 738.

¹⁸⁹ Akt. Dülger, **a.g.e.** , s. 739 (Cem Günel, “**Adli Bilişim ve Delillerin Toplanması**”, Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu, 18 Şubat-11 Mart 2012, İstanbul).

¹⁹⁰ Henkoğlu, **a.g.e.** , s. 1.

¹⁹¹ Keser Berber, **a.g.e.** , s. 39.

bilişimin kullanılabileceği kaynaklar olarak görülmektedir¹⁹². Görüldüğü gibi adli bilişim süreci sonucunda elde edilen deliller sadece ceza muhakemesi hukukuna özgü olarak kullanılmamakta; özel hukuka ilişkin pek çok hukuki aykırılıkta da kullanılabilmektedir¹⁹³.

2. Adli bilişimin evreleri

Toplanacak olan deliller, dijital deliller olduğunda, durum farklılaşmakta ve karmaşıkmaktadır. Daha önce de bahsedildiği gibi dijital deliller, elektronik aygıtların içerisinde bulunan verilerden meydana gelmektedir. O halde, içerisinde delil bulunduğu şüphesiyle incelenen bir elektronik aygıtın içerisinde suç delilinin bulunup bulunmadığı, ilk anda kesin olarak belirli olmamaktadır. Dolayısıyla dijital delillerin elde edilmesinde ortaya çıkan ilk önemli zorluk, delil olarak düşünülen aygıtların suça ulaşmada vasıta olup olamayacakları hususundaki belirsizliktir. Bu nedenle her suç tipine göre ayrı adli bilişim uygulamaları devreye girmekte ve aygıt incelemeleri de suç tipine göre yapılmaktadır¹⁹⁴. Ancak buna rağmen, adli bilişimin bir yol haritası olarak genel bir adli bilişim evre şeması kullandığı ve adli bilişim uygulamalarının da genellikle bu evreler içerisinde değişiklik gösterdiği söylenebilir.

Adli bilişimin evreleri ile ilgili olarak, evrelerin isimleri ve zamanları konusunda ortaya atılan bazı tartışmalar ve farklılıklar vardır¹⁹⁵. Ancak burada çalışmanın devamı açısından bir yol seçilerek devam edilecektir. Sonuç olarak yapılan ayrımlardan biri kullanılarak adli bilişimin dört evreden oluştuğunun kabul edildiği söylenecektir. Bu evreler toplama, inceleme, analiz ve raporlamadır.

¹⁹² Keser Berber, **a.g.e.** , s. 40.

¹⁹³ Keser Berber, **a.g.e.** , ss. 76-77.

¹⁹⁴ Konuyla ilgili olarak bkz. Henkoğlu, **a.g.e.** , ss. 7-12.

¹⁹⁵ Keser Berber, **a.g.e.** , s. 45 içerisinde adli bilişim toplama, inceleme, analiz ve belge hazırlama olarak dörde ayrılmıştır. Say, **“Data İncelemeleri”**, s. 531 içerisinde adli bilişim kopyalama, belirleme, çözümleme, yorumlama ve belgeleme olarak beşe ayrılmaktadır. Karagülmez, **a.g.e.** , s. 454 içerisinde ise adli bilişim elde etme, analiz ve sunma olarak üç evreden oluşmaktadır. Carlos Alberto Rohrmann/Jason S. de Albergaria Neto, **“Digital Evidence and Electronic Lawsuits: How far do we go?”**, Sylvia Mercado Kierkegaard (ed.), Cyberlaw, Security & Privacy, 2. Baskı, Ankara: Ankara Barosu Yayınları, 2007, s. 616 içerisinde adli bilişim tanımlama, koruma, analiz ve sunma evrelerinde oluşmaktadır. Ayrıca konuyla ilgili yapılmış geniş çaplı inceleme için bkz. Değirmenci, **a.g.e.** , s. 165 vd.

a. Toplama

Toplama, adli bilişim evrelerinin ilkidir ve dijital delillerin elde edilmesidir¹⁹⁶. Bu evre içerisinde; dijital delillerin aranması, tespit edilmesi, toplanması ve dokümantasyonunun yapılması sağlanmalıdır. İlk duruma göre bu evre, gelecek zamanı ve olay yerinde gerekli önlemler alınmadığı için kaybedilebilecek bilgilerin saklanması da içerebilir¹⁹⁷.

Toplama aşamasının sağlıklı olması ve başarıya ulaşmasının anahtarı olay yerinin korumasını iyi bir şekilde sağlamaktan geçmektedir. Bu görev adli kolluk tarafından yapılacaktır. Bu nedenle adli kolluğun da adli bilişim süreci ve dijital deliller hakkında bilgi sahibi olması sağlanmalıdır. Olay yeri koruması sağlanınca olay yeri incelemesinin de daha sağlıklı bir şekilde yapılması mümkün olacaktır.

Böylece adli bilişim uzmanları tarafından toplama işlemi başlatılabilecektir. Bu işlem sırasında olay yerinde sorumluluğu olmayan kişiler bulunmamalıdır¹⁹⁸. Toplama işlemi dijital delillerin aranmasıyla başlasa da, aramadan önce bir takım ön hazırlık uygulamaları yapılacaktır. Bunlara örnek olarak, olay yerinin fotoğrafının çekilmesi, şemalandırılması, toplamaya ilişkin gerekli malzemelerin hazırlanması ve yapılacak işlemlere yönelik bir kontrol listesi hazırlanması verilebilir.

Arama başladığında aranmakta olan aygıtların son hallerine veya özelliklerine göre yapılması ve yapılmaması gerekenler olacaktır. Genellikle adli bilişim uzmanının karşılaştığı durum iki türlü olmaktadır. Bunlardan ilkinde elektronik aygıt açık durumda bulunarak çalışmaktadır. Diğer halde ise elektronik aygıt kapalı durumda bulunmakta yani çalışmamaktadır. Her iki halde de amacın dijital delillerin daha sonra analiz edilmek üzere muhafazasının gerçekleştirilmesi olduğu unutulmamalıdır¹⁹⁹. Bu nedenle iki halde de yapılmaya çalışılacak işlem imaj alma olarak da adlandırılan bir çeşit kopyalama işlemi olacaktır²⁰⁰. Ancak genelde olay yeri incelemesi sırasında bu işlemin yapılması zaman alabilmekte, yapılacak en

¹⁹⁶ Dülger, **a.g.e.**, s. 746.

¹⁹⁷ Keser Berber, **a.g.e.**, s. 45.

¹⁹⁸ Dülger, **a.g.e.**, s. 747.

¹⁹⁹ Karagülmez, **a.g.e.**, s. 456.

²⁰⁰ Değirmenci, **a.g.e.**, ss. 373-374. Uygulamada birebir olarak yapılan kopyalama işlemine imaj alınması da denilmektedir. Aynı zamanda yedekleme olarak da adlandırılan bu işlem klasik kopyalama işleminden farklıdır.

küçük bir yanlış hareket veri kaybına neden olabilmektedir. Bu nedenle imaj alma işlemi o an elde edilmesi gerekli ve o anda ulaşılabilir olan veriler ile sınırlı tutularak, genelde bir sonraki evre olan inceleme evresine bırakılmaktadır²⁰¹.

Arama sonucunda ortaya çıkan dijital deliller ve dijital delil içeren aygıtların tespiti yapılmış olur. Tespit edilen eşyanın etiketlenmesi ve delil olarak kaydının yapılması gerekir. Daha sonra ise tespiti yapılmış dijital delillerin ve dijital delil içeren aygıtların toplanmasına yönelik çalışma başlar. Dikkatlice toplanacak olan eşya inceleme aşaması için laboratuvara taşınacaktır. Bu noktada elektronik aygıtların çevresel faktörlere olan duyarlılığına dikkat edilmelidir. Nitekim bu aygıtlar kolaylıkla zarar görebilirler²⁰².

Toplama açısından en önemli husus, bu aşamada yapılan her işlemin mutlaka dokümantasyonunu yapma gereğidir. Bu aşamadaki yapılan tüm işlemler sırasıyla belirtilmeli ve bunu içeren belgelerde şüphelinin veya müdafinin imzası bulunmalıdır. Böylece yapılan işlemlerin hukuka uygun ve denetlenebilir olması sağlanacaktır²⁰³.

Olay yerinin klasik olmadığı ve belki de fiziki olarak bulunmadığı durumlarda²⁰⁴ toplama aşamasının hizmet sağlayan belli kurumlardan yapıldığı durumlar olabilmektedir. Bu durumda görevlendirilmiş adli bilişim uzmanının toplama işlemini bu kurumun tuttuğu ya da bulundurduğu kayıtlar üzerinden yapması gerekecektir. Ancak toplanacak dijital verilerin sağlıklı ve güvenilir bir şekilde kalabilmesinin kontrolü hususunda ilgili kurumların da adli bilişim uzmanı istihdam etmeleri gerekecektir. Böylece toplama aşaması daha sağlıklı bir şekilde yürütülebilecektir. Nitekim kurum içerisinde herhangi bir adli bilişim desteği almadan yapılan işlemlerde hata yapılarak ilgili kayıtların yok edilmesi ihtimali bulunmaktadır.

²⁰¹ Dülger, **a.g.e.** , s. 750.

²⁰² Dülger, **a.g.e.** , s. 750.

²⁰³ Dülger, **a.g.e.** , s. 748.

²⁰⁴ Ağ bağlantıları gibi.

b. İnceleme

Toplama evresinden sonra gelen inceleme evresinde; dijital delillerin somutlaştırılması ile somutlaştırılan delilin orijinal halinin ve soruşturma açısından öneminin açıklanması sağlanmaktadır. Bu evre ile adli bilişim sürecinde önemli bir aşama kaydedilmektedir.

Bu aşamada yapılacak ön hazırlık, elde edilen delillerin imajının alınması işlemidir. Böylece inceleme orijinalinin aynısı olan imaj üzerinde yapılarak, orijinal delil üzerinde bir oynama yapılmayacak, delil bütünlüğü korunacaktır²⁰⁵. Böylece inceleme sırasında meydana gelebilecek aksaklıklarda zarar görecektir olan orijinal delilin yedeği olacaktır. Bu durumda orijinal delil zarar görmeyeceği için en kötü senaryolarda bile yeniden imaj alma işlemi yapılması mümkün olacaktır.

Bu noktada adli bilişim işlemi açısından bahsedilmesi gereken bir değer konu ise dijital delillerin “*hash*” değerinin alınması meselesidir. Hash değeri dijital verilerin bütünlük ve sağlamlık kontrolünde kullanılan, hatta verilerin DNA’sı olarak adlandırılan bir değerdir²⁰⁶. Gelecekte yapılacak denetim açısından kopyalama işlemi sırasında hash değerinin de alınması gerekir. Nitekim inceleme aşaması öncesinde alınan hash değerinin sonraki aşamalarda alınan hash değerleri ile farklılık göstermesi halinde veri üzerinde değişiklik yapıldığı ispat edilebilmektedir²⁰⁷.

İnceleme evresi ile delil olan verilerin zarar görmesi önlenerek delil sağlamlığı ve bütünlüğünün korunması da amaçlanmaktadır. Böylece delilin içeriğinin ve durumunun dokümantasyonu sağlanır. Bu dokümantasyon tarafların, delilin içerisinde ne olduğunu keşfetmelerine olanak verir. Bu süreç kapsamına giren diğer bir konu ise, şifreleme gibi nedenlerle gizli kalmış veya ulaşılamamış bilgilerin araştırılmasıdır. Bir kez tüm bilgilerin somutluğu sağlandıktan sonra, artık önemli verileri önemsizlerden ayıklama işlemine başlanabilecektir²⁰⁸.

²⁰⁵ Bu konu özellikle delil güvenliği ve sağlamlığı açısından önem arz etmektedir. Bkz. Dülger, **a.g.e.** , s. 752.

²⁰⁶ Henkoğlu, **a.g.e.** , s. 56.

²⁰⁷ Semih Dokurer, “**Adli Bilişim**”, Ses Görüntü ve Data İncelemeleri, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008, s. 244.

²⁰⁸ Keser Berber, **a.g.e.** , s. 45.

c. Analiz

Analiz evresi, inceleme aşamasında elde edilen sonuçlara hukuki önemleri ve davadaki ispat değerleri açısından yaklaştığı için, incelemeden farklıdır²⁰⁹. İnceleme, bilişim alanı açısından daha teknik bir gözden geçirme iken, analiz aşamasında işin hukuki yönü de dikkate alınarak bir inceleme yapılmaktadır. Buradaki değerlendirme daha çok eldeki verileri hukuksal öneme göre sınıflandırma şeklindedir.

Bu sınıflandırma aynı zamanda bir sınırlandırma işlemi olarak da görülebilir. Bu aşamada dava ile ilgisi olmayan veriler elenecektir. Bu eleme yapılırken dijital delilin elde edildiği aygıtlara göre kullanılacak pek çok farklı yazılım türü bulunmaktadır²¹⁰. Böylece, analiz evresindeki çalışmaların etkin ve hızlı olması sağlanmaktadır.

Analiz evresinde ulaşılan sonuçlar son aşama olan raporlamada kullanılacaktır.

d. Raporlama

Bilirkişi olarak atanan adli bilişim uzmanı, incelemesi sona erdiğinde, yaptığı işlemleri ve vardığı sonuçları açıklayan bir raporu, kendisinden istenen incelemeleri yaptığını ayrıca belirterek, imzalayıp ilgili makama verir (CMK 67). Görüldüğü gibi burada belirtir delillerinin bilirkişi raporu yoluyla belge haline getirilmesi söz konusudur²¹¹. Birden fazla sayıda bilirkişi atanmış ise, bilirkişilerin arasında farklı görüşler veya ortak sonuçlar bulunması durumunda, bu durum gerekçesiyle birlikte raporda belirtilir (CMK, 67/2). Ancak bilirkişi raporu hâkimde yeterli vicdani kanaat oluşturmazsa yeni bir bilirkişi incelemesi yaptırılabilir. Yine bilirkişi incelemesine itirazda bulunmak da mümkündür.

Aslında adli bilişimin tüm evrelerinde yapılan işlemlerin belgelenerek kayıt altına alınması gereklidir. Böylece adli bilişimin son evresi olan raporlamada tüm bu işlemler silsilesi mahkemeye sunulacaktır. Raporun içerisinde işlemlerin içerikleri ile

²⁰⁹ Keser Berber, **a.g.e.** , s. 45.

²¹⁰ Bu konuda detaylı bilgi için bkz. Dülger, **a.g.e.** , s. 756 vd; Karagülmez, **a.g.e.** , s. 464 vd.

²¹¹ Centel/Zafer, **a.g.e.** , s. 246.

birlikte işlemlerin hangi tarihte başlatıldığı ve hangi tarihte son bulduğu hususlarına yer verilmelidir. Bu hususlardaki belirsizlikler delil güvenlik zincirini (*chain of custody*) olumsuz yönde etkileyecektir. Delil güvenlik zinciri, delilin elde edilme anından mahkemeye sunulmasına kadar geçen süreçteki devamlılığını temsil ettiğinden, delil sağlamlığının ve bütünlüğünün bozulmadığının ispatı açısından önemli bir araçtır²¹².

Görüldüğü gibi raporlama aşamasında, analiz aşaması sonucunda dava ile ilgili olabilecek hususların belirlenmesi sonucunda varılan değerlendirmelere ilişkin dokümantasyon yapılacaktır. Toplama ve inceleme notlarını da içeren ve analiz evresinin özetlendiği bu rapor ile araştırmayı yapan adli bilişim uzmanlarının olaya sadece şekli açıdan değil nitelikleri açısından da tanıklığı da sağlanmaktadır²¹³. Böylece delillerin bütünlüğü ve sağlamlığı daha iyi bir şekilde korunacaktır.

C. Dijital delillerin ispat gücü

Bu çalışmada dijital deliller, ceza hukuku delil teorisine göre belirti delilleri içerisinde sınıflandırılmıştır. Dolayısıyla belirti delillerinin sahip olduğu ispat gücüne sahip olmaları gerekir. Bu noktada belirti delillerinin bir beyan veya belge deliline göre daha zayıf bir ispat gücüne sahip olduğunu söylemek gerekir. Dolayısıyla bir belirti delili (emare), hükmün verilmesi için yeterli olmaz²¹⁴. Örneğin, olay mahallinde bulunan şüpheliye ait parmak izi, şüphelinin suçu işlediğini değil; sadece şüpheli olayın gerçekleştiği yerde bulunduğunu ispatlar. Ancak birden çok birbirini destekleyen belirtinin bir araya gelmesi halinde mahkûmiyet kararı verilebilmesi mümkündür²¹⁵.

Hatta bu konuda gerek Anayasa Mahkemesi'nce verilen²¹⁶ gerekse Yargıtay'ca verilen kararlara göre²¹⁷ belirtilerin delil olarak tek başlarına ispata

²¹² Peter Sommer, **Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers**, 3. Edition, Information Assurance Advisory Council, 2012, s. 30.

²¹³ Keser Berber, **a.g.e.**, s. 45.

²¹⁴ Centel/Zafer, **a.g.e.**, s. 245; Erem, **a.g.e.**, s. 370.

²¹⁵ Centel/Zafer, **a.g.e.**, s. 246; Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.**, s. 1375; Metin Feyzioğlu, **"Belirtilerin Şüphelinin Yenilmesindeki İşlevi ve Benzer İsnadlara Ait Delil Araçlarının Somut Olayın Çözümünde Birlikte Değerlendirilmesi"**, Ankara Barosu Dergisi, 2000-1, s. 21.

²¹⁶ AYM 19.08.1971-41/67, Resmi Gazete, Tarih: 15.01.1972, Sayı: 14073: *"Başkaca inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının ve gizli ajan raporlarının, bir yurttışa*

yeterli olamayacakları ve başkaca delillerle desteklenmeleri gereği ortaya konmuştur. Yani bu türdeki tek bir delilin varlığı ispata yeterli olmayacağından, mahkûmiyet sonucu doğmamalı; ancak bu türde birbirini destekleyen başkaca delillerin de varlığı halinde mahkûmiyet hükmü kurulabilmelidir. Nitekim bir şeyin delil olması ile delil olan şeyin belirli bir vakıayı ispatlama konusundaki gücü farklı şeylerdir²¹⁸.

Dijital delillerin ispat güçleri açısından bir diğer önemli husus ise, bu delillerin ceza yargılamasında kullanılabilmesi için hukuka uygun olmalarına ek olarak, gerekli teknik incelemelerin yapılması sonucunda sağlam ve güvenilir olduklarının da tespit edilebilmesidir. Bu tespit ise vicdani ispat sisteminin hakim olduğu bir sistemde, hâkim tarafından yapılmalıdır. Böylece elde edilen belirtinin delil olarak kullanılıp kullanılamayacağı da ortaya çıkacaktır. Adli bilişim uzmanlarının sunduğu rapor hâkim açısından önemli bir yol gösterici olsa da raporun içeriğinin de denetimi gerekir. Raporun içeriğinde denetlenecek hususlar ise, özellikle dijital delillerin elde edilme anından itibaren başlayan ve adli bilişim incelemesi sürecini de kapsayan kurallara uyulması gereği olacaktır. Türkiye’de henüz bu yönde kurallar olmamakla birlikte, bazı ülkelerde adli bilişim uygulamalarına yönelik kurallar, gerek hukuki düzenlemeler, gerekse yol gösterici rehberler çıkartılmak suretiyle çoktan koyulmuş ve uygulanmaktadır²¹⁹.

Türkiye’de mevcut durumda adli bilişim incelemeleri Adli Tıp Kurumu bünyesinde bulunan Fizik İhtisas Dairesi Başkanlığı ve il adli yargı adalet komisyonları tarafından her yıl düzenlenen bir listede yer alan gerçek veya tüzel kişiler tarafından yapılmaktadır²²⁰.

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

²¹⁷ Detaylı bilgi için bkz. Ali Kemal Yıldız, "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu", Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, Aralık 2006, ss. 259-260.

²¹⁸ Centel/Zafer, **a.g.e.** , s. 245.

²¹⁹ Örneğin ABD için bkz. s. 84, Birleşik Krallık için bkz. s. 95.

²²⁰ Adli bilirkişilik konusu ile ilgili görüşler için bkz. s. 172 vd.

İKİNCİ BÖLÜM: DİJİTAL DELİLLERE YÖNELİK HUKUKİ DÜZENLEMELER

Ceza muhakemesi açısından dijital delilin yerini genel delil teorisi açısından açıklığa kavuşturduktan sonra, bu konuda bulunan hukuki düzenlemeleri incelemek ve analiz etmek gereklidir. Böylece mevcut düzenlemelerin yeterliliği tartılarak mevcut hukuki tablo ortaya çıkacaktır. Ayrıca uluslararası hukukta ve bazı yabancı hukuklardaki durumu görerek Türk hukukundaki düzenlemelerin yeterliliği de değerlendirilebilecektir.

Bilişim suçlarının işlenmesine yardımcı olsun veya olmasın, dijital delillerin uluslararası niteliği ve geniş bir alana yayılmış olabileceği gerçeği, dijital delillere yönelik hukuki düzenlemeler yapılırken uluslararası bir yeknesaklık bulunması gerektiği sonucunu ortaya koymaktadır. Özellikle dış bağlantıları bulunan siber ağ olan internetin yaygınlaşması sonucunda, ceza muhakemesi alanında herhangi bir uluslararası adli işbirliğinin olmadığı durumlarda yetkili makamlar da çaresiz kalmakta, bu makamların suçların soruşturulması ve kovuşturulmasına yönelik çabaları yetersiz kalmaktadır²²¹. Ayrıca bilişim teknolojilerinin ve siber ağın gelişmesi ile her geçen gün yeni bir suç türü de ortaya çıkabilmektedir²²². Dünyada bu konuyla ilgili ilk hukuki tartışmalar da dijital teknoloji sayesinde çeşitlilik kazanan ve zarar potansiyeli yükselen suçlara karşı devletlerin dijital yöntemlerle korunması üzerine yoğunlaşmıştır. Siber güvenlik olarak adlandırılan bu geniş tartışma penceresi içerisinde, dijital delillere ilişkin düzenlemelerin yapılması gerekliliği de kendisine yer bulmuştur.

Dolayısıyla günümüzde öncelikli olarak siber ağa yönelik düzenlemelerin uluslararası temelini kurulmasını amaçlayan çalışmalar ve görüşmeler yapılmaktadır. Devletler bunu öncelikli sorun olarak ele almakta, siber güvenlik

²²¹ Konuyla ilgili görüşler için bkz. s. 166 vd.

²²² Karagülmez, **a.g.e.** , ss. 90-91.

meselesi her geçen gün daha büyük bir önem kazanmaktadır. Ayrıca bu yolla devletler arasında işbirliği ve ortaklığın artması sağlanacaktır. Bu temelin kurulması ile dijital delillere yönelik düzenlemelerin de belli bir uluslararası bütünlük içerisinde olacağını söylemek yanlış olmayacaktır.

Tüm bu uluslararası çalışmalar ve görüşmeler sonucunda alınan kararlar, ulusal mevzuatlarda bilişim teknolojilerine ilişkin pek çok yeni düzenleme yapılmasını sağlamıştır. Bilişim teknolojileriyle ilgili tüm bu hukuksal düzenlemeler tam olarak yeterli görünmeseler de gelişim halindedirler. Buna neden olarak ise gerek bu alanın henüz çok yeni olması ve kendi içerisinde sınırlar çizmenin teknolojinin gelişim hızı göz önüne alındığında neredeyse imkânsıza yakın olması, gerekse alınacak katı önlemler sonucunda temel hak ve özgürlükler konusunda güvenlik-özgürlük dengesini özgürlükler aleyhine etkileyecek sonuçlar doğurması gibi durumlar gösterilebilir. Yine de bir değerlendirme yapılmasına rahatlıkla yetecek kadar uluslararası ve ulusal hukuki düzenleme çoktan yapılmıştır. Bu bölümde incelenecek örnekler üzerinden dijital delillere yönelik hukuki düzenlemelerin son durumu ortaya çıkacaktır.

I. Uluslararası hukukta dijital delillere ilişkin düzenlemeler

Gelişen bilişim teknolojisi kullanılarak işlenen suçlar ve yapılan saldırılara yönelik hukuki düzenleme yapılması fikri ilk olarak bilgisayar teknolojisinin ortaya çıktığı ABD’de 1970’li yılların başlarında başlayan tartışmalarla ortaya konulmuştur. Daha sonra konu yine ABD başta olmak üzere Avrupa Konseyi, Avrupa Birliği (1992 öncesi Avrupa Toplulukları zamanı), Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)²²³ ve Uluslararası Polis Teşkilatı (INTERPOL)²²⁴ gibi kurumlar tarafından da ele alınmıştır²²⁵. Yine G-8 ülkeleri²²⁶ tarafından da konuyla ilgili bazı çalışmalar

²²³ Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) bünyesinde, 1982 yılında bilgisayar aracılığıyla işlenen suçları ve bu suçların ceza hukukunda getireceği değişiklikleri tartışmak için Paris’te toplanan uzmanlar komitesi tarafından verilen 1986 tarihli tavsiye metni bulunmaktadır. Ayrıca bu konuda 2002 yılında OECD Konseyi tarafından kabul edilen “Bilgi Sistemleri ve Ağlarının Güvenliği İçin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru” adlı belgeden de bahsetmek gerekir. Detaylı bilgi için bkz. Stein Scholberg, “**The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva**”, Aralık 2008, s. 4.

²²⁴ INTERPOL bilişim suçları ve bunların ceza hukukuna etkilerini ilk tartışan uluslararası kuruluştur. 1979 yılında Paris’te toplanan bir konferansın sonucunda Interpol Genel Kurul’u tarafından bu konuda bir çalışma yapılması kararı alınmıştır. Bkz. Scholberg, **a.g.e.**, s. 3.

²²⁵ Scholberg, **a.g.e.**, ss. 2-3.

yapılmıştır. Konunun uluslararası boyutu ve giderek problemli bir hal alması, bilişim teknolojileri aracılığıyla işlenen suçların artış gösterdiği ülkelerin de yönlendirmesiyle, Birleşmiş Milletler'in de dikkatini çekmiştir. Artık suçla mücadelenin sadece tek bir devletin veya birkaç devletin bir araya gelmesi yoluyla gerçekleştiremeyeceğinin görülmekte ve birçok alanda olduğu gibi, suçla mücadelede ve suç soruşturmalarında da uluslararası işbirliğinin sağlanmasının gereği belirtilmektedir. Dolayısıyla birçok uluslararası örgüt bu konuda çalışmalar yapmaktadır. Bu çalışmada hepsini tek tek incelemek yerine Türkiye'ye hukuki etkileri açısından diğerlerine göre daha ağırlıklı yere sahip olan Birleşmiş Milletler, Avrupa Birliği ve Avrupa Konseyi'nin çalışmaları daha detaylı olarak ele alınacaktır.

A. Birleşmiş Milletler

Birleşmiş Milletler içerisinde hem bireysel ve hem de örgütlü olarak işlenen bilişim suçları açısından gerekli çalışmalar Birleşmiş Milletler Uyuşturucu ve Suç Ofisi altında bulunan Suç Önleme ve Ceza Adalet Komisyonu tarafından yapılmaktadır. Birleşmiş Milletler (BM)'in Havana'da gerçekleştirilen Suçların Önlenmesi ve Suçlulara Muamele konusunda gerçekleştirilen 8. kongresinde tartışılarak genel kurulun aldığı kararla²²⁷, her yönden uluslararası boyut kazanmaya başlayan suçların ve bu suçlarda bilgisayarların etkisinin öncelikli ele alınması gereken hususlardan olduğu belirtilmiştir. Böylece BM, hem üye devletlerden, hem de kendi komitelerinden bu konuda uluslararası bir ceza adaleti politikası geliştirme yolunda çalışmalar yapmalarını istemiştir. Suç Önleme ve Ceza Adalet Komitesi'nin komisyon haline gelerek daha etkili çalışmasına önayak olacak diğer bir kararla birlikte Birleşmiş Milletler, bu konuda kendi adına önemli bir adım atmıştır²²⁸. Böylece 1992 yılında hala Suç Önleme ve Ceza Adalet Komitesi olarak çalışmalarını yürüten komitenin, Ekonomik ve Sosyal Konsey (*Economic and Social Council*

²²⁶ Dünya ölçeğinde gelişmiş 8 büyük devletten (ABD, Almanya, Fransa, İngiltere, İtalya, Japonya, Kanada ve Rusya) oluşan G-8 üyeleri, 1998 yılında (Rusya'nın bulunmadığı o tarihte ismi G-7 idi) Uluslararası Örgütlü Suçlara Dair Kıdemli Uzmanlar Komitesi altında "İleri Teknoloji Alt Komitesi" kurarak bilişim suçları ile mücadele konusuna eğilmiştir. Sonuç olarak ileri teknoloji kullanılan suçlara karşı bir ortak eylem planı hazırlanmıştır. G-8 üyeleri ayrıca sınır aşan suç soruşturamalarında görev alan ve yardım alması gereken adli makamlara yapılacak desteğe ilişkin bir prensipler listesi oluşturmuştur. Detaylı bilgi için bkz. Scholberg, **a.g.e.**, s. 6.

²²⁷ A/RES/45/121, (14.12.1990), <http://www.un.org/documents/ga/res/45/a45r121.htm>. (Erişim tarihi: 15.01.2015)

²²⁸ A/RES/46/152, (18.12.1991), <http://www.un.org/documents/ga/res/46/a46r152.htm>. (Erişim tarihi: 15.01.2015)

[ECOSOC]) tarafından verilen kararlar Suç Önleme ve Ceza Adalet Komisyonu olarak çalışmalarına devam etmesi kararlaştırılmıştır²²⁹. Bu komisyonun görevleri ve öncelikleri de aynı yıl içinde verilen bir başka Ekonomik ve Sosyal Konsey kararıyla belirlenmiştir²³⁰.

1994 yılında da Suç Önleme ve Ceza Adalet Komisyonu'nun yaptığı çalışmalar sonucunda Birleşmiş Milletler Bilgisayarla Gerçekleştirilen Suçların Önlenmesi ve Kontrolüne İlişkin Strateji Metni (*United Nations Manual on the Prevention and Control of Computer-Related Crime [UNMPCCRC]*) kabul edilmiştir²³¹. Metnin içerisinde bilişim yöntemleri ile mücadele konusunda yapılacak çalışmalardan bahsedilirken usul hukukuna yönelik sıkıntılar ve öneriler de ayrı bir bölüm olarak dikkat çekmektedir. Ayrıca bu metin içerisinde bilişim suçları terimi yerine bilgisayar suçları terimi kullanılmaktadır.

İşbu metne göre, bilgisayar temelli usul hukukuna yönelik sıkıntılar yalnızca bilgisayar suçlarına özgü olmayıp, diğer suç tiplerine yönelik soruşturmalarda da ortaya çıkabilmektedir. Bunlara ekonomik suçlardan örnek olarak veri işleyen sistemlere bağımlı çalışan bankacılık sektörü ile klasik suçlara örnek olarak özellikle telekomünikasyon ve bilgisayarları sıklıkla kullanan uyuşturucu tacirlerini içeren soruşturmalar verilebilir. Ancak bu konu yukarıda sayılan örneklerle sınırlandırılmamalıdır. Teknolojinin gelişmesiyle birlikte bilgisayarların günlük yaşam içerisinde artan kullanım oranı, hâkimlerin ve savcılarının delil konusunda da yeni teknolojileri kullanan eşyaya yönelmesini zorunlu kılacaktır²³². Böylece gözle görülür ve maddi (cismani) nitelikteki eşya, yerini günden güne gözle görülemeyen ve gayri maddi eşyaya bırakacaktır. Bu nedenle bu konuya yönelik olarak yargılama makamlarının cebri gücü, kişisel veriler, bilgisayar temelli delillerin kabul edilebilirliği ve uluslararası işbirliği ile ilgili pek çok yeni düzenlemeye ihtiyaç olacaktır²³³. Birleşmiş Milletler'in belirlediği bu dört alan, dijital delillerin ceza hukuku içerisinde yarattığı problemlerin de temellerini oluşturmaktadır.

²²⁹ ECOSOC Resolution 1992/1, http://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-1_E.pdf. (Erişim tarihi: 15.01.2015)

²³⁰ ECOSOC Resolution 1992/22, http://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-22_E.pdf. (Erişim tarihi: 15.01.2015)

²³¹ Belgenin tamamı için <http://www.uncjin.org/Documents/irpc4344.pdf>. (Erişim tarihi: 16.01.2015)

²³² UNMPCCRC, p. 146.

²³³ UNMPCCRC, p. 147.

Öncelikle yargılama makamlarının dijital delil elde etmelerini gerektiren bir soruşturma içerisinde uygulayacakları cebri güçlerine yönelik bazı problemler bulunmaktadır.

Bu alandaki problemlerin ilki arama ve elkoymaya yönelik sıkıntılardan oluşmaktadır. Bilgisayar içindeki bir veriyi elde edebilmek için öncelikle bu bilgisayar sisteminin aranması, daha sonra ise gereklilik halinde ulaşılan verilere elkonması durumu ortaya çıkacaktır²³⁴. Nitekim maddi veri taşıyıcılar içerisinde bulunan verileri arama ve elkoyma durumu, ceza muhakemesinde arama ve elkoyma kuralları açısından gerçeğe ulaşmanın maddi eşya ile sınırlandırılmış olduğu devletler açısından sıkıntı doğuracaktır. Ancak kabul edilebilirlik açısından artık kâğıda yazılmış veri ile manyetik dalga halinde bulunan veri arasında bir fark olmamalıdır ki, bu da hemen her şeyin delil olarak kabul edilebilir olması sonucunu doğurabilir²³⁵. Bunun dışında herhangi bir maddi veri taşıyıcısı içerisinde bulunmayan veya bilgisayar ağları içerisinde bulunan veriler açısından durum daha da karmaşıklaşacaktır. Özellikle bu verilerin elde edilmesinde kullanılacak farklı teknik yöntemler, gerek orantılılık ilkesi gerekse uluslararası hukuk açısından problemler yaratabilirler²³⁶.

Bu alandaki ikinci problem yardımda bulunma yükümlülükleri ile ortaya çıkacaktır. Arama ve elkoymaya yönelik özel düzenlemeler yapılması adli makamların bilgisayar teknolojileri konusunda yeterli bilgi sahibi olmaması sebebiyle de sıkıntılar doğuracaktır. Ancak polislerin bu konularda eğitilmesi yoluyla çözülebilecek bu problem nedeniyle adli makamların, bilgisayarları erişimi kısıtlayan yöntemlere yönelik çözüm üretmede vatandaşların yardımına başvurması kaçınılmaz olacaktır²³⁷. Bu konuda özellikle elkonulacak eşyanın tesliminin istenmesi hali ile tanığın doğruyu söylemesi yükümü farklılık kazanmaktadır. İki halde de verilerin elde edilmesine yönelik işbirliği klasik delil elde edilmesinde beklenen yardıma göre farklılık gösterecektir. Örneğin iki halde de bahsedilen verilerin yazdırılarak adli makamlara teslim edilmesi beklenemeyecektir²³⁸.

²³⁴ UNMPCCRC, p. 149.

²³⁵ UNMPCCRC, p. 150.

²³⁶ UNMPCCRC, p. 151 vd.

²³⁷ UNMPCCRC, p. 157.

²³⁸ UNMPCCRC, p. 159 vd.

Bu alandaki bir diğer problem ise iletişimin denetlenmesi hallerinde ortaya çıkacaktır. Bazı ceza soruşturmaları açısından telekomünikasyon hatları ve bilgisayar sistemlerinin denetlenmesi önemli olacaktır. Ancak kişilerin temel haklarına çok büyük bir müdahale içeren bu gibi önlemler arama ve elkoymadan farklı olarak gizli bir şekilde yapılmaktadır²³⁹. Bu noktada farklı terimlere sahip olan hukuk düzenlemelerinin yeknesaklaştırılarak gerek telekomünikasyon servislerini gerekse bilgisayar sistemlerini bir arada içerecek şekilde düzeltilmeleri gerekecektir²⁴⁰.

Bu konudaki ana problemlere geri dönüş yaparak kişisel veriler açısından oluşacak problemi de ortaya koymak gereklidir. Delil elde edilmesi aşamasında gerek kişisel olan, gerekse kişisel olmayan veriler adli makamların karşısına çıkacaktır. Bu noktada kişisel verilerin toplanmasına ve depolanmasına ilişkin detaylı düzenlemeye sahip devlet sayısı çok azdır. Bireylerin özel yaşamına saygı hakkı ile kamunun çıkarları arasındaki dengenin anayasal olarak düzenlendiği devletler arasında bile bu konuda büyük anlayış farklılıkları olabilmektedir²⁴¹. Bu anlayış farklılıklarının ortadan kaldırılarak özellikle ceza soruşturması için toplanacak kişisel verilere yönelik bireylerin temel haklarına daha saygılı, içerik olarak gerektiğinde bu verilerin adli kayıtlardan silinmesini sağlayacak kadar detaylı düzenlemeler yapılmalıdır²⁴².

Bir başka ana problem ise, dijital delillerin kabul edilebilirliği problemidir. Bu problem sadece bir kabul edilebilirlik problemi olarak algılanmamalıdır. Nitekim sonuç olarak bu problem, adli makamların cebri güçlerini de ilgilendiren bir problemidir. Birçok ülkede bilgisayar çıktıları, verilerin kolaylıkla değiştirilebilir yapıları ve ikinci el nitelikleri nedeniyle ceza yargılamasında delil olarak kabul edilmemektedir²⁴³.

Yine bu metinde bulunan delillerin kabul edilebilirliği konusundaki görüş göz önüne alındığında; delil serbestisinin hakim olduğu Kıta Avrupası hukuku açısından bilgisayar temelli delillere yönelik olarak hakimler sağlamlık değerlendirmesi yapacaklar; kanunlardaki konuyla ilgili eksikler ve resmi belge değerlendirmeleri

²³⁹ UNMPCCRC, p. 163.

²⁴⁰ UNMPCCRC, p. 164.

²⁴¹ UNMPCCRC, p. 167.

²⁴² UNMPCCRC, p. 168 vd.

²⁴³ UNMPCCRC, p. 171.

hariç her hangi bir problem çıkmayacaktır²⁴⁴. İslam Ceza Hukuku'nda bilişim suçlarının tazir suçları arasında yer alması sebebiyle delil serbestisinin uygulanması mümkün olacağından işbu delillerin kabul edilebilirliği aynı Kıta Avrupası sisteminde olduğu gibi yine sıkıntı yaratmayacaktır²⁴⁵. Dolayısıyla bu konudaki problemin daha çok Anglosakson hukuk sistemi ekolünde yer alan delil kuralları açısından sıkıntı yaratacağı söylenebilir. Anglosakson sisteminde yargılamanın sözlülüğü ve çelişmeli yargı daha yoğun kullanılmaktadır. Bazı istisnalar dışında en iyi ve sağlam delil kuralını (*best evidence rule*) kabul eden, bu nedenle belli istisnalar dışında dolaylı delillerin (*hearsay evidence*) genellikle kabul edilmediği sistem nedeniyle, bilgisayar verilerinin durumu çok tartışmalıdır²⁴⁶.

Bu konudaki son ana problem ise uluslararası işbirliği ile ilgilidir. Ancak ceza usul hukuku açısından bahsedilen tüm bu problemlili alanları çözmek için bir uluslararası işbirliği dönemi çoktan başlamıştır²⁴⁷. Buna örnek olarak ise AİHM'nin genel olarak ilgili makamların sahip olduğu cebri güçlerini (özel olarak örneğin iletişimin denetlenmesine yönelik problemleri) AİHS'nin 8. maddesi kapsamında inceleyerek değerlendirmeye başlaması gösterilebilir²⁴⁸.

1994 yılında yapılan ve yukarıda bahsedilen tüm değerlendirmeleri içeren bu geniş çaplı çalışmadan sonra, 2000 yılında bilişim teknolojilerinin suç işlemek amacıyla kötüye kullanılmasına karşı mücadele konusu da BM tarafından ele alınmıştır²⁴⁹. 2001 yılında aynı konuda bir genel kurul kararı²⁵⁰ daha alınmıştır. 2002 yılında alınan bir başka karar²⁵¹ ile siber güvenlik alanında uluslararası işbirliği kurulmasının önemi belirtilmiştir. 2003 yılında alınan bir kararda²⁵² ise 2002

²⁴⁴ UNMPCCRC, p. 173.

²⁴⁵ UNMPCCRC, p. 175.

²⁴⁶ UNMPCCRC, p. 174.

²⁴⁷ UNMPCCRC, p. 176.

²⁴⁸ UNMPCCRC, p. 177.

²⁴⁹ A/RES/55/63, (04.12.2000), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf. (Erişim tarihi: 23.01.2015)

²⁵⁰ A/RES/56/121, (19.12.2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf. (Erişim tarihi: 23.01.2015)

²⁵¹ A/RES/57/239, (20.12.2002), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf. (Erişim tarihi: 23.01.2015)

²⁵² A/RES/58/199, (23.12.2003), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf. (Erişim tarihi: 23.01.2015)

yılındaki karara bir kez daha vurgu yapılmış, siber güvenlik meselesi bakımından önemli olan bilgi merkezlerinin korunması gerekliliğine dikkat çekilmiştir. 2005 yılında alınan bir kararda²⁵³ bir kez daha siber suçlarla mücadelenin önemine değinilmiştir. 2009 yılında alınan bir başka kararla²⁵⁴ siber güvenlik meselesi bir kez daha gündeme getirilmiş, bu sefer üye devletlerin bilgi merkezlerini koruma konusundaki çalışmaları da ele alınmıştır.

Bu konuda yukarıda bahsedilen kararlar dışında Ekonomik ve Sosyal Konsey'in de verdiği kararlar ile yine 2011 yılında Viyana'da siber suçlara yönelik uluslararası meseleleri tartışmak üzere toplanan hükümetler arası bir uzman grubu toplantısı da bulunmaktadır²⁵⁵. Ancak görüldüğü gibi BM bünyesinde dijital delillerin ceza muhakemesine etkisi bakımından yapılmış en kapsamlı çalışma, 1994 yılındaki Birleşmiş Milletler Bilgisayarla Gerçekleştirilen Suçların Önlenmesi ve Kontrolüne İlişkin Strateji Metni (*United Nations Manual on the Prevention and Control of Computer-Related Crime [UNMPCCRC]*)'dir.

Günümüzde BM tarafından kurulmuş olan ve merkezi Cenevre'de bulunan Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union [ITU]*), Birleşmiş Milletler'in bilgi ve iletişim teknolojilerine yönelik uzman kuruluşu olarak çalışmaktadır²⁵⁶. Dolayısıyla siber suçlar ve siber güvenlik konularında yapılacak çalışmalar bu kuruluş bünyesinde devam ettirilerek hızlandırılmış ve genişletilmiştir. Artık ceza muhakemesinde bu konudaki gelişmeler açısından da bu kurumun konuyla ilgili ortaya koyduğu esaslar takip edilmektedir.

²⁵³ A/RES/60/177, (16.12.2005),
https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/General_Assembly/A-RES-60-177.pdf. (Erişim tarihi: 23.01.2015)

²⁵⁴ A/RES/64/211, (21.12.2009),
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211. (Erişim tarihi: 23.01.2015)

²⁵⁵ Marco Gercke, **Understanding Cybercrime: Phenomena, Challenges and Legal Response**, ITU Publication, Eylül 2012, s. 120.
<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>. (Erişim tarihi: 30.01.2015)

²⁵⁶ Gercke, **a.g.e.**, s. 121.

B. Avrupa Birliği

Avrupa Birliği (AB) içinde dijital delillere yönelik çalışmalar incelenmeden önce, AB'nin 2009 yılında yürürlüğe giren Lizbon Antlaşması (*The Treaty of Lisbon*)²⁵⁷ öncesi durumunu incelemek gerekir. Lizbon Anlaşması öncesinde 1993 yılında yürürlüğe giren Maastricht Antlaşması (*The Treaty of Maastricht*)²⁵⁸ uyarınca birlik politikaları üç ana sütun olarak ayrılmaktaydı. Ceza hukukuna yönelik olan, polisiye ve adli işbirliğine dayanan üçüncü sütun²⁵⁹ açısından yapılan düzenlemeler, sütun sisteminin yarattığı sıkıntılar nedeniyle bu alandaki ilerlemeyi de engellemiştir²⁶⁰.

Dijital delillerle ilgisi olabilecek düzenlemeler açısından AB bünyesinde dikkat çeken ilk düzenleme kişisel verilerin işlenmesine ilişkin olan 1995 tarihli Veri Koruma Direktifi (*Data Protection Directive*)²⁶¹, dir. Ayrıca 1997 yılında telekomünikasyon sektörüne ilişkin olarak özel hayatın korunması ve kişisel verilerin işlenmesine ilişkin bir diğer Direktif kabul edilmiştir²⁶². Bunların dışında 1996 yılından beri AB bünyesinde bilgisayar, internet ve siber suçluluğu içeren konularda çalışmalar yapılmaktadır²⁶³.

Bu konuda bahsedilmesi gereken düzenlemelerden biri de 2000 yılında hazırlanarak uygulanan, ancak 2009 yılında AB hukukunun tam olarak bir parçası haline gelen Avrupa Birliği Temel Haklar Bildirgesi (*Charter of Fundamental Rights*

²⁵⁷ The Treaty on the functioning of the European Union (TFEU), <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN>. (Erişim tarihi: 30.01.2015)

²⁵⁸ Treaty on European Union (TEU).

²⁵⁹ Konuyla ilgili bilgi için bkz. Ümit Kocasakal, **Avrupa Birliği Ceza Hukukunun Esasları**, İstanbul: Vedat Yayıncılık, 2004, s. 11.

²⁶⁰ Bu konuda detaylı bilgi için bkz. Gercke, **a.g.e.**, s. 128; Marcin Rozmus/Ilona Topa/Marika Walczak, **“Harmonisation of Criminal Law in the EU Legislation-The Current Status and The Impact of the Treaty of Lisbon”**, ss. 3-8, <http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf>; C-176/03, Commission v Council. (Erişim tarihi: 29.01.2015)

²⁶¹ Directive 95/46/EC, (24.11.1995), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. (Erişim tarihi: 25.01.2015)

²⁶² Directive 97/66/EC, (15.12.1997), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML>. (Erişim tarihi: 25.01.2015)

²⁶³ Detaylı bilgi için bkz. Gercke, **a.g.e.**, s. 129.

of the European Union)²⁶⁴ olmalıdır. Bu belge, AİHS'e üyeleri ayrı ayrı taraf olan ancak birlik bütünlüğü içerisinde taraf olmayan AB'nin, kendi düzenlemeleri açısından bir temel hak temeli oturtmasını sağlamıştır. Özellikle kişilerin özel hayatını, aile hayatını, konutunu ve haberleşme özgürlüğünü koruyan özel hayata ve aile hayatına saygı başlıklı 7. madde ile kişisel verilerin korunmasına ilişkin kuralları düzenleyen 8. madde dijital delillerle ilgili düzenlemelere örnek gösterilebilir.

Bu süreçte AB Konseyi'nin 2005 tarihli Bilişim Sistemlerine Yönelik Saldırlara Dair Çerçeve Kararı (*Council Framework Decision on Attacks Against Information Systems*)²⁶⁵ önem taşımaktadır. Yine 2006 yılı içerisinde Veri Saklama Direktifi (*Data Retention Directive*)²⁶⁶ kabul edilmiştir. Bu Direktif ile internet servis sağlayıcılarına belli trafik verilerini saklama yükümü getirilmektedir. Böylece siber uzaydaki suçluların kimlik tespitinin yapılması amaçlanmaktadır. Ancak internet üzerinden yapılan iletişimin bu şekilde kayıt altına alınması yoğun eleştirilere neden olmuş ve bu konu yargıya taşınmıştır²⁶⁷.

2007 yılı ele alınırsa, AB'nin siber suçlulukla mücadele politikasına yönelik bir belge²⁶⁸ daha bulunmaktadır. 2008 yılında ise AB'ye üye devletlerin ceza muhakemesi kapsamında birbirlerinden delil talep edebilmelerine yarayan bir çerçeve karar olan Avrupa Delil Müzekkeresi (*European Evidence Warrant*)²⁶⁹ kabul edilmiştir. Elektronik verilerin de talep edilebilecek deliller kapsamına girdiği bu çerçeve karar içerisinde belirtilmektedir. Yine delil niteliği taşıyan bu verilerin güvenli bir iletim aracı olacak olan Avrupa Yargı Ağı (*European Judicial Network*) sistemi ile de gönderimi de mümkün kılınmıştır. Türkiye'de de bu sistemin bir parçası olmaya aday olan UYAP mevcuttur.

²⁶⁴ Charter of Fundamental Rights of the European Union

http://www.europarl.europa.eu/charter/pdf/text_en.pdf. (Erişim tarihi: 30.01.2015)

²⁶⁵ Framework Decision 2005/222/JHA, (24.02.2005),

<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN>. (Erişim tarihi: 25.01.2015)

²⁶⁶ Directive 2006/24/EC, (15.03.2006),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>. (Erişim tarihi: 25.01.2015)

²⁶⁷ Bkz. ss. 138-139.

²⁶⁸ COM (2007) 267 final, (22.05.2007),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>. (Erişim tarihi: 25.01.2015)

²⁶⁹ Framework Decision 2008/978/JHA, (18.12.2008),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF>. (Erişim tarihi: 25.01.2015)

2009 yılında Lizbon Antlaşması'nın yürürlüğe girmesi AB içerisinde önemli bir değişiklik yaratmıştır. Antlaşma'nın 82. maddesinden 86. maddesine kadar olan hükümler ile üye devletlere, ceza hukuku alanında adli işbirliği ve uyumu artırma yükümü verilmiştir. Özellikle 83. madde ile bilgisayar suçları da sınır aşan ve ciddi suçlar arasında sayılmış, bunlara yönelik suç tanımlarının ve yaptırımlarının belirlenmesi bakımından asgari standartları tespit eden kurallar öngörme yetkisi tanınması ile üye devletlerce bu konuda gerekli olan mücadelenin gösterilmesi gereği belirtilmiştir. Bu bakımdan, artık bilgisayar suçlarına ilişkin mevzuatın geliştirilmesi AB ile üye devletler açısından paylaşılmış yetki kapsamına girmektedir²⁷⁰. Bu nedenle AB'nin konuya ilişkin hukuken bağlayıcı tasarruflarda bulunma yetkisi doğduğu söylenebilir.

Bunun dışında 2011 yılında Çocuk Pornografisine Dair Direktif (*Directive on Child Pornography*)²⁷¹ kabul edilmiştir. Ayrıca 2013 yılında Avrupa Parlamentosu siber suçlara karşı mücadelede önem taşıyan bir başka Direktif'i kabul etmiştir. Bilişim Sistemlerine Yönelik Saldırlara Dair Direktif (*The Directive on Attacks Against Information Systems*)²⁷², 2005 yılında kabul edilen Bilişim Sistemlerine Yönelik Saldırlara Dair Çerçeve Kararı'nı geliştirmektedir. 2005 yılındaki çerçeve karar ele alınırken, “botnet” denilen ve geniş ölçekli saldırılar için birçok bilgisayarı uzaktan aynı anda kontrol etmeyi sağlayan yöntem göz önünde bulundurulmamıştır. Bu Direktif ile bahsedilen yöntemin eklenmesinin yanı sıra bilişim sistemlerine ve verilere yasadışı erişime yönelik de bazı yeni hususlar ortaya konmuştur. AB'nin ceza adaleti sistemini ve polis işbirliğini geliştirmeyi hedefleyen bu Direktif, Avrupa Polis Teşkilatı (*EUROPOL*) bünyesinde Avrupa Siber Suçlar Merkezi (*European Cybercrime Centre*) kurulması²⁷³ ve AB siber güvenlik stratejisinin (*Cybersecurity*

²⁷⁰ Murat Önok, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, Prof. Dr. Nur Centel'e Armağan, İstanbul: Beta Yayınevi, 2013, s. 1240.

²⁷¹ Directive 2011/92/EU, (13.12.2011), <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093&from=EN>. (Erişim tarihi: 26.01.2015)

²⁷² Directive 2013/40/EU, (12.08.2013), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>. (Erişim tarihi: 26.01.2015)

²⁷³ COM (2012) 140 final, (28.03.2012), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF>. (Erişim tarihi: 26.01.2015)

Strategy of the EU)²⁷⁴ kabulü ile AB'nin bu alandaki güçlenerek süren gelişimi devam etmektedir.

Ayrıca dijital delillere yönelik olarak büyük önem arz eden Avrupa Soruşturamalar Nizamı (*European Investigation Order*)²⁷⁵ ile ceza muhakemesi alanındaki işbirliğinin arttırılması ve delillerin elde edilmesi açısından daha etkili bir sisteme geçilmesi amaçlanmaktadır.

Avrupa Konseyi başlığı altında daha detaylı bir şekilde ele alınacak olan Siber Suçlar Sözleşmesi (*Convention on Cybercrime*)²⁷⁶ de AB için önemli bir belgedir. 2010 yılında AB'nin önceliklerini belirlediği Stockholm Programı (*Stockholm Programme*) ile AB üyelerinin Siber Suçlar Sözleşmesi'nin onaylaması istenmektedir. Hatta uluslararası hukuk açısından bu belgenin temel referans noktası olması gereği ortaya konmaktadır. Ancak bu durumun AB'nin kendi siber suçlar düzenlemesini oluşturmayacağı anlamına gelmediği belirtilmektedir. Nitekim AB her alanda hızlı bir şekilde gelişme yanlısı politikalar izlemektedir. Üstelik Siber Suçlar Sözleşmesi'nin ilk halinin üzerinden on yıldan fazla bir süre geçmesine rağmen, Sözleşmede herhangi bir güncelleme yapılmamıştır²⁷⁷.

Bunun yanı sıra AB'nin mevcut yapısı²⁷⁸ çerçevesinde ve AİHS'e ek 14. Protokol'ün getirdiği değişiklik²⁷⁹ sayesinde, AB'nin kendisine üye devletlerden ayrı bir tüzel kişi olarak AİHS'e taraf olması hedeflerden biri olarak belirlenmiştir. AB'nin yürütme organı olan Avrupa Komisyonu da, AİHS'ye taraf olmanın AB'nin kendi düzenlemeleriyle uyumlu olup olmadığı konusunda, AB'nin en üst mahkemesi olan Adalet Divanı'na başvurmuştur, ancak bu başvuru olumsuz bir karar ile sonuçlanmıştır²⁸⁰.

²⁷⁴ JOIN(2013) 1 final, (07.02.2013) ,

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. (Erişim tarihi: 26.01.2015)

²⁷⁵ Directive 2014/41/EU, (03.04.2014),

<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0041&from=EN>. (Erişim tarihi: 26.01.2015)

²⁷⁶ Convention on Cybercrime ETS no. 185

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. (Erişim tarihi: 10.01.2015)

²⁷⁷ Gercke, **a.g.e.** , s. 135.

²⁷⁸ TEU ve TFEU'nun birleştirilmiş hali için bkz.

<http://www.consilium.europa.eu/uedocs/cmsUpload/st06655-re01.en08.pdf>.(Erişim tarihi: 30.01.2015)

²⁷⁹ İşbu değişiklik ile AİHS 59/2 maddesi “Avrupa Birliği bu sözleşmeye katılabilir.” şeklinde düzenlenmiştir.

²⁸⁰ Bu konudaki karar için bkz. ss. 139-140.

Tüm bu gelişmeler ortaya konulunca, AB'nin ortak bir Avrupa Ceza ve Ceza Muhakemesi Hukuku oluşturabilme yolundaki çalışmalarında ilerlediği söylenebilir. Zamanında ilk olarak mali suçlar açısından ortaya konmuş olan *Corpus Juris*²⁸¹ anlayışının farklı düzenlemeler ile hızlı fakat emin adımlarla gerçekleşmekte olduğu söylenebilir.

C. Avrupa Konseyi

Avrupa Konseyi (AK)'nin düzenlemelerinden bahsederken akla ilk gelen belgeler İnsan Haklarını ve Ana Hürriyetleri Korumaya dair Sözleşme (*European Convention on Human Rights* {Avrupa İnsan Hakları Sözleşmesi [AİHS]})²⁸² ve bu Sözleşme ek protokolleridir. 1953 yılında yürürlüğe giren AİHS zaman içerisinde bazı değişiklikler ve gelişmeler geçirirse de günümüzde hala etkili bir biçimde kullanılmaktadır. AİHS'in özel yaşam, aile yaşamı ile konut dokunulmazlığı ve haberleşme özgürlüğü meselelerini düzenleyen özel hayatın ve aile hayatının korunması başlıklı 8. maddesi ile kişilerin mülkiyetinin korunması konusunu içeren AİHS'e ek Protokol'ün mülkiyetin korunması başlıklı 1. maddesi dijital delillere yönelik uygulamalarda önemli olabilecek maddelerdir²⁸³. BM'de 1994 yılındaki Birleşmiş Milletler Bilgisayarla Gerçekleştirilen Suçların Önlenmesi ve Kontrolüne İlişkin Strateji Metni içerisinde dijital delillere yönelik olarak AİHM'in AİHS üzerinden yaptığı yargı denetiminin öneminden bahsetmiştir²⁸⁴.

AİHS'i bir kenara koyacak olursak, dijital delillere ilişkin yapılan uluslararası düzenlemelerden belki de en önemlisi olan Sanal Ortamda İşlenen Suçlar Sözleşmesi yani diğer adıyla Siber Suçlar Sözleşmesi (SSS) (*Convention on Cybercrime*), Avrupa Konseyi'nin çalışmalarıyla ortaya çıkmıştır.

²⁸¹ Ceza hukuku kuralları açısından suçlara yönelik daha merkeziyetçi ve ortak bir Avrupa vurgusu üzerine yapılan çalışmalar (Örneğin Avrupa Savcılığı kurumunun kurulması) hakkında detaylı bilgi için bkz. Keskin, Serap, “**Avrupa Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi**”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, ss. 178 vd.

²⁸² European Convention on Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf (Erişim tarihi: 20.01.2015); Resmi Gazete, Tarih: 19.03.1954, Sayı: 8662, İnsan Haklarını ve Ana Hürriyetleri Korumaya dair Sözleşme (Avrupa İnsan Hakları Sözleşmesi [AİHS])

²⁸³ Bu konudaki AİHM kararları için bkz. s. 125 vd.

²⁸⁴ Bkz. s. 67.

SSS'nin son metninin kabulü öncesinde yaşanan gelişmelere bakıldığında, AK'nin bünyesinde 1985 yılında bilgisayar suçlarının hukuki yönlerini tartışmak ve bu konuda çalışma yapmak üzere bir uzman komitesi kurulmuştur. Bu komitenin çalışmaları sonucunda 1989 yılında Bilgisayarlara İlişkin Suçlara Dair Uzman Raporu (*Expert Report on Computer-Related Crime*) hazırlanmıştır²⁸⁵. Avrupa Konseyi Bakanlar Komitesi tarafından yine bu suçlara ilişkin olarak 1989 yılında kabul edilen bir tavsiye kararı bulunmakla birlikte, 1995 yılında ise bu sefer sınır aşan bilgisayar suçlarından kaynaklanan sorunlara yönelik olarak başka bir tavsiye kararı kabul edilmiştir²⁸⁶.

Daha sonraki dönemde ise SSS ortaya çıkmıştır. AK bünyesinde 1997 yılında siber suçlarla mücadele konusunda kurulan bir uzman komitesinin yaptığı toplantılar ve çalışmalar sonucunda ortaya çıkan bu metin, üyelerin dışişleri bakanlarınca 8 Kasım 2001 tarihinde imzalanarak kabul edilmiş ve 26 Kasım 2001 tarihinde ise Macaristan'ın Budapeşte kentinde imzaya açılmıştır. Daha önce de belirtildiği gibi bilişim teknolojileri aracılığıyla işlenen suçların soruşturmaları açısından, SSS önemli bir uluslararası belgedir. Nitekim bu uluslararası belge AK üyeleri dışında bazı ülkeler tarafından da imzalanmıştır²⁸⁷.

Sözleşme'nin 36. maddesine göre, en az üçü AK üyesi olan beş ülkenin onaylarını beyan ettikleri tarihten sonraki üç aylık sürenin bittiği tarihten itibaren gelen ilk ayın ilk gününde yürürlük kazanacağı belirtilmiştir. Belirtilen şartları sağlayarak 1 Temmuz 2004 tarihinde yürürlüğe giren bu uluslararası sözleşmenin içeriğinde, ceza muhakemesinde dijital delillerin nasıl elde edileceğine, korunacağına ve değiştirileceğine yönelik hükümler yer almaktadır. Ayrıca 2006 yılında bilgisayar sistemleri aracılığıyla yapılan ırkçılık ve yabancı düşmanlığı konularını da içeren bir

²⁸⁵ Gercke, **a.g.e.**, s. 123.

²⁸⁶ Gercke, **a.g.e.**, s. 124.

²⁸⁷ Sözleşme, Avrupa Konseyi üyelerinden Rusya ve San Marino tarafından imzalanmamıştır. Ancak Avrupa Konseyi üyesi olmayan ABD, Güney Afrika, Japonya ve Kanada sözleşmeyi imzalamıştır. Ayrıca şu an ABD, Avustralya, Dominik Cumhuriyeti, Japonya, Mauritius ve Panama tarafından sözleşme onaylanmış bulunmaktadır.

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>. (Erişim tarihi: 10.01.2015)

Ek Protokol yürürlüğe girmiştir. Türkiye de SSS'yi 10 Kasım 2010 tarihinde imzalamış ve 2014 yılında da onaylamıştır²⁸⁸.

Sözleşme dijital deliller açısından incelendiğinde, dijital delillere yönelik maddelerin Sözleşme'nin usule yönelik hazırlanmış ikinci kısmındaki 14. madde ile 21. madde arasında bulunduğu görülecektir.

Sözleşme'nin usul hukukuna yönelik genel hükümleri olan 14. maddesi ile Sözleşmeye taraf devletlerin, Sözleşme'nin 16. maddesinden 21. maddesine kadar sayılan önlemleri, iç hukuklarında gerekli çalışmaları yaparak düzenlemesi gerektiği belirtilmektedir. Ancak bu düzenlemelerin yapılması ve daha sonra uygulanması

²⁸⁸ 22 Nisan 2014 tarih ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanmış ve Kanun'un 2 Mayıs 2014 tarihinde 28988 sayılı Resmi Gazete'de yayımlanmasıyla yürürlüğe girmiştir.

Türkiye Sözleşme'nin madde 2, 7, 14/3 (b), 22, 24, 27/2, 29/4, 35/1, 40 ve 42 hükümlerine toplam 8 başlık altında beyan ve çekince koymuştur.

**“DİŞİŞLERİ KOMİSYONUNUN KABUL ETTİĞİ METNE EKLİ ÇEKİNCELER VE BEYANLAR
SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİ (ETS-NO. 185) İLE İLGİLİ ÇEKİNCELER VE
BEYANLAR**

1) 40 ıncı madde ve 2 nci maddeye istinaden, Türkiye Cumhuriyeti Devleti, suçun bilgisayar verilerini elde etmek veya başka bir sahtekar niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koştuğunu beyan eder.

2) 40 ıncı madde ve 7 nci maddeye istinaden, Türkiye Cumhuriyeti Devleti, bilgisayarla bağlantılı sahteciliğe ilişkin 7 nci maddedeki suç tanımının Türk kanunlarına göre dolandırma veya benzeri hileli davranış kastını gerektirdiğini beyan eder.

3) 42 nci madde ve 14 üncü maddenin 3 (b) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak, söz konusu sistemin belli bir kullanıcı grubunun menfaatine işletiliyor olması; halka açık iletişim şebekelerini kullanmıyor olması ve halka açık ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması halinde, söz konusu aktarıma ilişkin olarak 20 nci ve 21 inci maddelerde belirtilen önlemleri uygulamama hakkını saklı tutar.

4) 42 nci madde ve 22 nci maddeye istinaden, Türkiye Cumhuriyeti Devleti, Türk vatandaşının yurt dışında işlemiş olduğu suçlardan dolayı Türk Ceza Kanununun 11 inci ve 13 üncü maddeleri çerçevesinde yargı yetkisini kullanma hakkını saklı tutar.

5) 42 nci madde ve 29 uncu maddenin 4 üncü paragrafına istinaden, Türkiye Cumhuriyeti Devleti, çifte suçluluk şartının verilerin açıklandığı tarihte yerine getirilemiyor olduğuna ilişkin gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması talebini reddetme hakkını saklı tutar.

6) 24 üncü maddenin 7 (a) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, suçluların iadesine ilişkin anlaşma mevcut olmadığı durumlarda, suçluların iadesi veya geçici tutuklama taleplerini iletmek veya almak üzere Adalet Bakanlığını yetkili makam olarak belirler.

7) 27 nci maddenin 2 (c) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, karşılıklı yardım taleplerinde bulunmak, talepleri yanıtlamak, bu taleplerin gereğini yerine getirmek veya bunların gereğini yerine getirecek makamlara bu talepleri iletmekle Adalet Bakanlığını merkezi makam olarak belirler.

8) 35 inci maddenin 1 inci paragrafına istinaden, Türkiye Cumhuriyeti Devleti, 7 gün/24 saat esasına göre temas noktasının Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı olduğunu beyan eder.”

sırasında uluslararası insan hakları standartları ile uyumlu olmaları gerekmektedir. Sözleşmenin 15. maddesi ile bu standartlar açısından ise 1950 tarihli Avrupa İnsan Hakları Sözleşmesi ve ek protokolleri, BM çerçevesinde 1966 tarihli Medeni ve Siyasal Haklar Sözleşmesi ve diğer bölgesel düzeydeki insan hakları sözleşmeleri dikkate alınacağı belirtilmiştir. Bu da şu anlama gelmektedir: Bu konuda yapılacak düzenlemeler kanunla belirlenecek ve kanun içeriği açık, anlaşılabilir, ulaşılabilir ve öngörülebilir olacaktır. Ayrıca temel haklara müdahalede bulunan bu önlemler hukuki bir amaç doğrultusunda, demokratik bir toplumun sosyal ihtiyacı için gerekli ve orantılı, aleyhine kanun yolu bulunan, kötüye kullanmaya karşı garanti içeren şekilde düzenlenmelidir²⁸⁹.

Sözleşme'nin 16. maddesinden 21. maddesine kadar sayılan önlemler ise bilişim koruma önlemleri olarak adlandırılabilirler²⁹⁰. Bu önlemler sayesinde ceza muhakemesi hukukunun klasik delil elde etme yöntemlerinin ilerisine geçilerek suç soruşturmalarında dijital delillerin modern yöntemlerle elde edilmesi mümkün olacaktır.

Bu yöntemlerden ilki 16. maddede düzenlenen depolanan bilgisayar verilerinin²⁹¹ hızlı şekilde korunması (*expedited preservation of stored computer data*) yöntemidir. Uygulamada bu yöntem için yapılan işleme hızlı dondurma (*quick freeze*) denilmektedir²⁹². Bilgisayar verilerinin kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olmaları nedeniyle böyle bir koruma önlemi ortaya konmuştur. Bu önlem sayesinde bilgisayar sistemlerinde²⁹³ bulunan ve delil olabilecek bilgisayar verilerinin orijinal halleri güvence altına alınmaktadır. Üstelik madde içeriğine göre sadece veri içeriği değil bu verilere ilişkin trafik verileri²⁹⁴ de korunacaktır (SSS 16/1).

²⁸⁹ AIHM değerlendirmesi açısından sahip olunması gereken özellikler bunlar olacaktır.

²⁹⁰ Keskin, **a.g.e.**, ss. 155-180.

²⁹¹ SSS 1/b ye göre bilgisayar verisi (*computer data*) terimi, bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade etmektedir.

²⁹² Kunter/Yenisay/Nuhoğlu (2013), **a.g.e.**, s. 1307.

²⁹³ SSS 1/a ya göre bilgisayar sistemi (*computer system*) terimi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade etmektedir.

²⁹⁴ SSS 1/d ye göre trafik verisi (*traffic data*) bir bilgisayar sistemi aracılığıyla gerçekleşen iletişimle ilgili olan, iletişim zincirinin bir halkasını teşkil eden bilgisayar sistemi tarafından üretilmiş, iletişimin başlangıç noktasını, hedefe varış noktasını, izlediği yolu, saatini, tarihini, boyutunu, süresini veya iletişimde kullanılan temel hizmetin türünü gösteren herhangi bir bilgisayar verisini ifade etmektedir.

Bilgisayar verisini elinde veya denetiminde bulunduran kişiye yönelik verilen bir hâkim kararı üzerine, veriler açısından azami 90 gün süre ile hızlı dondurma emri verilebilir. Üstelik bu sürenin daha sonra uzatılabilmesi de mümkündür (SSS 16/2). Verilen bu kararda aynı zamanda ilgili kişiye, hâkim tarafından öngörülen bir süre boyunca, işlemi gizli tutma yükümü de getirilmektedir (SSS 16/3) .

Bir başka bilişim koruma önlemi ise 17. maddedeki trafik verilerinin hızlı şekilde korunması ve kısmen açıklanması (*expedited preservation and partial disclosure of traffic data*) işlemidir. Bu madde ile bilgisayar verilerinin iletişimini sağlayan hizmet sağlayıcılara²⁹⁵ yönelik yükümlülükler getirilmesi gereği ortaya konmaktadır (SSS 17/1-a). Nitekim 16. maddedeki trafik verilerinin de dondurulmasını içeren taleplerin gerçekleşebilmesi için gerekli olan trafik verileri ile ilgili bilgiler hizmet sağlayıcılarda bulunmaktadır.

Trafik verilerinin hızlı şekilde korumaya alınması kararı alınmadan önce yetkili makamlar, trafik verileri ve bu verilerin izledikleri yol hakkında herhangi bir bilgiye sahip değildirler. Bu nedenle yetkili makamlar bir karar almadan önce, hizmet sağlayıcılardan bu verilerin izlediği yol ile ilgili bilgiyi alacak kadar trafik verisi açıklamalarını da talep edebileceklerdir (SSS 17/1-b).

Sözleşmedeki üçüncü bilişim koruma önlemi, 18. maddede bulunan üretim emri (*production order*) önlemidir. Bu önlem yoluyla kişilere, kendi mülkiyetlerinde ya da kontrollerinde bulunan ve depolanmış durumdaki bilgisayar verilerini teslim etme zorunluluğu getirilmektedir (SSS 18/1-a). Ayrıca ulusal sınırlar içindeki hizmet sağlayıcıların, mülkiyetlerinde ya da kontrollerinde bulunan hizmete ilişkin abone bilgilerini²⁹⁶ teslim etmeye zorlamaları olanağı da getirilmektedir (SSS 18/1-b).

²⁹⁵ Sözleşme 1/c ye göre hizmet sağlayıcı (*service provider*);

i. hizmetlerini kullananlara bir bilgisayar sistemi aracılığıyla iletişim kurma olanağı sağlayan her türlü kamu veya özel sektör tüzel kişisini, ve

ii. böylesi iletişim hizmeti veya bu hizmetlerin kullanıcıları adına bilgisayar verilerini işleyen veya depolayan diğer her türlü tüzel kişiyi ifade etmektedir.

²⁹⁶ SSS 18/3 e göre abone bilgisi terimi, bir hizmet sağlayıcı tarafından bilgisayar verileri biçiminde veya başka bir biçimde tutulan, trafik veya içerik verileri hariç olmak üzere, hizmetlerin abonelerine ilişkin:

a. kullanılan iletişim hizmeti türünün, ayrıca belirlenen teknik hükümlerin ve hizmet süresinin;

b. hizmet anlaşması veya düzenlemesi bağlamında erişilebilir abone kimliğinin, posta veya coğrafi adresinin, telefon veya diğer erişim numarasının, fatura ve ödeme bilgilerinin;

Bir diğ er biliřim koruma  nlemi ise 19. maddedeki depolanmıř bilgisayar verilerinin aranması ve bunlara elkoyma (*search and seizure of stored computer data*) iřlemidir. Bu maddeye g re yetkili adli makamların bir bilgisayar sisteminin tamamı veya bir kısmı i erisinde depolanmıř bilgisayar verilerine ve sisteme baėlı olmadan bir veri depolama aygıtında depolanan verilere eriřebilmesi i in arama veya arama benzeri tedbirler d zenlenmelidir (SSS 19/1). Hatta bu arama tedbiri verilerin ger ek te  lke i inde bařka bir sistemde olduėuna dair yeterli ř phe bulunması halinde geniřletilebilmelidir (SSS 19/2). Koyulacak bu arama veya arama benzeri tedbirlerinin, bir bilgisayar sisteminin tamamına veya bir kısmına veya sisteme baėlı olmayan veri depolama aygıtına elkoymasına veya g vence altına alınmasına y nelik tedbirlerle desteklenmeleri gerekmektedir. Bunun yanı sıra bu verilerin kopyalanmasını ve muhafazasını, verilerin b t nl ė n n korunmasını ve verilerin eriřilemez hale getirilmesini ya da kaldırılmasını ama layan tedbirler de bulunmalıdır (SSS 19/3).

S zleřme'nin 20. maddesinde bulunan trafik verilerinin ger ek zamanlı olarak toplanması (*real-time collection of traffic data*) bir bařka biliřim koruma  nlemidir. Bu  nleme g re devletler mevcut teknik olanakları elverdiėi  l  de kendi  lke sınırları i erisinde bilgisayar sistemleri aracılıėıyla iletilen ve iletiřime iliřkin trafik verilerini toplayabilirler ya da kaydedebilirler. Ayrıca hizmet saėlayıcıların da, bu iřlemler ile ilgili devletin yetkili organları ile iřbirliėi i erisine girmesi saėlanmalıdır (SSS 20/1).

Son olarak 21. maddedeki i erik verilerinin denetlenmesi (*interception of content data*) biliřim koruma  nleminden de bahsetmek gerekir. I erik verilerinin denetlenmesi  nleminde, verilerin i eriklerine iliřkin bir denetim yapılması ile  zel yařamın dokunulmazlıėı hakkı ve iletiřim  zg rl ė ne yapılacak m dahale daha yoėun olacaėı i in, bu  nlemin ulusal hukuk tarafından belirlenecek daha ciddi su lara iliřkin soruřturmalarda uygulanması yerinde olacaktır (SSS 21/1). Ayrıca internet servis saėlayıcıların tedbirlerin uygulanmasını gizli tutma y k mlerine y nelik d zenleme yapılması gereėi de ek olarak belirtilmiřtir (SSS 21/3).

c. hizmet anlařması veya d zenlemesi baėlamında eriřilebilir iletiřim te hizatının kurulduėu yere iliřkin diėer bilgilerin;
belirlenmesini saėlayabilecek herhangi bir bilgiyi ifade etmektedir.

Ayrıca sözleşmede taraflara, bilgisayar sistemleri ve verileri ile ilgili ceza soruşturma ve kovuşturmalarda, elektronik ortamda delillerin toplanabilmesi açısından, ceza hukukundaki ulusal ve uluslararası düzenlemeler çerçevesinde bir uluslararası işbirliğine gitmeleri gereğinden bahsedilmiştir (SSS 23).

Görüldüğü gibi SSS alanındaki boşlukları dolduran önemli bir uluslararası kaynaktır. 2001 yılından bugüne ilgili konularda pek çok değişim ve gelişim olduğu için, SSS'nin de bu değişimlere ayak uydurması gerektiği ve dolayısıyla güncellemeye ihtiyaç duyduğu belirtilmektedir²⁹⁷. Ancak 2014 yılında bile hala SSS'yi onaylayan devletler bulunmakta ve yeni çalışmalar yapılırken hali hazırda iyi bir altyapısı olan SSS'nin en azından asgari standartlar açısından kullanılması gerektiği görüşü de güç kazanmaktadır.

II. Bazı yabancı hukuk düzenlerinde dijital delillere ilişkin düzenlemeler

A. Almanya

Almanya'da ceza muhakemesinde delil serbestisi esas alınmaktadır. Dolayısıyla mahkemeye her tür delil sunulabilir (StPO 261). Dijital deliller de buna dâhildir. Hatta delilin kendine has özellikleri bulunması hâkimin kanaatini etkilemede daha etkili bile olabilir²⁹⁸. Almanya'da dijital delillere yönelik genel hükümler Almanya Ceza Usul Kanunu (*Strafprozessordnung[StPO]*)²⁹⁹ içerisinde bulunmaktadır. Bu nedenle inceleme bu kanun üzerinden yapılacaktır.

Öncelikle Almanya'daki ceza muhakemesi işlemlerinin Alman Dijital İmza Kanunu'na uygun olması halinde elektronik yöntemlerle de yapılabileceği belirtilmelidir (StPO 41a). Bu durum aynı Türkiye'deki UYAP sistemine benzemektedir.

²⁹⁷ Gercke, **a.g.e.**, s. 125.

²⁹⁸ RAND Europe & Lawford, **Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs**, Aralık 2005, s. 115, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf. (Erişim tarihi: 08.10.2014)

²⁹⁹ Bu kanunun İngilizce metni için bkz. http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

Almanya’da suçlar polise ihbar veya polisin keşfi üzerine savcının yürüteceği ceza soruşturmasında inceleneceklerdir. Polisin, delil elde edileceğine dair şüphe bulunması halinde; şüpheliye veya üçüncü kişilere yönelik üst, eşya, ev, işyeri ve onlara ait diğer yerleri araması mümkündür (StPO 102, 103). Ancak yapılacak aramada hâkimin bu aramayla ilgili özel olarak vereceği arama kararı olması gerekir. Acil durumlarda bu kararı savcı da verebilir (StPO 105). Dijital delillere yönelik özel bir arama şekli düzenlenmediği için, genel arama kuralları dijital deliller açısından da geçerli olacaktır. Arama bittikten sonra, aramaya maruz kalanların isteği üzerine aramanın sebebi ve aramaya sebebiyet veren suçu gösteren yazılı bir belge verilir (StPO 107).

Yine elkoymada dijital delillere ilişkin özel bir hüküm bulunmamakta, bu nedenle elkoymada da genel hüküm dijital delillere de uygulanmaktadır (StPO 94). Kanunda kişilere elkoyulacak eşyaları teslim etme yükümü getiren bir madde (StPO 95) ile elkoyulamayacak eşya listesi içeren bir madde (StPO 97) de bulunmaktadır. Elkoyma kararı mahkeme tarafından verilmekte olup, acil hallerde savcı tarafından da verilebilmektedir (StPO 98). Yine elkonulan eşya listesi veya elkonulan eşya bulunmuyorsa buna ilişkin belge de aynı aramada olduğu gibi ilgilinin isteği üzerine düzenlenecektir (StPO 107).

Arama sonucunda elkonulan verileri inceleme yetkisi savcıya veya onun görevlendirdiği personele aittir. Bunun dışında elektronik veri taşıyan aygıtların içerisindeki verilerin kaybolma riskinin bulunduğu durumlarda, bahsedilen aygıtta erişim mümkün olduğu sürece, ilgili inceleme başka bir yerden de yapılabilir (StPO 110/3).

Konuyla ilgili bir diğer düzenleme ise belli katalog suçlar açısından adli makamlara kişisel verilerin birbirleriyle değerlendirilebilmesi imkânı veren uygulamadır (StPO 98a). Kişisel verilerin değerlendirmesi kararı mahkeme tarafından verilmekle birlikte, acil hallerde savcı da bu kararı verebilecektir. Değerlendirme işleminden sonra veriler gecikmeksizin iade edilecek, ceza yargılaması açısından gereği kalmayınca silinecektir. Ayrıca bu işlemin uygulandığına dair ilgili denetim mekanizmalarına da haber verilecektir (StPO 98b).

Ayrıca elde edilen kişisel verilerin adli makamlar elinde önceden bulunan verilerle karşılaştırılması da düzenlenmiştir (StPO 98c).

Dijital delillere ilişkin bir başka düzenleme ise telekomünikasyon iletişiminin denetlenmesi tedbiridir (StPO 100a). Bu tedbire başvurulabilmesi için, şüphelinin suçta fail ya da muharrik olduğuna ilişkin somut delil olması ve başka türlü delil bulunmasının ya da konum tespiti yapılmasının imkânsıza yakın olması veya mümkün olmaması gerekir (StPO 100a/1). İşbu önlem yalnızca belli katalog suçlar açısından uygulanabilmektedir (StPO 100a/2). Ayrıca hakkında tedbire başvurulacak kişinin suç soruşturması açısından, şüpheliyle iletişim kurduğuna dair somut deliller bulunmalıdır (StPO 100a/3). Bu tedbir açısından özel hayatın çekirdek alanına yapılan müdahalelerle elde edilen deliller yargılamada kullanılamazlar ve hemen silinmeleri gerekir (StPO 100a/4). Telekomünikasyon iletişiminin denetlenmesi kararı yalnızca savcı istemi üzerine mahkeme kararı ile uygulanabilir (StPO 100b/1). Bu kararda biliniyorsa tedbirin uygulanacağı kişinin adı ve adresi, tedbirin uygulanacağı telefon numarası, iletişim kodu ya da iletişim terminaline ilişkin bilgi, tedbirin tipi, kapsamı ve ne zaman sona ereceği de yazacak şekilde süresi de belirtilir (StPO 100b/2). Bu konuda telekomünikasyon hizmetinde bulunanların mahkemeye yardım etme yükümü bulunmaktadır (StPO 100b/3). İşbu tedbirin sürdürülemediği hallerde, tedbir durdurularak, mahkemeye bu konuda haber verilmesi gerekir (StPO 100b/4). Ayrıca savcılar Adalet Bakanlığı'na bilgi vermek amacıyla, yıl içerisinde uygulanan tüm tedbirlere ilişkin yıllık rapor hazırlarlar (StPO 100b/5).

Dijital delillere ilişkin bir başka tedbir ise özel ortamlardaki özel konuşmaların denetlenmesi ve kayıdır (StPO 100c). Bu tedbirin uygulanabilmesi için şüphelinin suçta fail ya da muharrik olduğuna ilişkin somut delil olması ve başka türlü delil bulunmasının ya da konum tespiti yapılmasının imkânsıza yakın olması veya mümkün olmaması gerekir (StPO 100c/1). Yine bu tedbirin uygulanabileceği suç soruşturmaları açısından da oluşturulmuş bir katalog vardır (StPO 100c/2). Ayrıca bu tedbir yalnızca şüpheliye yönelik kullanılabilir (StPO 100c/3). İşbu tedbire savcı tarafından karar verilebilir, ancak bu kararın üç gün içerisinde hâkim tarafından onaylanması gerekir (StPO 100d). Tedbire yönelik kararda biliniyorsa tedbirin uygulanacağı kişinin adı ve adresi, ithamın çeşidi ve tedbirin gerekçesi, tedbirin tipi, kapsamı ve süresi, elde edilecek bilginin çeşidi ve soruşturma açısından önemi de

belirtilir (StPO 100d/2). Bu tedbir belli şartlara baęlı olarak uzatılabilir (StPO 100d/3). Savcılar bu tedbirin uygulanmasına ilişkin olarak da Adalet Bakanlığı'na yıllık rapor yazacaklardır (StPO 100e). Hükümet meclise bu raporlar hakkında bilgi verdikten sonra, raporlara ilişkin bilgiler internette yayınlanmaktadır

Bir başka tedbir ise teknik yöntemlerin kullanılmasıyla denetleme yapılmasıdır (StPO 100f). Bu tedbir kişinin özel ortamlar dışındaki denetimini ve kaydını içerir. Bu tedbirin uygulanabilmesi için şüphelinin suçta fail ya da muharrik olduğuna ilişkin somut delil olması ve başka türlü delil bulunmasının ya da konum tespiti yapılmasının imkânsıza yakın olması veya mümkün olmaması gerekir (StPO 100f/1). Bu tedbire başvurulabilmesi açısından da belli bir suç kataloęı bulunmakla birlikte, bu tedbir yalnızca şüpheliye yönelik kullanılabilir (StPO 100f/2).

Bir başka tedbir ise telekomünikasyon baęlantılarına ilişkin bilgi toplamadır (StPO 100g). Telekomünikasyon yoluyla ilgili katalog suçlardan birinin işlenmesi halinde şüphelinin yerine ve telekomünikasyon trafik verilerine ilişkin bilgi toplanabilir. Ancak bu denetimle elde edilen bilgilerin delil olarak kabul edilebilir olması için şüphelinin yerinin tespiti açısından başka bir yöntemin izlenememesi ve elde edilen bilginin davadaki önemi açısından orantılı olması gerekir. Bu yöntemle ilişkin olarak da savcılar tarafından yıllık raporlar hazırlanır (StPO 100g/4).

Dijital delillerle ilgili olan bir başka tedbir ise fotoğraf çekimi ve teknik takiptir (StPO 100h). Fotoğraf çekimi tedbirine şüphelinin konumuna başka yöntemlerle ulaşmanın mümkün olamayacağı gerekçesiyle başvurulabilirken; teknik takip için teknik takip yapılacak kişinin şüpheli ile olan iletişimi aracılığıyla, yine başka yöntemlerle ulaşmanın mümkün olamayacağı şüphelinin konumuna erişmek için başvurulmaktadır (StPO 100h/2).

Bu konuda kanunda bulunan bir başka yöntem ise cep telefonu IP (*IP Multimedia Subsystem [IMS]*)'lerinin takibidir (StPO 100i). Bu yöntemle cep telefonunun aygıt kimlik numarası aracılığıyla kullandığı terminalin ve telefonun içerisinde bulunan kartın tespitinin yanı sıra terminal konumu da tespit edilebilmektedir. Bu tedbirin uygulanabilmesi için şüphelinin suçta fail ya da

muharrik olduğuna ilişkin somut delil olması ve başka türlü şüphelinin konum tespitinin yapılmasının imkânsıza yakın olması veya mümkün olmaması gerekir.

Yukarıdaki tedbirlerden farklı olarak polisin görevleri kısmında bulunan bir yöntem ise bilgisayar aracılığıyla arama hükmüdür (StPO 163d). Bu yöntemde ise Almanya'ya girişlerde yapılan sınır kontrolü sırasında, hakkında bu maddede belirtilen katalog suçları işlediği konusunda şüphe bulunan kişilerin bilgilerinin elektronik sistem aracılığıyla kaydedilebileceği hüküm altına alınmıştır. Ayrıca kişisel tanıtıcı bilgilerin elde edilmesine yönelik emir bulunan genel polis kontrollerinde, suç şüphesi hallerinde, bu bilgiler de kaydedilebilmektedir (StPO 163e).

Yukarıda sayılan tüm bu yöntemlere ilişkin uygulamalar sonrasında adli makamların, maddede sayılan ilgili kişileri uygulanan tedbir hakkında bilgilendirme yükümü bulunmaktadır (StPO 101).

Bu arada Almanya ile ilgili kısmı bitirmeden önce son bir hükümden daha bahsetmek yararlı olabilir. Bu hüküm ise Telekomünikasyon Kanunu (*Telekommunikationsgesetz[TKG]*)'na göre bilgi toplama yetkisi olanların adli makamların bilgi taleplerini karşılama yöntemleri ve yükümlerine ilişkindir (StPO 100j).

Ayrıca hâkimlerin gerekli hallerde uzman yardımına başvurması da mümkündür (StPO 73). Bu genel madde dijital delillere yönelik de uygulanabilir. Böylece tüm bu tedbirlerin uygulanması sırasında adli bilişim uzmanı yardımı alınması mümkün olacaktır.

B. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri (ABD)'nde ceza muhakemesi sistemi genel olarak federal devlet düzenlemeleri ve ABD Anayasası çerçevesinde şekillenmektedir³⁰⁰. Delillere yönelik kurallar ise, delil kurallarını ceza muhakemesi

³⁰⁰ Paul Marcus/Vicky Waye, “**Australia and the United States: Two Common Criminal Justice Systems Uncommonly at Odds**”, College of William & Mary Law School Faculty Publications,

kanunlarıyla düzenleyen Kıta Avrupası hukuk sistemlerine göre farklılık göstermektedir. ABD’de bütün delillere yönelik kurallar Delillere Dair Federal Kurallar (*Federal Rules of Evidence [FRE]*)³⁰¹ ile düzenlenmektedir. Böylece ceza muhakemesinde dijital delillere yönelik kurallar da bu düzenlemenin hükümlerine göre değerlendirilmektedirler.

Anglosakson hukuk sisteminin etkisinin yoğun olduğu ABD’de ceza yargılaması daha çok sözlülüğe dayanmakta olduğundan FRE’nin birçok kuralı da beyanlar ve yargılamadaki kişiler üzerine yoğunlaşmaktadır. Ancak belge ve belirtilere yönelik kurallar da az da olsa bulunmaktadır. Nitekim FRE’nin 1001. kuralı ile bunlar yazı (*writing*)³⁰², kayıt (*recording*)³⁰³ ve fotoğraf (*photograph*)³⁰⁴ olarak üçe ayrılmışlardır. FRE’nin 1002. kuralına göre başka bir federal kanunla aksi belirtilmemişse yazı, kayıt veya fotoğrafların içeriklerini ispat edebilmeleri için orijinal (*original*)³⁰⁵ olmaları gerekir. Ayrıca 1003. kurala göre orijinalin gerçekliğine dair problem varsa ya da koşullar ikinci kopyanın kabulünü haksız hale getirmiyorsa, ikinci kopya (*duplicate*)³⁰⁶ da delil olarak kabul edilebilir. Bu kural yargılamada dijital delillerin kullanımını kolaylaştırmaktadır.

FRE 1004. kuralına göre ise orijinalinin, kötü niyetli haller dışında, kaybolması veya yok olması, hiçbir adli yöntem ile elde edilememesi, taraflardan birinin kontrolünde olup getirilmemesi gibi hallerde delilin kabul edilebilirliği açısından eşyanın orijinal olması aranmayacaktır.

2004, s. 32, <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1245&context=facpubs>. (Erişim tarihi: 03.02.2015)

³⁰¹ FRE erişim için bkz. <http://www.uscourts.gov/uscourts/rules/rules-evidence.pdf>. (Erişim tarihi: 04.02.2015)

³⁰² FRE 1001/a’ya göre yazı; harf, kelime, sayı, veya bunlara eşdeğer olanların herhangi bir şekilde yazılı bulunduğu eşyayı ifade etmektedir.

³⁰³ FRE 1001/b’ye göre kayıt; harf, kelime, sayı, veya bunlara eşdeğer olanların herhangi bir şekilde kaydını içeren eşyayı ifade etmektedir.

³⁰⁴ FRE 1001/c’ye göre fotoğraf; fotoğraf şeklinde bulunan görüntü veya bunun eşdeğeri olan eşyanın herhangi bir biçimde depolanmış halini ifade etmektedir.

³⁰⁵ FRE 1001/d’ye göre bir yazının veya kaydın orijinali; yazının veya kaydın kendisini veya bunları yapan kişinin aynı şekilde iradesini yansıtan eşi veya kopyasıdır. Elektronik veriler açısından orijinal ise verinin içerdiği bilgiyi tam olarak yansıtan yazdırılmış çıktıyı –veya okunabilecek başka bir çıktı türünü– ifade etmektedir. Fotoğrafın orijinali ise fotoğrafın negatifi veya onun basılmış halini ifade etmektedir.

³⁰⁶ FRE 1001/e’ye göre ikinci kopya; mekanik, fotografik, kimyasal, elektronik veya eşdeğer bir yöntem ya da teknik aracılığıyla orijinalin aynısının üretilmesini ifade etmektedir.

Bunların dışında 901. kuralla, bir şeyin gerçekten delil olduğunun ispatı için, başka bir şey aracılığıyla sahip olduğu niteliğin doğrulanabilmesi gereği getirilmiştir.

Dijital delilleri ilgilendirebilecek delillere yönelik kuralları bu şekilde özetledikten sonra, ABD’de dijital delillerin nasıl elde edildiği konusuna geçilebilir.

ABD hukukunda dijital delillerin aranması genel arama hükümlerine tabidir. Bu hükümlerin ise ABD Anayasası’nın 4. Eki (*Constitution of the United States Amendment IV*)³⁰⁷ kapsamında şekillendirildiği görülmektedir. 4. Ek, kişileri makul olmayan (*unreasonable*) arama ve elkoymalara karşı korumaktadır. Arama kararı verirken kişilerin 4. Ek içerisindeki hakları ile kamu güvenliği gibi kamu yararı gözetilen durumların dengesinin kurulması gerekir. Bu da arama ve elkoyma için olası neden (*probable cause*) varlığını gerekli kılmaktadır. Bu genel kurallar dışında arama ve elkoymaya yönelik bütün diğer kurallar Federal Ceza Muhakemesi Kuralları (*Federal Rules of Criminal Procedure*)³⁰⁸ içerisinde 41. kural kapsamında düzenlenmektedir.

ABD’de iletişimin denetlenmesine ilişkin kurallar ise 1986 yılında çıkarılmış olan Elektronik İletişim Mahremiyet Kanunu (*Electronic Communications Privacy Act [ECPA]*)³⁰⁹ çerçevesinde çözülmektedir.

Dijital delillerin elde edilmesi söz konusu olduğunda ilgili tedbirin türüne göre, ya 4. Ek çerçevesindeki ya da ECPA içerisindeki kurallar yoluyla harekete geçilecektir. Bu noktada 4. Ek kapsamındaki düzenlemenin somut eşya ile soyut eşya arasındaki farklılığı karşılamaktan uzak olduğu, bu nedenle soyut niteliğe sahip dijital verilerin bu hükmün doğrudan uygulanması yoluyla aranamayacağı da tartışılmıştır³¹⁰. Ancak dijital delillere yönelik doğabilecek tüm bu sorunların çözümü zaman içerisinde bu konuda verilen mahkeme kararları içerisinde bulunmaktadır.

³⁰⁷ Amerikan Anayasası (*Constitution of the United States*) için bkz.

http://www.senate.gov/civics/constitution_item/constitution.htm. (Erişim tarihi: 04.02.2015)

³⁰⁸ Federal Rules of Criminal Procedure,

http://judiciary.house.gov/_cache/files/86a03f0f-cbfb-4624-8029-b2eec078d211/criminal2014.pdf.

(Erişim tarihi: 04.02.2015)

³⁰⁹ Electronic Communications Privacy Act,

<http://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf>.

(Erişim tarihi: 04.02.2015)

³¹⁰ Kaitlin R. O’Leary, “What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine”, *Suffolk University Law Review*, Vol. XLVI, 2013,

Bu konuda pek çok farklı mahkeme kararı bulunsa da, ABD hukukunda arama ve özellikle dijital verilerin elde edilmesine yönelik yapılan bilişim sistemlerindeki aramaların mahremiyet hakkı (*right to privacy*) ekseninde geliştiğini söylemek mümkündür³¹¹.

Hatta dijital deliller öncesinde başka teknolojiler için kabul edilmiş kurallar, dijital delillere yönelik uygulamalara da yansımıştır. Bu konuda örnek olarak Katz kararı³¹² ele alınacak olursa, karar içerisinde 4. Ek ile mekânlar değil, kişiler korunmaktadır denilmek suretiyle 4. Ek'in koruması soyut eşya açısından da tanımış olmaktadır. Burada telefon ile iletişim kuran kişinin, kurduğu iletişimin içeriğinin mahremiyetinin korunması konusunda beklentisi olduğu belirtilmiştir. Ancak kişinin söz konusu şey üzerinde makul bir mahremiyet beklentisi iradesi göstermesi gerekir. Üçüncü kişilere devredilen eşyada bu beklenti olamaz.

Bu noktada aramalara ilişkin olarak ortaya konulmuş olan kapalı konteynır prensibinden de bahsetmek gerekir. Bu prensibe göre her eşya, kapalı bir konteynır olarak değerlendirilmektedir. Kişilerin mahremiyet beklentisi de buna göre değerlendirilmektedir. Bilgisayarlarda yapılan aramalarla veri depolayan aygıtlar, konteynıra benzetilirken; konteynırın içerisinde bulunan görünmeyen içeriği oluşturan veriler açısından, özel hayatın gizliliğine ilişkin bir mahremiyet beklentisi olduğu belirtilmektedir. Bu durum, işbu veriler, parola ile korunsun da korunmasa da değişiklik göstermemektedir³¹³. Sonuç olarak bilgisayarlarda yapılacak aramalar açısından genel kural olarak, konteynır olarak nitelendirilen bilgisayarın içinin aranması haklı gösteren makul nedenin de bulunduğu bir arama kararı alınması yolu uygulanmaktadır³¹⁴.

s. 211, http://suffolkawreview.org/wp-content/uploads/2013/02/OLeary_Note_PDF_Web.pdf (Erişim tarihi: 05.02.2015); ayrıca konuyla ilgili bkz. Kerr, “**Digital Evidence...**”, ss. 285-286.

³¹¹ Daniel J. Solove/M. Neil Richards, “**Privacy’s Other Path: Recovering the Law of Confidentiality**”, The Georgetown Law Journal, Vol. 96, 2007, s. 128, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2078&context=faculty_publications. (Erişim tarihi: 05.02.2015)

³¹² United States v. Katz, 389 U.S. 347 (1967) kararına ilişkin değerlendirme özeti için bkz. <http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/wiretaps-cell-phone-surveillance/facts-case-summary.aspx>. (Erişim tarihi: 05.02.2015)

³¹³ Orin S. Kerr, “**The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?**”, Connecticut Law Review, Vol. 33, 2001, s. 532.

³¹⁴ Orin S. Kerr, “**Searches and Seizures in a Digital World**”, Harvard Law Review, Vol. 119, 2005, s. 537.

Yukarıda bahsedilen duruma istisna olarak arama kararı olmadan da elkoyma yoluyla delil elde edilmesi mümkündür. Rızanın varlığı, acil durumlar, makul sebebe dayanarak arabada yapılacak aramalar, havaalanı ve gümrük aramaları, kamuya açık alanlardaki aramalar, çıplak gözle görme doktrinine (*plain view doctrine*) istinaden yapılan aramalar ve terkedilmiş mülkiyette yapılacak aramalarda ise, genel kural olan arama kararı alınması gereği bulunmamaktadır³¹⁵. Bu konu dijital delillere ilişkin olarak ele alınırsa rızanın varlığı ve çıplak gözle görme doktrinine göre yapılan aramalar önem kazanmaktadır.

Rızanın varlığı için, rızayı verenle tedbirlere maruz kalan arasında hukuki bir ilişki mevcut olmalıdır³¹⁶. Bunun dışında kişi tarafından ifşa edilen bilgilerde de kişinin mahremiyet beklentisinin bulunmadığından yola çıkarak rıza var sayılır³¹⁷.

Çıplak gözle görme doktrini³¹⁸ ise Türkiye’deki tesadüfen elde edilen delil kavramına benzetilmektedir³¹⁹.

Arama ve elkoymalara ilişkin hükümler ele alındıktan sonra iletişimin denetlenmesi tedbirleri için kullanılan ECPA incelenecektir. ECPA üç bölümden oluşmaktadır. İlk bölüm iletişime hukuka aykırı müdahaleleri engelleyen Dinlemeler Kanunu (*Wiretap Act*), ikinci bölüm servis sağlayıcılarda depolanan bilgilerin ve kayıtların gizliliğini sağlayan İletişimin Depolanması Kanunu (*Stored Communications Act*) ve üçüncü bölüm teknik takibe ilişkin kurallardan

³¹⁵ Joanne Banker Hames/Yvonne Ekern, **Constitutional Law: Principles and Practice**, The West Legal Studies Series, New York: Thomson/Delmar Learning, 2004, s. 436.

³¹⁶ Burada hukuki ilişki teriminin karşılığı olarak hakkında tedbir uygulanan kişi ile rızayı veren kişi arasında aile bağı, işveren-işçi ilişkisi, sistem yöneticisi-kullanıcı gibi bir bağlantı bulunması koşulu aranmaktadır. Bilgi için bkz. Fred Galves/Christine Galves, “**Ensuring Admissibility of Electronic Forensic and Enhancing Its Probative Value At Trial**”, Criminal Justice Magazine, Vol: 19, Number 1, Spring 2004.

http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html. (Erişim tarihi: 05.02.2015)

³¹⁷ Bu durumda internet üzerinde ifşa edilen bilgilerde de mahremiyet beklentisi bulunmamaktadır. Bilgi için bkz. Jerry Wegman, “**Computer Forensic: Admissibility of Evidence in Criminal Cases**”, 2004.

<http://www.webpages.uidaho.edu/wegman/JerryWegmanPapers/Computer%20Forensics%20AA%202004.htm>. (Erişim tarihi: 05.02.2015)

³¹⁸ Kunter/Yenisey/Nuhoğlu (2010), **a.g.e.** , ss. 1431-1432 bölümünde bu husus şu şekilde örneklendirilmiştir: “*Mesela müsade edilen hız limitinin üzerine çıktığı için polis tarafından durdurulan bir aracın içerisinde bulundurulması suç teşkil eden bir eşya açık olarak gözüküyorsa, söz gelimi arka koltuğun üzerinde bir tabanca duruyorsa, polis bu eşyaya hâkim kararı olmadan el koyabilir (plain view doctrine).*”.

³¹⁹ Değirmenci, **a.g.e.** , s. 282.

oluşmaktadır. Bu düzenlemelerde yer alan en önemli husus, bilgilerin hassasiyetlerine göre farklı kategoriler altında gruplandırılmış olmasıdır. En hassas bilgilere³²⁰ ulaşmak isteniyorsa, makul sebep olarak adlandırılacak gerekçe de o ölçüde kuvvetli olmalıdır³²¹.

ABD’de dijital delillerin elde edilmesi konusundaki kurallara ilişkin olarak, 2009 yılında Adalet Bakanlığı Bilgisayar Suçları ve Fikri Sınai Haklar Dairesi Ceza Bölümü (*Computer Crime and Intellectual Property Section Criminal Division*) tarafından yayınlanan Bilgisayarların Aranması, Bilgisayarlara Elkoyulması ve Ceza Soruşturamalarında Elektronik Delil Elde Edilmesi (*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*) adlı bir rehber bulunmaktadır³²². Yine 2004 yılında adli bilişim işlemleri bakımından yapılmış bir rehber daha bulunmaktadır³²³.

ABD’de dijital delillerin güvenilirliği genel olarak iki farklı açıdan değerlendirilmektedir. Bunlardan ilki delilin kendi güvenilirliği iken, diğeri kolluğun delili elde ettiği ve muhafaza altına aldığı ilk andan itibaren yapılan işlemlerin güvenilirliğidir³²⁴. Dijital deliller bilimsel deliller kategorisi altında sınıflandırıldıkları için, bu delillerin her iki açıdan da güvenilirliği bilimsel testler aracılığıyla yapılabilmektedir³²⁵. Bu testlerle delilin bütünlüğü ve sağlamlığı kesin bir şekilde ispat edilmektedir.

³²⁰ En hassas bilgi olarak adlandırılabilirken, en sıradan sayılabilecek bilgiler ise abonelerin isimleri ve faturalarını ödeme şekilleridir.

³²¹ Wegman, **a.g.e.**

³²² *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>. (Erişim tarihi: 06.02.2015)

³²³ *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>. (Erişim tarihi: 06.02.2015)

³²⁴ Karagülmez, **a.g.e.**, s. 530.

³²⁵ Bu husus FRE 702. kuralına dayanmaktadır. Buna göre bir delil değerlendirilirken bilimsel anlamda teknik veya uzmanlık bilgisi gerektiriyorsa, o delilin doğruluğu, özellikleri, niteliği bir uzmanca bilimsel yöntemlerle test edilecektir. ABD’de dijital delillerle ilgili olarak yapılan Daubert testi, Frye testi vb. bilimsel testler bulunmaktadır. Örneğin, dijital delillerin güvenilirliğini bilimsel olarak ispata yarayan Daubert testi ilk olarak ABD’de Yüksek Mahkemenin (*Supreme Court*) 1993 yılında Daubert vs. Merrel Dow Pharmaceuticals davasında ortaya çıkmıştır. Bu konuda daha detaylı bilgi için bkz. Karagülmez, **a.g.e.**, s. 530 vd.

C. Avustralya

Avustralya’da ceza muhakemesi sistemi federe devlet ve federal devlet düzenlemeleri göz önüne alındığında iki basamaklıdır. Federe devletler kendi içerilerinde düzenlemelerini yaparlarken, federal devletin de sahip olduğu genel düzenlemeler mevcuttur³²⁶.

Bu düzenlemelerden doğrudan delillere yönelik olan 1995 tarihli Delil Kanunu (*Evidence Act 1995*)³²⁷ mevcuttur. Bu kanunda dijital delillerin kullanımını kolaylaştırmak için koyulmuş bazı maddeler mevcuttur. Örneğin, 51. madde aracılığıyla dijital deliller açısından problem çıkarabilecek bir kural olan ispatta orijinal belge zorunluluğu kaldırılmış, 71. madde aracılığıyla elektronik iletişim kayıtlarının “*hearsay*” kuralına istisna oluşturduğu kabul edilmiştir.

Bu düzenlemelerden bir diğeri olan 1914 tarihli Milletler Topluluğu Suçlar Kanunu (*The Commonwealth’s Crimes Act 1914 [CCA]*)³²⁸ ise, ceza muhakemesine yönelik genel düzenlemelerin bulunduğu kanundur. Dijital delil elde etmede kullanılan genel düzenlemeler, bu Kanun içerisinde bulunmaktadır. Bunun yanı sıra bazı özel kanunlarda da dijital delillere ilişkin hükümler bulunmaktadır³²⁹.

Bu kanunu incelerken ilk olarak dikkat çeken husus kanunun 3 maddesinde yer alan veri (*data*)³³⁰ ve veri depolama aygıtı (*data storage device*)³³¹ tanımlarıdır. Yine kanunun 3C maddesinde “bilgisayarda tutulan veri” (*data held in a computer*) nin ne olduğuna ilişkin bir tanımlama yapılmıştır³³².

³²⁶ Marcus/Waye, **a.g.e.** , s. 29.

³²⁷ Evidence Act 1995, http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/. (Erişim tarihi: 11.02.2015)

³²⁸ The Commonwealth’s Crimes Act 1914, http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/. (Erişim tarihi: 11.02.2015)

³²⁹ Detaylı bilgi için bkz. Osman Gazi Ünal, **Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara 2011, s. 73.

³³⁰ Veri, herhangi bir biçimde bulunan bilgiyi, bir programı veya program parçasını ifade etmektedir.

³³¹ Veri depolama aygıtı, bilgisayarların işleyebileceği verileri içeren ya da içermek için tasarlanmış olan şeyi ifade etmektedir.

³³² Tanıma göre bilgisayarda tutulan veri, (a) bilgisayara bağlı olduğu süre boyunca çıkartılabilir veri depolama aygıtlarında bulunan veri ile (b) bilgisayarın parçası olan bir bilgisayar ağındaki veri depolama aygıtında bulunan veriyi içerir.

Aramaya ilişkin genel düzenlemeye gelirse; CCA 3E maddesine göre, bir mülkte (*premises*)³³³ delil olabilecek materyalin (*evidential material*)³³⁴ var olduğuna veya 72 saat içerisinde bu tip materyalin var olabileceğine ilişkin olarak makul sebepler (*reasonable grounds*) içeren bir şüphe mevcut olursa, yetkili kişiler (*issuing officer*)³³⁵ tarafından ilgili yerde delil elde etmeye yönelik bir arama kararı verilebilmektedir. Delil olabilecek materyalin kapsamı nedeniyle bilgisayarlar ve veri depolama aygıtları da arama kararı kapsamında aranabilecektir. Arama kararı talep edilirken, soruşturulmakta olan suç, olay yeri adresi, delil ile bulunması beklenen delillerin çeşitleri, aramayı yapacak sorumlu polis memurunun ismi, arama kararının ne zaman uygulanacağı ve süresinin ne zaman dolacağı da yazılır (CCA 3E/5).

Yine CCA 3K maddesinde arama konusu eşyayı incelemek amacıyla, aranılan yere gerekli aletlerin getirilmesinden bahsedilmiştir. CCA 3L maddesinde ise bu husus verilere erişimin sağlanabilmesi açısından elektronik aygıtlar için düzenlenmektedir. Dolayısıyla CCA 3L maddesi ile 3K maddesi bir arada değerlendirildiğinde, 3L maddesinin 3K maddesine göre, özel hüküm olduğu sonucuna ulaşılabilecektir. Böylece 3L maddesinin eksik olduğu kısımlar 3K maddesi aracılığıyla doldurulacaktır.

3L maddesi ile ilgili verilerin delil olabilecek materyal olabileceğine yönelik şüphe halinde, polislerin bilgisayardaki ve veri depolama aygıtlarındaki verilere erişme ve kopyalama yetkisi bulunmaktadır. Bu yetki kullanılırken mülke getirilen elektronik aygıtların yanı sıra mülkün sahibinin yazılı izni ile mülkte bulunan başka bir elektronik aygıt ile de yapılabilir (CCA 3L/1A).

Mülke getirilen elektronik aygıtların kullanılması ile delil olabilecek materyale erişim sağlandıysa, erişim sağlanan materyale elkonulabilir (CCA 3L/2-a). Ancak bu elkoymanın gerçekleşebilmesi için erişim sağlanan materyalin CCA 3L/1A

³³³ Milletler Topluluğu Suçlar Kanunu'nun 3C maddesine göre mülk, bir mekânı veya taşıtı (*conveyance*) belirtebilir.

³³⁴ Milletler Topluluğu Suçlar Kanunu'nun 3C maddesine göre, delil olabilecek materyal içerisine elektronik yapıdaki eşya da dâhildir.

³³⁵ 3C maddesinde "arama kararını düzenlemeye yetkili kişiler" deyiminden (*issuing officer*) bir hâkim (*magistrate*) veya sulh hâkimi (*justice of peace*) veyahut da Avustralya'nın başkent eyaleti (*Capital Territory*) ve diğer eyaletlerinin adli mercilerinde görev yapan tutuklama için arama, bina ve eklentileri için arama ve diğer soruşturmalar için arama kararlarını vermeye yetkili kişiler anlaşılır.

kapsamında kopyalanmasının pratik olmaması ya da delil olabilecek materyalin CCA 3L/2-b hükmünde belirtilen şekilde belgeye dönüştürülememesi gerekir.

Delil olabilecek materyalin orijinaline elkoyulması halinde, mülk sahibinin veya olay yerinde hali hazırda mülk sahibini temsil eden herhangi bir kimsenin talebi üzerine; elkoyulan belgelerin, görüntülerin, bilgisayar dosyalarının ya da veri depolama aygıtının içerisindeki bilgilerin bir kopyasının talep eden kişiye, kopyalama işleminin gerçekleşebileceği en kısa süre içerisinde verilmesi gerekir (CCA 3N/1). Ancak zaten kopyaya elkoyulan haller ile ilgili materyalin içeriğinin suç oluşturduğu haller bu duruma istisna oluşturacaktır (CCA 3N/2).

Delil olabilecek materyale erişimin mülkteki bir elektronik aygıtla ve uzman yardımıyla erişebilmenin mümkün olacağına, aksi halde ilgili materyalin zarar görebileceğine dair makul sebepler varsa mülkteki bu elektronik aygıtın korunması için gerekli önlemleri alacaktır (CCA 3L/4). Ancak bu koruma en fazla 24 saat sürebilir (CCA 3L/6). Bu 24 saatte materyalin incelenemeyeceğine ilişkin makul sebepler varsa, bu sürenin uzatılması için arama kararını düzenlemeye yetkili kişilere başvuru yapmak zorundadırlar (CCA 3L/7).

CCA 3LA maddesi bilgisayar veya bilgisayar sistemlerinden elde edilecek delillere erişimi sağlayabilecek kişilerin yardımına ilişkin düzenlenmiş bir maddedir. Mahkeme bu hükmeye dayanarak, makuliyet ve gereklilik çerçevesinde, ilgili verilere erişimi sağlayabilecek kişilere yardımda bulunma yükümü yükleyebilmektedir. CCA 3LB maddesi ise, erişimi istenen verilerin aranılan yer dışında, farklı bir yerde bulunması koşullarını düzenlemiştir.

Son olarak bahsedilecek CCA 3M maddesi ise adli incelemeler sırasında zarar verilen elektronik aygıtların zararlarının tazmini konusunu içermektedir.

İletişimin denetlenmesi tedbiri açısından ise 1979 yılında çıkartılmış ve pekçok değişikliğe uğramış Telekomünikasyon (Denetleme ve Erişim) Kanunu (*Telecommunications {Interception and Access} Act [TIA]*)³³⁶ tarafından düzenlenmektedir. Bu konuda genel kural iletişimin denetlenmesinin yasak olmasıdır

³³⁶ Telecommunications (Interception and Access) Act 1979, <http://www.comlaw.gov.au/Details/C2014C00786>. (Erişim tarihi: 11.02.2015)

(TIA 7). Dolayısıyla iletişimin denetlenmesi tedbiri sadece TIA içerisindeki kurallara göre uygulanabilecektir. Nitekim bu kurallar aracılığıyla, genel kurala getirilen istisnalar belirlenmiş olmaktadır.

D. Belçika

Belçika ceza muhakemesi hukukunda her tür delilin mahkemeye sunulabileceği ve dijital delillerin de delil serbestisi içerisinde bir delil türü olarak kabul edilebileceği ortaya konmuştur. Hatta Alman ceza muhakemesi açısından da bahsedildiği üzere, Belçika ceza muhakemesi sisteminde de bir delilin sıra dışılığının, hâkimin karar vermesine sıradan bir delile göre daha çok yardımcı olacağı düşünülmektedir³³⁷.

Dijital delillerin elde edilmesine yarayan bilişim koruma tedbirleri ise Belçika Ceza Usul Kanunu (*Code d'instruction criminelle [CDC]*)³³⁸ içerisinde yer almaktadır. Belçika hukukunda bu konuya ilişkin olarak depolanmış verilerin hızlı şekilde korunması, verilere elkoyma, bilgisayar ve ağ bağlantılarını arama ile yardım etme yükümlülüklerine ilişkin düzenlemeler bulunmaktadır.

Bilgisayar ve ağ bağlantılarını arama kararına yalnızca sorgu hâkimince karar verilebilir (CDC 88ter/1). Bilgisayar sistemleri veya parçalarına yönelik verilmiş arama kararının içeriği, maddi gerçeğe ulaşma konusunda gerekli olma ve verilerin yok olma riskinin bulunması hallerinde genişletilerek, başka yerde bulunan bilgisayar sistemleri veya parçalarına da sirayet edebilir. Ancak bu genişletme sadece tedbir kararının verilebileceği yetki alanı kadar genişletilebilir (CDC 88ter/2). Bu arama sonucunda elde edilen veriler, verilere elkoyulması hükümlerine göre (Article 39bis) işleme tabi olacaklardır. Yetki alanı dışında bulunan, örneğin yurtdışında bulunan, veriler açısından yalnızca kopyalama işlemi uygulanabilecek, bu verilerin kayıtlı bulunduğu sistemlere yönelik herhangi bir işlemde bulunulmayacaktır. Ayrıca bu gibi durumlarda yapılan işlemlerin, diğer devlete bu konuda bilgi vermek üzere, Belçika Adalet Bakanlığı'na bildirilmesi gereklidir (CDC 88ter/3).

³³⁷ RAND Europe & Lawford, s. 38.

³³⁸ Belçika Ceza Usul Kanunu'nun konuyla ilgili maddelerinin ingilizce çevirisi için Johan Vandendriessche, "**Belgian Cybercrime Provisions**", Digital Evidence and Electronic Signature Law Review, Vol. 9, 2012, ss. 173-177.

Verilere elkoyma tedbirinde savcı, bir sabit diskin başka bir sabit diske kopyalanarak adli inceleme laboratuvarına konmak üzere saklanmasına karar verebilir (CDC 39bis/2). Gerekli görülen durumlarda ilgili verilere veya bunların kopyalarına ulaşmanın engellenmesi veya silinmesi kararına da başvurabilir (CDC 39bis/3). Ancak tüm bu durumlarda savcının ilgili sistemin yöneticisine karşı bir bildirim yükümü oluşmaktadır (CDC 39bis/5). Ayrıca delilin sağlamlığını ve güvenilirliğini sağlayacak olan teknik önlemlerin alınması da savcının yükümlülüğündedir (CDC 39bis/6).

Sorgu hâkimi veri toplamak istediği bilişim sisteminin nasıl çalıştığı ya da bu sisteme erişimin nasıl sağlandığı hakkında ilgili konuda bilgi sahibi olan kişilerin yardımına başvurabilir (CDC 88quater/1). Örneğin bir şifre ya da güvenlik sistemi konusunda ilgili ağ yöneticisinden bilgi isteyebilir. Ancak bilgi alınacak kişiler şüpheli veya kanunun 156. maddesinde sayılan şüphelinin yakınları olamaz (CDC 88quater/2). Telekomünikasyon iletişimi içerisindeki verilere erişim de benzer şekilde 90quater maddesi içerisinde düzenlenmiştir.

Bu tedbirlerden haberi olan kişilerin soruşturmanın gizliliğine riayet etmeleri istenir (CDC 88quater/4, 90quater/4). Yardımın reddi ya da soruşturma gizliliğinin ihlali durumunda bu kişilere Belçika Ceza Kanunu'nun 458. maddesine göre cezai yaptırımlar uygulanmaktadır.

Ayrıca tüm bu tedbirler sonucunda bilgisayar sistemine ya da verilere verilecek zararlardan Belçika Devleti sorumludur (CDC 88quater/5).

E. Birleşik Krallık

Anglosakson hukuk sisteminin uygulandığı Birleşik Krallık'ta delillere yönelik kurallar 1984 tarihli Polis ve Suç Delilleri Kanunu (*Police and Criminal Evidence Act [PACE]*)³³⁹, 1990 tarihli Bilgisayar Kullanımının Suistimali Kanunu

³³⁹ Police and Criminal Evidence Act, <http://www.legislation.gov.uk/ukpga/1984/60/contents>. (Erişim tarihi: 13.02.2015)

(*Computer Misuse Act [CMA]*)³⁴⁰ ve Soruşturma Yetkilerini Düzenleyen Kanun (*Regulation of Investigatory Powers Act [RIPA]*)³⁴¹ tarafından düzenlenmiştir. Bunun sebebi ise Birleşik Krallık'ta bir ceza muhakemesi kanununun bulunmamasından ileri gelmektedir.

Genel arama ve elkoyma tedbirine ilişkin kurallar PACE içerisinde yer almaktadır. Bu kanunun 8. maddesi ile genel arama hükümleri düzenlenirken, 19. maddesi ile genel elkoyma hükümleri düzenlenmektedir.

Dijital delillerin temelini oluşturan bilgisayarlarla ilgili önemli bir düzenleme olan CMA içerisinde ilginç bir şekilde bilgisayar, bilgisayar programı ve veri gibi kavramların tanımı yapılmamıştır. Buna neden olarak ise, ilgili kavramların tanımlarının yapılması durumunda, yapılan tanımların yeni gelişmeler karşısında eski kalacakları için kanunun uygulanmasını kısıtlayacakları belirtilmektedir³⁴². Bu Kanun ilk 3 maddesinde bilgisayara ilişkin suçları içermekle birlikte, bu suçlara yönelik ceza muhakemesi işlemleri açısından da hüküm barındırmaktadır. Bahsedilen hüküm kanun içerisinde sayılan bilgisayara ilişkin suçlarla ilgili aramalar başlığı altında 14. maddede düzenlenmekteydi. Ancak bu madde 2006 tarihli Polis ve Adalet Kanunu (*Police and Justice Act*)³⁴³, nun 14. listesi (*Schedule 14*) ile kaldırılmıştır.

2000 yılında iletişimin denetlenmesi ve teknik takip gibi konuları düzenleyen RIPA yürürlüğe girmiştir. Kanun içerisinde telekomünikasyon sistemi, telekomünikasyon servisi ve trafik verisi gibi kavramların tanımı 2. madde içerisinde yapılmış bulunmaktadır. Bunun yanı sıra kanundaki genel düzenlemeler bir kenara bırakılarak birkaç ilginç düzenlemeden bahsetmek gerekirse, 3. maddede bazı haller açısından herhangi bir yargı kararı olmadan iletişimin denetlenmesi olanağı verilmektedir. Yine 49. madde vd. hükümleri ile şifre ve diğer yöntemlerle korunan elektronik verilerin araştırılmasına ilişkin hükümler de dikkat çekmektedir.

³⁴⁰ Computer Misuse Act, <http://www.legislation.gov.uk/ukpga/1990/18/contents>. (Erişim tarihi: 13.02.2015)

³⁴¹ Regulation of Investigatory Powers Act, <http://www.legislation.gov.uk/ukpga/2000/23/contents>. (Erişim tarihi: 13.02.2015)

³⁴² Karagülmez, **a.g.e.**, s. 117.

³⁴³ Police and Justice Act, <http://www.legislation.gov.uk/ukpga/2006/48/contents>. (Erişim tarihi: 13.02.2015)

Birleşik Krallık'ta 2006 yılına kadar, ağ bağlantısı trafiğinin gerçek zamanlı olarak izlenmesi ve incelenmesi ile elkonulmuş olan depolama amaçlı kullanılan elektronik aygıtların incelenmesi gibi iki ana dal üzerinde çalışan İleri Teknoloji Suçlar Birimi (*National Hi-Tech Crime Unit [NHTCU]*), 2013 yılına kadar içine katıldığı Ciddi Organize Suçlar Ajansı (*Serious Organised Crime Agency [SOCA]*) aracılığıyla uygulamalarına devam etmiştir. Şu anda ise bu uygulamalar Ulusal Suç Ajansı (*National Crime Agency[NCA]*) tarafından yapılmaktadır.

Dijital deliller Birleşik Krallık ceza yargı sisteminde kabul edilmektedirler. Üstelik daha önce de pek çok davada kullanılmışlardır. Delillere ilişkin temel kurallar ile dijital deliller arasında pek bir farklılık bulunmamakla birlikte; dijital delil elde edilmesi açısından, İngiliz Polis Teşkilatı'nın elinde (*Association of Chief Police Officers [ACPO]*) Bilgisayar Temelli Deliller için Uygulama Rehberi (*Good Practice Guide for Computer Based Evidence*)³⁴⁴ gibi yol gösterici bir rehber mevcuttur. Mahkemelerde olaylar incelenirken genel olarak bu rehberdeki ilkeler yoluyla dijital delillerin sağlamlığının ve güvenilirliğinin denetimi yapılmaktadır. Bu nedenle dijital delillerin kabul edilebilirliği açısından rehberde bulunan ilkelerinin uygulanması önemlidir.

Bu ilkeleri bir değerlendirme içerisine sokacak olursak; öncelikle iddia makamı, mahkemeye, delilin polis tarafından elde edildiği ana göre ne eksik ne de fazla durumda olmadığını yani aynı durumda olduğunu ispat etmelidir³⁴⁵. Soruşturmada yer alanların veriler üzerinde herhangi bir değişiklik olmamasına dikkat etmeleri gerektiği belirtilmiş, aksi halde mahkeme tarafından bu verilerin sağlamlığına güvenilemeyeceği belirtilmiştir³⁴⁶. Bu yüzden ilgili kişilerin konuya yönelik araştırmalarını orijinal veriler üzerinde yapmamaları, mümkünse aldıkları kopyalar üzerinde bu tür çalışmaları sürdürmeleri gerektiğine dikkat çekilmiştir³⁴⁷. Bu nedenle orijinal veriler üzerinde inceleme gerektiren hallerin yalnızca orijinal veriye yaptığı müdahaleleri ve bu müdahalelerin olaya etkisini ispatlayabilecek,

³⁴⁴ ACPO Good Practice Guide for Computer Based Evidence, <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf>. (Erişim tarihi: 13.11.2014)

³⁴⁵ ACPO Good Practice Guide for Computer Based Evidence 2.2.2.

³⁴⁶ ACPO Good Practice Guide for Computer Based Evidence 2.1.1.

³⁴⁷ ACPO Good Practice Guide for Computer Based Evidence 2.1.3.

alanında uzman olan kişiler tarafından yapılması istenmektedir³⁴⁸. Yani veriden ulaşılabilecek sonuçlara yönelik nedensellik bağının zedelenmesinden kaçınılmalı ve veriyi inceleyen üçüncü kişilerce de bu sonuç aynı şekilde ortaya konulabilmelidir³⁴⁹. Tüm bu ilkelere bağlılık açısından sorumluluk, soruşturmadan sorumlu olan kişinin sorumlulukları içerisindedir³⁵⁰.

Son olarak, Birleşik Krallık'ta adli bilişim incelemelerini yapabilecek pek çok kaliteli uzman yetiştirilmektedir. Bazı üniversitelerde sadece bu alana yönelik özel dersler verilmektedir. Ayrıca kolluk güçlerinin, adli bilişim konusunda uzmana başvururken gerek çağın gerekleri hakkında bilgi sahibi ve gelişim göstermekte olan adli bilişim uzmanı piyasasından, gerekse müthiş bir ulusal gücü elinde bulunduran istihbarat birimlerinden yardım istemesi mümkündür³⁵¹.

F. Çin

Bilişim suçları ile mücadele konusunda gösterilen uluslararası çabaya yeterli katkı vermeyen Çin, bu konuda herhangi bir anlaşma imzalamaktan da kaçınmakta olan bir ülkedir. Bu sebeple iç hukuk düzenlemeleri de çağın gerisinde kalmış bir görüntüdedir. Her ne kadar bu konudaki gelişmelere yavaş yavaş ayak uydurulsa da dijital delillerin elde edilmesi ve kabul edilebilirliğine ilişkin özel maddeler, Mart 2012'e kadar ceza muhakemesi sisteminde yer almamaktaydı.

Ancak Mart 2012'te yeni kabul edilen Çin Halk Cumhuriyeti Ceza Muhakemesi Kanunu (《中华人民共和国刑事诉讼法》)³⁵² ile ceza yargılamasında her geçen gün daha da kullanılır hale gelen dijital delillere yönelik eksikliklerin giderilmeye çalışıldığı görülmektedir. Kanunun 48. maddesi yoluyla, elektronik veriler de ispata uygun delil çeşitleri içerisine sokulmuştur. Yine 52. maddede, soruşturma

³⁴⁸ ACPO Good Practice Guide for Computer Based Evidence 2.1.2.

³⁴⁹ ACPO Good Practice Guide for Computer Based Evidence 2.1.3.

³⁵⁰ ACPO Good Practice Guide for Computer Based Evidence 2.1.4.

³⁵¹ RAND Europe & Lawford, ss. 268-269.

³⁵² Kanunun İngilizce çevirisi için bkz. <http://www.cecc.gov/resources/legal-provisions/criminal-procedure-law-of-the-peoples-republic-of-china>; Çince'si için bkz. http://www.gov.cn/flfg/2012-03/17/content_2094354.htm. (Erişim tarihi: 20.02.2015)

aşamasında kolluk tarafından elde edilen elektronik verilerin kovuşturma aşamasında delil olarak kullanılabileceği hüküm altına alınmıştır³⁵³.

Buna rağmen 1 Ocak 2013 tarihinde yeni kanunda yapılan değişikliklere kadar, dijital delillerin mahkemeye doğrudan sunulması mümkün olmamakta, bu deliller açısından öncelikle geçmeleri gereken bir idari prosedür öngörülmekteydi. Ancak şu anda yanlış bilgilerin analizinin yapılmadığı veya veri bütünlüğünün bozulmadığı hallerde, gerekli sertifika ve yetkilere sahip uzmanlar tarafından verilecek raporlar doğrudan mahkemeye sunulabilmektedir³⁵⁴.

Çin’de dijital delillerin yargılamada kabul edilmesi hususu Avrupa’daki gelişmelere göre daha farklı şekilde gelişim göstermiştir. Dijital delillerin kabul edilebilirliği açısından önemli olan adli bilişim evrelerinde, Batı dünyasının örnekleri ile Çin arasında büyük bir farklılık olmasa da adli bilişim modeli bakımından bazı farklılıklar söz konusudur. Burada adli bilişim incelemesi, birbirinden farklı ama aynı zamanda birbirine bağlı olan delil aşaması, başvuru aşaması, teknik aşama ve temel aşama olarak adlandırılan dört aşamadan oluşan bir sistem olarak işlemektedir³⁵⁵.

G. Endonezya

Endonezya’da ceza muhakemesi işlemlerine ilişkin kurallar genel bir ceza usul kanunu (*Kitab Undang-Undang Hukum Acara Pidana [KUHP]*)³⁵⁶ aracılığıyla yapılmaktadır. KUHP 184. maddesinde tanık beyanı, bilirkişi beyanı, belge, belirti, şüpheli/sanık beyanı olmak üzere beş çeşit delil sayılmıştır. Bu kanun içerisinde dijital delillerden bahseden bir düzenleme mevcut değildir. Bu nedenle ceza

³⁵³ Frank Law/K. P. Chow/Y. H. Mai, “Understanding Computer Forensics Requirements in China via the “Panda Burning Incense” Virus Case”, *Understanding Computer Forensics Requirements...*, 2014, s. 54.

³⁵⁴ Law/Chow/Mai, *a.g.e.*, ss. 54-55.

³⁵⁵ Bu model hakkında detaylı bilgi için bkz. Law/Chow/Mai, *a.g.e.*, s. 55 vd.

³⁵⁶ Kitab Undang-Undang Hukum Acara Pidana, http://www.kontras.org/uu_ri_ham/Kitab%20Undang-undang%20Hukum%20Acara%20Pidana_KUHAP.pdf (Erişim tarihi: 21.02.2015); kanunun ilgili maddelerinin İngilizce çevirisi (Indonesian Law No. 8 of 1981 concerning General Criminal Proceedings) için bkz. Edmon Makarim, “Electronic Evidence and Electronic Signatures in Indonesia: The Probative Value of Digital Evidence”, *Digital Evidence and Electronic Signature Law Review*, Vol. 10, 2013.

muhakemesi işlemlerinde dijital delillerin kullanılıp kullanılmayacağına yönelik tartışmalar mevcuttur³⁵⁷.

Ancak Elektronik Bilgi ve İşlemler Kanunu (*Undang-Undang Informasi Dan Transaksi*)³⁵⁸, nun 5. maddesinin bu konudaki tartışmalara son noktayı koyduğu düşünülmektedir. Nitekim maddenin 1. fıkrasına göre; elektronik bilgi, belge veya bunların yazılı çıktılarının delil olarak kullanılması mümkün olacaktır. 2. fıkra ise 1. fıkra hükmünün Endonezya'daki geçerli usul kanunlarındaki delillere ek niteliği taşıdığı belirtilmiştir. İşbu delillerin hukuka uygunluğu 3. fıkra da öngörüldüğü üzere Elektronik Bilgi ve İşlemler Kanunu hükümlerine göre belirlenecektir. Ancak 4. fıkraya göre, ispat açısından belirli belgeleri öngören kanuni istisna halleri bu durumun dışında kalmaktadır.

Dijital delillerin yargılamada hâkim tarafından kabul edilip edilmeyeceği ise elde edildiği elektronik sistemin ve mahkeme önüne getirilene kadar geçtiği güvenlik sisteminin güvenilirliği üzerinden değerlendirilmektedir. Bu hususlar dijital delillerin sağlamlığı ve bütünlüğü açısından önemli olmaktadır. Bir yandan da bunlara ek olarak, adli bilişim incelemelerini yapan uzmanların ilgili devlet kurumları ya da noterler tarafından onaylanmış sertifika ve akreditasyonlara sahip olmaları gereği aranmaktadır³⁵⁹.

H. Fransa

Diğer pek çok kıta Avrupası ülkesi gibi Fransa'da da delil serbestisi sistemi geçerlidir. Ceza yargılamasında suçluluk her tür delil ile ispatlanabilir. Dijital deliller de bu delil sisteminin bir parçasıdır. Ancak hâkim kararını verirken delilleri vicdani kanaatine göre değerlendirecektir (CPP 427). Dijital delillere ile ilgili olarak yapılan düzenlemeler açısından Fransa Ceza Usul Kanunu (*Code de Procédure Pénale*[CPP]) incelemeye değerdir.

³⁵⁷ Makarim, **a.g.e.**, ss. 139-140.

³⁵⁸ Undang-Undang Informasi Dan Transaksi, <http://www.bpn.go.id/Portals/0/ppid/Undang%20undang%20nomor%2011%20Tahun%202008%20Tentang%20Informasi%20dan%20Transaksi%20Elektronik.pdf> (Erişim tarihi: 21.02.2015); kanunun ilgili maddelerinin İngilizce çevirisi (*Electronic Information and Transaction Law*) için bkz. Makarim, **a.g.e.**, s. 138.

³⁵⁹ Makarim, **a.g.e.**, s. 143.

Fransa’da suç oluşturabilecek bir olay ihbar veya keşif yoluyla haber alındığında, olaya bir sorgu hâkimi (*juge d’instruction*) atanır. Bu hâkim soruşturma işlemlerini gerektiğinde adli kolluk görevi olan kurumlardan yardım da alarak sürdürür (CPP 49).

Arama kararı gibi koruma tedbirlerinde yetki sadece ilgili sorgu hâkimindedir (CPP 92). Fransa’da aramayı düzenleyen CPP 94, 2004 yılında değişikliğe uğrayarak, aramalarda maddi gerçeğe ulaşılmasında yardımcı olacak eşyanın yanı sıra elektronik verileri (*données électroniques*) de kapsayacak şekilde genişletilmiştir. Böylece bilgisayar sistemleri ve ağlarında arama yapmanın önü açılmış oldu.

CPP 97 ise bu önlemin nasıl gerçekleştirileceğine dair esaslar ortaya konmuştur. İlgili maddeye göre arama sonucunda elkonulan tüm eşya, belgeler ve verilerin listesi çıkarılacak ve bunlar mühürlenecektir (CPP 97/2). Veriler ya içerisinde bulunduğu fiziki aygıtı (örnek: sabit disk) elkoyma (CPP 57-1) ya da kopyalama yoluyla elde edileceklerdir. Kopyalama yolu tercih edildiğinde orijinal veriler hukuka aykırı ya da tehlikeli bir içeriğe sahip olmaları halinde silinebilirler (CPP 97/3).

Ayrıca sorgu hâkimi ya da bu konuda görevlendirdiği adli kolluk, herhangi bir kişi ya da topluluğa ellerinde soruşturmayı ilgilendiren belgeler bulundurdukları hallerde, bu belgeler veriler aracılığıyla oluşturulmuş olsa da, istem halinde bu belgeleri teslim etme yükümü altındadırlar (CPP 99-3).

Bunların yanı sıra Fransız hukukunda da telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri de mevcuttur. Sorgu hâkimi telekomünikasyon yoluyla yapılan iletişimin denetlenmesini, kaydedilmesini, telekomünikasyon verilerinin sicilinin teslimini emredebilir. Ancak bu emrin verilebilmesi için suçun en az iki yıl hapis cezasını gerektirmesi gerekir (CPP 100/1). Emri içeren yazılı kararda denetlenecek bağlantının kimliği, elde edilecek bilginin soruşturma açısından önemi ve denetiminin süresinin belirtilmesi gereklidir (CPP 100/2). Bu karar en fazla dört aylık bir süre için alınabilir ve sürenin bitiminde en fazla bir o kadar daha uzatılabilir (CPP 100-2).

Sorgu hâkimi ya da bu konuda görevlendirdiği adli kolluğa telekomünikasyonun denetlenmesi tedbirini uygulayabilmeleri için telekomünikasyonun başında bulunan Bakanlığın yetkilendirdiği servislerden, ağ bağlantılar operatörlerinden veya yetkili telekomünikasyon servis satıcılarından herhangi bir kalifiye çalışanı tedbirde kullanılacak aygıtın kurulması için görevlendirebilir (CPP 100-3).

Sorgu hâkimi ya da bu konuda görevlendirdiği adli kolluk uygulanan denetim işlemi ile ilgili resmi bir rapor hazırlayacaklardır. Bu raporlar mühürlenerek saklanacaklardır (CPP 100-4).

Sorgu hâkimi ya da bu konuda görevlendirdiği adli kolluk onları maddi gerçeğe ulaştırabilecek bulguların resmi kayıt olarak suretini çıkarırlar. Bu kayıt dosyaya eklenir (CPP 100-5/1). Suret çıkarma işlemi verileri çevirmede görevlendirilmiş kişinin yardımıyla yapılacaktır (CPP 100-5/2). Hükümsüz olmaları nedeniyle, bu bulgulardan şüphelinin savunma hakkı kapsamında müdafî ile ilgili olanların sureti çıkarılmayacaktır (CPP 100-5/3).

Bu yöntemle elde edilen bilgiler tedbirin süresinin dolumu ile birlikte savcı talebiyle yok edileceklerdir. Yok etmeye ilişkin de resmi kayıt yapılacaktır (CPP 100-6).

Meclis üyesi ya da senatörlerin telefon ile iletişimi, ait oldukları meclis ya da senatoya bu konuda gerekli bildirim yapılmadıysa denetlenemez (CPP 100-7/1). Yine avukatların işyerleri ve evlerindeki telefon iletişimi, Barolar Birliği Başkanı'na bu konuda bilgi vermeden gerçekleşemez (CPP 100-7/2). Yine savcı ve hâkimlerin işyerleri ve evlerindeki telefon iletişimi, ilgili bölgenin mahkeme başkanı ya da başsavcısının bilgisi haricinde denetlenemez (CPP 100-7/3). Eğer bu madde içerisinde sayılan ilgili makamlara bilgi verilmeden böyle bir tedbir uygulanmışsa, tedbir aracılığıyla elde edilen bulgular hükümsüz olur (CPP 100-7/4).

Soruşturma sırasında ilgili makamın teknik bir konuda soruşturmaya yardım etmesi açısından uzman görevlendirilmesini isteme hakkı vardır. Ayrıca tarafların da böyle bir istekte bulunmaları mümkündür (CPP 156). Uzman kendisine uzmanlık

alanına yönelik sorulan soruları, objektif olarak cevaplama yükümüne sahiptir (CPP 158). Ayrıca bir sorunun çözümü için birden fazla uzmanın da görevlendirilmesi mümkündür (CPP 159).

Tüm bunlara ek olarak soruşturmaya yönelik şifrelenmiş olan bir verinin elde edilmesi için, bu konuda teknik bilgi sahibi olan uzmanlardan şifrenin çözülmesini talep edilebilir (CPP 230-1).

Ayrıca kanun içerisinde adli işlemlerin elektronik yöntemlerle bilgisayarlara kaydını içeren bir hüküm (CPP 48-1) ile belli katalog suçlarda failin bulunabilmesi açısından genetik bilgilerin biyolojik kalınlardan elde edilen genetik bilgilerin bilgisayar sistemine kaydedilmesine ilişkin bir hüküm (CPP 706-54) de bulunmaktadır. DNA veri tabanı oluşturulmasına yönelik bu hükümler de kişisel verilerin korunması açısından dijital delillerle ilgilidirler.

I. Hollanda

Hollanda ceza muhakemesi hukukuna yönelik genel kurallar Hollanda Ceza Muhakemesi Kanunu (*Wetboek van Strafvordering [WS]*)³⁶⁰ içerisinde yer almaktadır. Hollanda'da da dijital delillere yönelik düzenlemelerin altyapısı bilişim suçlarına yönelik yapılan düzenlemeler yoluyla oluşturulmuştur. Bilişim suçlarına yönelik en önemli düzenlemeler 1993 tarihli Bilgisayar Suçları Kanunu (*Wet computer criminaliteit*) ve 2006 tarihli Bilgisayar Suçları II Kanunu (*Wet computer criminaliteit II*)'dur. Bu düzenlemeler aracılığıyla WS içerisinde de bazı değişiklikler yapılmıştır.

Bu konuda öncelikle arama ve elkoyma incelenecek olursa, Hollanda ceza muhakemesi hukukunda bilgisayarlarda arama ve elkoymaya yönelik özel hükümler bulunmamaktadır. Bu nedenle bilgisayarlarda yapılan aramalar genel arama hükümleri çerçevesinde yapılmaktadır (WS 96b, 96c, 97, 110). Yine genel elkoyma hükümleri uygulanarak, arama sonucunda bulunan verilerin depolanmış bulunduğu aygıtlara elkonulabilmektedir (WS 95, 96, 96a, 104). Ancak veriler mal olarak kabul

³⁶⁰ Wetboek van Strafvordering,

<http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html>. (Erişim tarihi: 27.02.2015)

edilmedikleri için verilere elkonulamamakta, bu veriler sadece için kopyalama tedbiri kullanılabilmektedir³⁶¹.

Bu durumun yarattığı sıkıntı olarak görülen verilere erişilebilirliğin engellenmesi gereken haller (örneğin çocuk pornografisi ya da virüs programı içeren veriler) açısından oluşan ihtiyaca da Bilgisayar Suçları II Kanunu ile çözüm üretilmiştir. Burada getirilen kurala göre, suç konusu verinin öncelikle kopyalanması gerekmektedir. Daha sonra ise kopyalanan bu verinin aslının bulunduğu aygıt üzerinde silinmesi ya da şifrelenmesi yoluyla bu veriye erişim engellenmiş olmaktadır (WS 125o). Verinin silinmesi emri ise 354. maddeye göre sadece hâkim tarafından verilecek bir karardır³⁶².

Verilerin aranılan bilgisayarın bağlı bulunduğu ağ bağlantıları içerisinde bulunduğu hallerde, aramaya konu bilgisayardan hukuki olarak bu verilerin bulunduğu ağa erişilebiliyorsa, arama bahsedilen ağ bağlantısını da içerecek şekilde genişletilebilir (WS 125j)³⁶³.

Bunun dışında verilerin şifreli olduğu hallerde, yetkili adli makam tarafından şüpheliler hariç olmak üzere (WS 125k/3) ilgili kişilere, şifreyi içeren güvenlik tedbirinin kaldırılması (WS 125k/1), şifreyi çözme, şifreyi çözen anahtarı teslim etme ya da şifrelenmiş veriyi teslim etme (WS 125k/2) emri verilebilir³⁶⁴.

Telekomünikasyon iletişiminin denetlenmesi tedbirinde ise savcı tarafından, sorgu hâkiminin onayının alınması ile servis sağlayıcıların sağladığı iletişim kaydedilebilir (WS 126m). Denetlenen iletişim içeriğinin şifreli olması halinde, şüpheli hariç olmak üzere, ilgili kişilere, şifreyi çözme emri verilebilir (WS 126m/6, 126m/7). Bunun dışında bahsedilen tedbir, 2000 yılından beri, sadece şüphelilere değil, soruşturmaya katkı sağlayabilecek bilgi elde edilebilecek herkese uygulanabilen bir tedbir haline gelmiştir³⁶⁵. Ancak belli gizlilik hakları olan kişilerin (avukat, noter vs. gibi) iletişimi sadece kendileri şüpheli ise denetlenebilir. Başka

³⁶¹ B. J. Koops, “Cybercrime Legislation in the Netherlands”, Electronic Journal of Comparative Law, Vol.14, No.3, December 2010, s. 17, <http://www.ejcl.org/143/art143-10.pdf>.

³⁶² Koops, **a.g.e.**, s. 18.

³⁶³ Koops, **a.g.e.**, s. 18.

³⁶⁴ Koops, **a.g.e.**, s. 18.

³⁶⁵ Koops, **a.g.e.**, s. 20.

kişiler için uygulanan denetimde bu kişiler hakkında elde edilen verilerin silinmesi gerekir (WS 126aa).

Bunlar dışında telekomünikasyon iletişiminin denetlenmesi hakkında son olarak bahsedilmesi gereken husus, telekomünikasyon servis sağlayıcılarının, Telekomünikasyon Kanunu (*Telecommunicatiewet*)’nun 13.1 maddesinde belirtildiği üzere, teknik olarak iletişimin denetlenmesini mümkün kılacak donanıma sahip olması gereğidir. Ayrıca Telekomünikasyon Kanunu 13.4 maddesine göre sağlayıcılara, kişilerin telekomünikasyon iletişim zamanlarının, iletişim sırasında cep telefonlarının yerlerinin ve ön ödemeleri kartlarla ödeme yapanların telefon numaralarının üç aylık bir süre boyunca kaydı zorunlu hale getirilmiştir³⁶⁶.

Hollanda hukukunda bulunan bir başka tedbir ise kullanıcı verilerinin toplanmasıdır. Soruşturma sırasında iletişimi sağlayan servislerden, kişinin ismi, adresi, numarası ve aldığı servisin çeşidi gibi bilgiler temin edilebilir (WS 126na). Ayrıca trafik verilerinin toplanması da kullanıcı verilerinin toplanması kapsamındadır (WS 126n).

Son olarak bahsedilecek tedbir ise üretim emridir. Bu tedbir yoluyla kişilere, kendi mülkiyetlerinde ya da kontrollerinde bulunan soruşturma ile ilgili verileri hâkime teslim etme ya da bu verilere hâkimin erişmesinin sağlanması zorunluluğu getirilmektedir (WS 125i).

J. İsviçre

İsviçre’de ceza muhakemesi kuralları 2011 yılına kadar 26 kantonun kendi düzenlemeleri ve 15 Haziran 1934 tarihli İsviçre Federal Ceza Usul Kanunu tarafından düzenlenmekteydi. Kantonların düzenlemeleri arasındaki farklılıklar nedeniyle pek çok yargılanması gereken kişinin yargılamadan kurtulduğu ve ceza adaletinin gerektiği gibi gerçekleşemediği gerekçeleriyle yapılan uzun süreli birleştirme çalışmaları sonunda yürürlüğe giren İsviçre Ceza Usul Kanunu (*Schweizerische Strafprozessordnung [StPO]/Code de procédure pénale suisse*

³⁶⁶ RAND Europe & Lawford, s. 201.

[CPPS])³⁶⁷ ile federal düzeyde bir kurallar bütünü oluşturulmuştur. İsviçre ceza muhakemesi sisteminde dijital delillere ilişkin temel kurallar bu kanun içerisinde bulunmaktadır³⁶⁸.

İsviçre ceza muhakemesinde de bilimsel açıdan veya tecrübe kuralları gereği maddi gerçeği ortaya çıkarabilecek her tür delil mahkemece kabul edilir (SStPO/CPPS 139/1). Bu nedenle dijital delillerin de ceza yargılamasında kullanılması mümkündür. Ancak delil serbestisi ile getirilen bu deliller hâkimin vicdani kanaati ile ölçülerek hükme konu edilebilirler.

İsviçre hukukunda aramalar SStPO/CPPS 241. maddesi ile 248. maddesi arasında düzenlenmektedir. Arama kararı savcı tarafından verilmektedir. Ancak acil hallerde polisler de bu yetki tanınmıştır (SStPO/CPPS 241/3). Bu arama doğrudan belgelere de kayıtlara da yönelik olabilir. Ancak imkân olduğu hallerde arama yapılan bilgisayara ilişkin verilerin kopyalanması gerekir.

Bu aramaya itiraz edilebilir. İtiraz sebepleri, ilgili kayıtların gizlilik hakları çerçevesinde korunduğu ya da şüpheliyle akrabalık ilişkisinin bulunduğu gibi hususlar olabilir. İtiraz halinde savcı ve polis tarafından ilgili kayıtların bulunduğu aygıt mühürlenecektir (SStPO/CPPS 248). Böylece savcı, aygıt üzerinde herhangi bir incelemede bulunamayacak, 20 gün içerisinde itirazın kaldırılması için mahkemeye başvurması gerekecektir. Mahkeme bir ay içerisinde bu konuda nihai bir karar verecektir.

Genelde bu durum bir problem oluşturmasa da bazı elektronik aygıtlar üzerinde itiraz usulünün uygulanması delil kaybına neden olabilmektedir. Bu nedenle örneğin, analizi için sürekli açık kalması gereken bir aygıt söz konusu olduğunda, mühür altındaki aygıtın güç bağlantısı sağlanmaya devam edilecektir. Ayrıca bazı durumlarda aygıtın kendi kendine güncelleme yapması, bilgileri silmesi ya da

³⁶⁷ Kanunun Almanca versiyonu için bkz.

<http://www.admin.ch/opc/de/classified-compilation/20052319/index.html> (Erişim tarihi: 02.03.2015); Fransızca versiyonu için bkz.

<http://www.admin.ch/opc/fr/classified-compilation/20052319/index.html> (Erişim tarihi: 02.03.2015); İngilizce çevirisi için bkz.

<http://www.admin.ch/opc/en/classified-compilation/20052319/index.html> (Erişim tarihi: 02.03.2015).

³⁶⁸ Bertrand Perrin/Marc Rémy/Romain Roubaty, “**Electronic Evidence in Swiss Criminal Procedure**”, Digital Evidence and Electronic Signature Law Review, Vol. 8, 2011, s. 72.

kapanması durumları da mümkün olabilmektedir. Bu durumda aygıtın nitelikli uzman bilgisi ve alet isteyen bir yöntem olan Faraday kafesi içerisine alınması gerekecektir³⁶⁹.

Aramaya alternatif olarak eşyayı teslim etme yükümü içeren depolama yükümü tedbiri bulunmaktadır (SStPO/CPPS 265). Bu tedbir aleyhe delil vermeye zorlama yasağına tabi kişilere ve dolayısıyla şüpheliye uygulanamaz (SStPO/CPPS 265/2-a, 265/2-b). Ancak şüphelinin ilgili eşyayı gönüllü olarak teslim etmesi mümkündür. Ancak bu sadece gizli olarak uygulanması gerekmeyecek tedbirler için mümkün olabilmektedir. Ancak bu kişiler dışındakiler için soruşturma makamlarının emri üzerine belirlenen bir süre içerisinde ilgili eşyayı teslim etme yükümü getirilmekte, buna uymayanlara ise cezai yaptırım uygulanmaktadır (SStPO/CPPS 265/3).

Arama tedbirinin uygulanmasını genelde elkoyma tedbirinin uygulanması takip etmektedir. Elkoyma tedbiri eşya üzerindeki kullanma veya tasarruf etme hakkının kaldırılmasıdır (SStPO/CPPS 263-268). Normalde savcılarının yetkisinde bulunan elkoyma işlemine, gecikmede sakınca olması halinde polis ve hatta vatandaşlar dahi elkoymayı uygulayabilirler (SStPO/CPPS 263/3). Ancak nihayetinde savcı onayı gerekeceği için bu geçici bir elkoyma olacaktır. Elkoyma pek çok çeşitli eşyayı kapsayabilmektedir. Bu nedenle bilgisayarla ilgili elkoymalarda sosyal medya veya ağ bağlantıları üzerinde bulunan ve delil olarak kullanılacak veriler de elkonulabilir³⁷⁰. Bunun dışında örneğin, bir bilişim suçu işlendiği halde şüphelinin bilgisayarına hem delil olarak hem de suç aleti olduğu için müsadere kapsamında elkonulabilmektedir (SStPO/CPPS 263/1). Elkoymaya yapılacak itirazlarda da aynı aramalarda olduğu gibi mühürleme işlemi uygulanmaktadır.

Trafik verilerinin gerçek zamanlı olarak toplanması da bu konuda düzenlenen tedbirlerden biridir (SStPO/CPPS 269-281). İşbu tedbir kapsamında İsviçre adli makamları tarafından trafik, fatura ve içerik verilerinin gerçek zamanlı olarak toplanması mümkündür. Ancak trafik ve fatura verilerinin elde edilmesinde

³⁶⁹ Perrin/Rémy/Roubaty, **a.g.e.**, s. 73.

³⁷⁰ Perrin/Rémy/Roubaty, **a.g.e.**, s. 74.

SStPO/CPPS 273 içerisindeki katalog uygulanırken, içerik verileri açısından daha ciddi suçları içeren SStPO/CPPS 269 hükmündeki katalog geçerli olacaktır.

Bunların dışında İsviçre'deki posta ve telekomünikasyon iletişimin denetlenmesi ile ilgili yapılmış Posta ve Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Kanunu (*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF]/Loi fédérale sur la surveillance de la correspondance par poste et télécommunication [LSCPT]*)³⁷¹ bulunmaktadır. Bu kanun ile internet servis sağlayıcılara, trafik ve faturalama verilerini altı aylık bir süre boyunca saklama yükümü getirilmektedir (BÜPF/LSCPT 15/3). Ayrıca bu kanun kapsamında yapılacak denetimler, adli makamlardan gelen karar üzerine, Posta ve Telekomünikasyon Denetimleri Servisi (*Überwachung Post- und Fernmeldeverkehr [ÜPF]/Surveillance de la correspondance par poste et télécommunication [SCPT]*) adında bağımsız bir otoritenin koordinasyonu ile yürütülmektedir.

K. Slovenya

Slovenya ceza muhakemesi hukukuna yönelik genel kurallar Slovenya Ceza Usul Kanunu (*Zakon o kazenskem postopku [ZKP]*)³⁷² içerisinde yer almaktadır. 2009 yılına kadar da ZKP içerisinde dijital delillere yönelik özel hükümler bulunmamaktaydı. Ancak 2009 yılında yapılan değişikliklerle ZKP'ye dijital delillerin elde edilmesine yönelik maddeler eklenmiştir (ZKP 219a, 223a). Ceza muhakemesinde dijital delillerin elde edilmesine yönelik temel oluşturan bu maddelerle ilgili dikkat çeken en önemli özellik, madde içerikleri düzenlenirken, elektronik aygıtların değil aynı SSS'de olduğu gibi verilerin temel alınarak düzenlemeye konu olmuş olmalarıdır³⁷³.

Sloven ceza muhakemesi sistemi içerisinde dijital delil elde edilmesi konusundaki düzenlemelerde, dijital delillere elkonulması ile bu delillerin

³⁷¹ Kanunun Almancası için bkz. <http://www.admin.ch/opc/de/classified-compilation/20002162/index.html> (Erişim tarihi: 02.03.2015); Fransızcası için bkz. <http://www.admin.ch/opc/fr/classified-compilation/20002162/index.html> (Erişim tarihi: 02.03.2015).

³⁷² Kanunun (Slovenian Criminal Procedural Act) ilgili maddelere İngilizce çevirisi için Liljana Selinšek, "Electronic Evidence in the Slovene Criminal Procedure Act", Digital Evidence and Electronic Signature Law Review, Vol. 7, 2010.

³⁷³ Selinšek, a.g.e., s. 77.

muhafazasının ardından, bu delilleri barındıran elektronik aygıtlar üzerinde yapılacak incelemelere yönelik yapılmış düzenlemeler dikkat çekmektedir.

ZKP 219a maddesi içerisinde elektronik aygıtlar geniş bir şekilde sayılmıştır. Telefon, faks, bilgisayar ve taşınabilir veri depolama aygıtları gibi veri içeren aygıtların yanı sıra bunlarla bağlantılı aygıtlarda da dijital delil araması yapılabilir. Ancak bu aramanın yapılabilmesi için suç işlendiğine dair makul nedenlere bağlı bir şüphenin bulunması ve elektronik aygıt içerisindeki veriler aracılığıyla şüpheli veya sanığın tespit edilecek veya yakalanabilecek olması ya da bu verilerin ceza yargılamasında delil olarak kullanılabilecek olmaları gerekir (ZKP 219a/1).

Elektronik aygıtın sahibi ya da kullanıcısının aygıtı cihaza erişimi sağlamakla yükümlülüğü bulunmaktadır. Aygıtta şifre varsa şifreyi de açması gerekir. Şüpheli, sanık ve tanıklıktan çekilebilecekler açısından bu yükümlülük uygulanmaz. Yükümlülük yerine getirilmezse karşılığında cezai yaptırım bulunmaktadır (ZKP 219a/6).

Arama yapılabilmesi için ya yazılı rıza ya da mahkeme kararı gerekmektedir (ZKP 219a/2). Karar içerisinde soruşturma konusu aygıtı ayırt etmeye yarayacak bilgi, soruşturmanın nedeni, kolluğun aradığı verinin tanımlanması ve neden bu soruşturma yönteminin kullanıldığına dair bilginin bulunması gereklidir (ZKP 219a/3). Bu kuralın istisnası kişilere ve mala yönelik ciddi tehlikenin bulunduğu durumlar açısından sözlü emirdir (ZKP 219a/5). Ancak sözlü emir mahkeme aracılığıyla 12 saat içerisinde yazılıya dönüşmezse kaydedilen veriler yok edilir. Bunlar dışında arama sırasında tesadüfen delil edilmesi hususu da kanun tarafından düzenlenmektedir (ZKP 219a/9). Tesadüfen elde edilen deliller üzerinden yeni bir soruşturma açılıp açılmayacağı ise savcı tarafından belirlenecektir.

Elektronik aygıtı elkoyma sonrası içerisindeki verileri korumak için iki yol bulunmaktadır. Bunlar; verilerin bütünlüğünün muhafaza edilerek ceza muhakemesinin ilerideki aşamalarında kullanılmak üzere başka bir aygıtta kaydedilmesi ile tüm verilerin kopyalanması ve bu kopyanın doğruluğunun sağlanmasıdır (ZKP 223a/1). Adli bilişim incelemeleri kopyalanan aygıt üzerinden

yapılırken, elkoyma süresi olarak adlandırılabilen tüm bu prosedürlerin toplam süresi ise altı ayla sınırlandırılmaktadır (ZKP 223a/7).

Bunun dışında ihtiyaç duyulmayan verilerin iadesi veya yok edilmesine ilişkin bir hüküm de kanun içerisinde yer almaktadır (ZKP 223a/8).

III. Türk hukukunda dijital delillere ilişkin düzenlemeler

Türkiye’de ceza muhakemesi hukukunda delil serbestisinin bulunduğu daha önce belirtilmişti. Buna bağlı olarak her tür delilin mahkemeye sunulabileceği ve dolayısıyla dijital delillerin de yargılama içerisinde kullanılabileceği söylenebilir. Üstelik Siber Suçlar Sözleşmesi’nin 2014 yılında onaylanması nedeniyle dijital delillerin elde edilmesi konusunda ülke içi mevzuatın SSS’ye uyum çalışmaları kapsamında daha da gelişme göstereceği söylenebilir.

Mevcut durumda SSS’ye uyumun tam olduğu ve kapsamlı düzenlemelerin bulunduğu söylenemese de, hali hazırda bazı önemli düzenlemelerin bulunduğu da yadsınamaz. Ancak bu düzenlemelerin durumunun tam olarak ne olduğu ortaya konulmadan eksiklerin de nerelerde olduğunun tespiti yapılamayacaktır. Bu yüzden dijital delillere yönelik düzenlemeler tek tek incelenecektir. Bu konuda her şeyden önce delilleri ilgilendirecek tüm düzenlemelerin, dijital delilleri de doğrudan ilgilendireceği söylenebilir. Bu düzenlemelere ilişkin bilgiler, bu çalışmanın ceza muhakemesinde delil teorisi ve dijital delillerin yeri başlıklı birinci bölümünde³⁷⁴ detaylı bir özet olarak aktarılmıştır. Bu yüzden burada sadece dijital delillere yönelik teknik düzenlemeler üzerinde incelemede bulunulacaktır.

A. CMK kapsamındaki düzenlemeler

Ceza muhakemesinde dijital delil ile ilgili düzenlemelerin bulunması açısından ilk bakılması gereken kanun, Türkiye ceza muhakemesi hukukunun Anayasa’dan sonraki ana kaynağı olan CMK’dır. Bu yüzden ilk olarak CMK incelenecektir. Dijital delillerin nelerden oluştuğu da göz önünde bulundurulduğunda CMK 134’ün kanun içerisindeki diğer maddelere göre daha dikkat çekici bir madde

³⁷⁴ Bkz. s. 4 vd.

olduğu belirtilmelidir. Nitekim CMK 134 dışındaki maddelerde öngörülen tedbirler aracılığıyla dijital olmayan deliller de elde edilirken, CMK 134 doğrudan dijital delil elde etmeye yarayan bir maddedir.

Bu maddeler dışında kalan uygulamaların kendilerine özel kanunları olmadığı sürece, CMK'nın konuyla ilgili genel hükümlerine gidilmesi suretiyle boşluklar doldurulacaktır. Dijital delillere ilişkin özel bir düzenleme mülga CMUK'ta bulunmamaktaydı. Bu yüzden çıkan problemler için, genel hükümlere başvurularak çözümler aranmaktaydı³⁷⁵.

CMK tasarı halindeyken bilgisayarlar konusunda dijital delillere yönelik bir düzenleme yapılma ihtiyacı hissedilmiş ve bu konuya ilişkin bir madde kendisine CMK içerisinde yer bulmuştur. İşbu madde tasarıda 110. madde olarak geçen mevcut CMK 134. maddesidir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma başlıklı CMK 134, tasarı gerekçesinde³⁷⁶ de belirtildiği üzere, başlığında belirtilen hususları düzenleyen, arama ve elkoyma tedbirinin özel bir halidir. Bilgisayarlara yönelik bir madde olması nedeniyle CMK içerisinde dijital delillere yönelik olarak akla gelen ilk düzenleme bu olmaktadır.

³⁷⁵ Bu konuda AİHM'in aldığı Ağaoğlu v. Turkey kararı için bkz. s. 131.

³⁷⁶ Maddenin gerekçesi şu şekildedir:

“Madde 110 - Madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır.

Ancak bilgisayarlardaki kayıtların gerçeğin açığa çıkarılması yönünden, ceza davasında delil, iz, eser ve emare oluşturacağı ortadadır. Bu itibarla madde hem bu olanağı sağlamak ve hem de bireysel yararları saklı tutmak amacıyla bilgisayar program ve kütüklerinde arama yapılmasını aşağıdaki belirli koşullara tâbi kılmış bulunmaktadır;

1. İki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve aygıtı 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, aygıtı geçici olarak elkonulabilir. Çözümünden hemen sonra bilgisayardaki bilgilere zarar vermeden aygıtın ilgisine hemen geri verilmesi gerekir.

Dikkat edilmelidir ki, bu maddenin amacı 107 nci maddeden farklıdır. 107 nci maddede bilgisayar işlemekte iken içeri girilmekte ve ilgilinin bundan haberi olmamaktadır. Bu maddede ise, durağan hâldeki aygıtta araştırma, arama yapılmaktadır.

Maddenin öngördüğü geçici elkoyma işlemine itiraz edilebilecektir.”

Maddenin içeriğini başlığından itibaren başlayarak, fıkra fıkra inceleyerek gitmek yoluyla maddeyi de kademe kademe incelemek mümkün olacaktır.

Bu durumda öncelikle maddenin başlığı incelenecektir. İşbu maddenin başlığı bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymadır. Daha maddenin başlığında da görüleceği üzere, maddenin içeriğinin bütün dijital delilleri kapsayıcı olmadığı kendisini açık bir şekilde göstermektedir. Madde başlığının ve içeriğinin sadece bilgisayarlara yönelik düzenlenmesi nedeniyle, bu konuda dar yorumlama yapıldığında bilgisayar niteliğini haiz olmayan aygıtlar üzerinde bu maddenin uygulanması mümkün olmayacaktır³⁷⁷. Bu sorun kanunun işbu maddesinin veri odaklı değil, bilgisayar odaklı düzenlenmiş olmasından ileri gelmektedir. Böyle bir durumda CMK 134 bilgisayar dışındaki aygıtlara hitap etmemiş olacak ve bu aygıtlar açısından dijital delil arama ve elkoyma yöntemleri genel kurallara göre yapılacaktır. Böylece bilgisayar dışındaki aygıtlar açısından kopyalama tedbirine başvurulması ile var olmayan bir düzenleme üstünden tedbir uygulanmaya çalışılacağı için bu yolla elde edilecek dijital deliller açısından hukuka aykırılık oluşması mümkün hale gelecektir. Ancak genel olarak uygulamada bilgisayar dışındaki aletler için de CMK 134 hükümlerinin kapsayıcı olarak uygulandığı görülmektedir³⁷⁸.

Buna ek olarak bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama ve elkoymalar CMK 116 ve 123 hükümlerinde bulunan genel hükümlere göre yapılamaz. Bu tip aramalarda mutlaka CMK 134 kapsamında alınmış kararın da bulunması gerekir³⁷⁹.

Maddenin ilk fıkrasının içeriği ise şu şekildedir: *”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*

³⁷⁷ Dülger, **a.g.e.** , s. 726 içerisinde madde başlığında bilişim sistemi demenin yeterli olacağı belirtilmektedir.

³⁷⁸ Cengiz Tanrıkulu, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara: Adalet Yayınevi, 2014, s. 358.

³⁷⁹ Dülger, **a.g.e.** , s. 729. Bu konu ABD’de cep telefonları açısından tartışma konusu oluşturmuş ve cep telefonlarına yönelik arama kararlarının cep telefonlarına özel bir şekilde verilmesi gerektiğine hükmedilmiştir. Konuyla ilgili olarak 25 Haziran 2014 tarihinde verilmiş bir karar için bkz. Riley v. California 573 U.S. (2014), <https://www.law.cornell.edu/supct/pdf/13-132.pdf>. (Erişim tarihi: 07.02.2015)

kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.”.

İçerikten de görüleceği üzere bilgisayar, bilgisayar programları ve bilgisayar kütüklerine yönelik yapılacak aramalar yalnızca soruşturma aşamasında yapılabilir izlenimi doğmaktadır. Üstelik madde içerisinde sanıktan bahsedilmeyerek sadece şüpheliden bahsedilmesi ile bu izlenim pekiştirilmiştir. Bu durumda dar lafzi yorumlama metodu tercih edildiğinde sanki kovuşturma aşamasında böyle bir aramanın yapılması mümkün olamayacakmış gibi bir sonuç doğmaktadır³⁸⁰.

Ayrıca madde içerisinde sonradan da görüleceği üzere herhangi bir suç kataloğu bulunmamaktadır. Bu nedenle, bu maddenin herhangi bir suç için yapılan soruşturmada kullanılması mümkündür. Oysaki maddenin tasarısındaki karşılığının gerekçesinde iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren suçlar için kullanılması öngörülmekteydi³⁸¹.

Ayrıca bu tedbire başvurulabilmesi için somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı gerekmektedir³⁸². Yeni getirilen bu şart ile içerisinde elde edilmiş somut delil³⁸³ bulunmayan bir suç soruşturmasında bu yöntemle başvurulamayacağı hüküm altına alınmış olmaktadır. Böylece aynı tutuklamada olduğu gibi, bu tedbirin verilmesi zorlaştırılmış, daha sıkı bir şart olan kuvvetli şüphe varlığı da aranır hale gelmiştir.

Yine bu tedbire başvurulabilmesi için gerekli olan bir diğer koşul ise başka surette delil elde etme imkânının bulunmaması halidir. Uygulamada en son çare ve zorunluluk koşulu olarak da adlandırılan bu koşulun özellikle aranmasının sıkıntılara

³⁸⁰ Centel/Zafer, **a.g.e.** , s. 386 içerisinde sanığın tedbiri, aleni duruşmada öğrenmesi ile ilgili verileri sileceği için bu uygulamanın etkisiz olacağı görüşündedir; Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1311 ise bu tedbirin yalnızca soruşturma aşamasında uygulanabileceğini belirtmektedir. Kovuşturma aşamasında da bu tedbirin uygulanabileceğine dair görüş için bkz. Değirmenci, **a.g.e.** , s. 318; Tanrıkulu, **a.g.e.** , ss. 353-354.

³⁸¹ Temel haklara müdahalenin böylesine yoğun olduğu bir tedbir açısından en azından belli ağırlıktaki suçların katalog olarak öngörülmesi gerektiği hakkında bkz. Centel/Zafer, **a.g.e.** , s. 387.

³⁸² İşbu hüküm daha önceden bulunmamakla birlikte, 6526 sayılı kanunun 11. maddesi ile CMK 134'e eklenmiştir.

³⁸³ Somut delil denildiğinde anlaşılacak olan deliller, maddi deliller olmaktadır. Bu hüküm dijital delil elde etmede kullanılan tüm tedbirlere ilişkin maddelere (CMK 134, 135, 140) konulmuştur. Böylece soyut yapıya sahip dijital delillerin elde edilebilmesi için verilecek karar için önceden elde edilmiş somut yapıda bir delilin varlığı gereği ortaya çıkmaktadır.

yol açtığı belirtilmektedir. Zira dijital deliller klasik delillere göre değiştirilmeye, bozulmaya ve yok edilmeye daha elverişli oldukları ve kolaylıkla karartılabilecekleri için başka şekillerde delil elde edilmeye çalışıldıktan sonra sıranın en son çare olarak dijital delillere gelmesi geç kalınmış bir tedbir olacak, dolayısıyla faillere ulaşmayı güçleştirecektir³⁸⁴.

Bunlara ek olarak maddenin içerisinde özellikle şüphelinin kullandığı³⁸⁵ ifadesine yer verilmiştir. Bundan da yola çıkarak üzerinde arama ve kopyalama işlemi yapılacak elektronik aygıtların şüpheliye ait olma gereği bulunmadığı söylenebilir³⁸⁶. Böylece şüphelinin malik olması aranmamakta, sadece kullanımda bulunması yeterli sayılmaktadır. Böylece üçüncü kişilere ait bilgisayarların da tedbir konusunu oluşturması mümkün olmaktadır. Hatta şüphelinin kullandığı ibaresinin de bir kısıtlama yarattığı ve delillere ulaşmada şüphelinin kullanmadığı bilgisayarlara yönelik de düzenleme yapılması gerekir³⁸⁷.

Bu yöntemin bir diğer özelliği de savcı istemi ve hâkim kararı olmaksızın uygulanamamasıdır. Yani bu tedbir uygulanırken gecikmesinde sakınca bulunan hal bulunması göz önüne alınmamıştır. Böylece hâkim kararı bu tedbir için olmazsa olmaz bir hale gelmektedir.

Ancak aramanın sonuca ulaşmadığı hallerde, yani verilerin yapısı nedeniyle arama konusunda bir engelle karşılaşıldığı takdirde, bilgisayar üzerinde bu engellerin aşılmasına yönelik çalışma yapmak gerekecektir. Bu gibi durumlar için ise maddenin ikinci fıkrası öngörülmüştür.

Maddenin ikinci fıkrasının içeriği şu şekildedir: ”*Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılabilmesi halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin*

³⁸⁴ Özellikle bilişim alanında suçlar ve bilişimin araç olarak kullanıldığı suçlar açısından bu durumun yaratacağı sıkıntı için bkz. Dülger, **a.g.e.** , s. 725. Ancak yazar bu şekilde bir hükmün konmasının da kişisel verilerin güvenliği ve özel hayatın gizliliğini etkileyebilecek bir yanı olduğunu da inkâr etmemektedir.

³⁸⁵ Buradaki kullanımın hem fiili hem de sanal kullanım şeklinde anlaşılması gerekeceğine yönelik görüş için bkz. Değirmenci, **a.g.e.** , s. 321.

³⁸⁶ Dülger, **a.g.e.** , s. 723.

³⁸⁷ Dülger, **a.g.e.** , s. 723; Değirmenci, **a.g.e.** , s. 320 içerisinde bu yönde yapılacak bir düzenlemede rıza koşulunun da aranması gerektiğini belirtmektedir.

çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.”

Burada ilk olarak belirtilmesi gereken husus, bilgisayara yönelik elkoyma tedbirine başvurabilmenin yalnızca bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülmemesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde mümkün olmasıdır. Buradan çıkan sonuca göre bu haller dışında bilgisayara elkonulamayacağı yorumu da yapılabilir. Bu şekilde kanun, şifrenin çözülmemesi veya gizlenmiş bilgilere ulaşılamaması halleri dışındaki hallerde kopyalamanın da olay yerinde yapılmasını gerektireceğini belirtmiştir. Ancak sadece şifrenin çözülmemesi veya gizlenmiş bilgilere ulaşılamaması hallerinde değil, detaylı inceleme gereken her durumda bilgisayarın adli bilişim laboratuvarında incelenmesi de mümkün olabilmelidir³⁸⁸.

İkinci fıkranın son cümlesinde ise şifre çözümü yapılan ve gerekli kopyaları alınan elkonulan cihazların gecikme olmaksızın iade edilmesi gerektiği belirtilmiştir. Bir kere burada gecikme olmaksızın tabiri büyük bir belirsizlik yaratmaktadır. Ayrıca iadenin tek sonuç olarak düzenlemesinin de doğru olmayan bazı sonuçlar çıkarabileceği de ortadadır. Örneğin içerikleri suç oluşturan veriler içeren aygıtların içerdikleri verilere erişimin engellenmesi ya da bu verilerin imhasına yönelik hükümler bulunmaması önemli bir eksikliktir³⁸⁹. Ayrıca madde içeriğinden şifre çözümü yapılamayan aygıtların iade edilmeyeceği sonucu da çıkmaktadır. Böyle bir durumda da mülkiyet hakkının ihlale uğramasının önü açılmış olmaktadır.

Maddenin üçüncü fıkrasının içeriği şu şekildedir: *“Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.”*

Bu fıkra da belirtilen hususun gerçekleştirilmesi delil sağlamlığı ve bütünlüğünü sağlama açısından mantıklı gözükmemektedir. Nitekim incelemelerin de çıkartılan yedeklerle yapılması halinde orijinal verilere zarar gelmesinin de önüne geçilebilir. Bunun yanı sıra imaj alma ve veri içeren aygıtın hash değerinin alınması

³⁸⁸ Uygulamada kolluk tarafından bilişim sisteminde şifre olduğuna dair tutulan tutanaklarla yasa dolanılmaktadır. Gerekçe olarak ise yeterli personelin bulunmadığı ve işlemlerin yetismeyeceği ileri sürülmektedir. Bu konuda bilgi için bkz. Dülger, **a.g.e.**, s. 727.

³⁸⁹ Bkz. s. 78; SSS 19/3 gereği.

gibi yedeklemeyi sağlayacak tüm bu işlemlerin şüpheli veya müdafî önünde yapılması gerekir. Aksi takdirde sistemdeki verilerin değiştirildiğine yönelik iddiaların önü açılmış olur³⁹⁰.

Maddenin dördüncü fıkrasının içeriği ise şu şekildedir: “Üçüncü fıkra göre alınan, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.”

Bu fıkranın değişmeden önceki hali³⁹¹ haklı bir şekilde eleştirilmekteydi. Değişikle, yedeğin kopyasının şüpheli veya müdafîne³⁹² verilmesi isteğe bağlılıktan çıkarılıp zorunlu hale getirilmiştir. Böylece, yedeklemesi yapılan sistemdeki verilerde değişiklik yapıldığı iddiasının gündeme gelmesi durumunda şüpheli veya müdafîne verilen yedek ile ekleme yapıldığı iddia edilen kopya arasında karşılaştırma yapılabilmesi imkânı sağlanmaktadır. Ancak bu noktada bir başka tartışma ise içeriği suç barındıran verilerin şüpheliye iade edilmesinin ne kadar doğru olduğu üzerine olacaktır.

Maddenin beşinci ve son fıkrasının içeriği ise şu şekildedir: “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.”

Bu fıkra elkoyma yapılmadan da ilgili verilerin kopyalanabileceği hüküm altına alınmıştır. Ancak yine devamında kopyası alınan verilerin kâğıda yazdırılarak tutanağa kaydedilebileceği belirtilmiştir. Ancak bu fıkra sadece az yer kaplayan içerikler veya örneğin yazı, şekil gibi kâğıda geçirilebilecek bazı içerikler açısından mümkün olabilir. Örneğin bir videoyu kâğıda yazdıramazsınız. Bunun dışında çok büyük yer kaplayacak ve milyonlarca sayfa tutabilecek bir yazılı içeriğin kâğıda aktarılması kadar çağdışı bir uygulama da mantıklı değildir³⁹³.

³⁹⁰ Dülger, **a.g.e.**, s. 660, 728.

³⁹¹ 6526 sayılı kanunun 11. maddesi ile değişmeden önce, “Üçüncü fıkra göre alınan” tabiri yerine “İstemesi” kelimesi vardı. Böyle bir belgenin isteğe bağlanmadan doğrudan verilmesi gereği üzerinde durulmaktaydı.

³⁹² Centel/Zafer, **a.g.e.**, s. 386 göre burada “vekil” kelimesi hatalı kullanılmıştır. Doğrusunun “müdafî” olması gerekir.

³⁹³ Tanrıkulu, **a.g.e.**, s. 375.

CMK 134 içeriğine genel olarak bakıldığında tedbirin sadece hareketsiz bulunan depolanmış bilgisayar verilerini konu aldığı görülecektir. Ancak dijital delillerin çekirdek değeri olan veriler her zaman bu durumda bulunmamaktadırlar. Böylece verilerin hareket ettiği, yani gerçek zamanlı olarak akış halinde bulunduğu haller, CMK 134 tarafından karşılanamamaktadır. Türk hukukundaki bu boşluk CMK 135 ile düzenlenen iletişimin denetlenmesi tedbirleri³⁹⁴ aracılığıyla karşılanmaktadır.

CMK 135'in içerisinde başlığında belirtilen iletişimin tespiti, iletişimin dinlenmesi ve kayda alınması tedbirlerinin yanı sıra sinyal bilgilerinin değerlendirilmesi gibi bir tedbir de bulunmaktadır³⁹⁵. Maddede bulunan bir diğer

³⁹⁴ Burada iletişimin denetlenmesi tedbirlerinin tümünün konuyla ilgili olduğu değil, CMK 135'in bu konudaki rolü vurgulamak istenmiştir. CMK 135 ile ilgili yapılmış çalışmalar için daha geniş çaplı çalışmalar için bkz. Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1339 vd.; Seydi Kaymaz, **İletişimin Denetlenmesi: Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan**, 4. Baskı, Ankara: Seçkin Yayınevi, 2015; Cumhuriyet Şahin, **"Telekomünikasyon Yoluyla İletişimin Denetlenmesi"**, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XI, Sayı: 1-2, 2007, ss. 1095-1112.

³⁹⁵ Bu tedbirlere ilişkin tanımlar konuyla ilgili olan iki yönetmeliğin içerisinde yapılmış bulunmaktadır:

Resmi Gazete, Tarih: 10.11.2005, Sayı: 25989 ile yayımlanmış Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik'in 3. maddesine göre;

"h) İletişimin dinlenmesi ve kayda alınması: Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri,

i) İletişimin tespiti: İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri,

p) Sinyal bilgisi: Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,

r) Telekomünikasyon: Her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını,"

ifade etmektedir.

Ancak Resmi Gazete, Tarih: 14.02.2007, Sayı: 26434 ile yayımlanmış Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'in 4. maddesine göre;

"e) İletişimin dinlenmesi ve kayda alınması: Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemler,

f) İletişimin tespiti: İletişimin içeriğine müdahale etmeden, iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler,

h) Sinyal bilgisi: Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,

i) Sinyal bilgilerinin değerlendirilmesi: İletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlaşılandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemleri,

tedbir olan mobil telefon yeri tespiti sadece yakalama amaçlı yapılabilir. Bu nedenle bu tedbir aracılığıyla delil elde edilemeyecektir³⁹⁶. Bunun dışında tanımlarına bakıldığında iletişimin dinlenmesi ve kayda alınması dışındaki tedbirlerin depolanmış veriler üzerinden gerçekleştiği görülmekte, bu nedenle gerçek zamanlı akış halindeki veriler açısından sadece iletişimin dinlenmesi ve kayda alınması tedbirinin önem kazandığı söylenebilmektedir.

CMK 135 içerisinde bahsedilen tedbirlerin uygulamasının nasıl gerçekleşeceği CMK içerisinde düzenlenmemiştir. Bu konudaki düzenleme de 5397 sayılı kanun tarafından getirilen “...5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu³⁹⁷ bünyesinde, Kurum başkanına doğrudan bağlı “Telekomünikasyon İletişim Başkanlığı” adıyla kurulan tek bir merkezden yürütülür.” hükmünün, şu anda PVSİ ek 7/10 olarak adlandırılan hükmü içerisinde bulunmaktadır. Kanun hükmünde kullanılan dinlemeler kelimesi yerine tedbirlerin açık bir şekilde tek tek yazılması kanun yapma tekniği açısından daha doğrudur. Telekomünikasyon İletişim Başkanlığı’nın bu konudaki görevi, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik’in 17. maddesinin b fıkrasında da açıkça belirtilmiştir³⁹⁸. İşbu hükümlere

j) Telekomünikasyon: İşaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması,”

olarak tanımlanmaktadır.

(2007 tarihli Yönetmelik’e ilişkin olarak Danıştay İdari Dava Daireleri Kurulu’nun 2011 yılında verdiği bir karar [Danıştay İdari Dava Daireleri Genel Kurulu, E. 2010/2072, K. 2010/1467, T. 4.11.2010] bulunmaktadır. Bu karara yönelik tartışma olmakla birlikte kararda özetle Adalet Bakanlığı’nın hazırladığı bu yönetmelikle ilgili iptali için başvuru maddeleri iptal etmiş, CMK 135 ila 140. maddeleri düzenlenen konularda Adalet Bakanlığı’nın düzenleme yetkisi bulunmadığını belirtmiştir.)

³⁹⁶ Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.**, s. 1358.

³⁹⁷ 4502 sayılı Telgraf ve Telefon Kanunu, Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun, Telsiz Kanunu ve Posta, Telgraf ve Telefon İdaresinin Biriktirme ve Yardım Sandığı Hakkında Kanun ile Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin Eki Cetvellerde Değişiklik Yapılmasına Dair Kanun’un 14. maddesi ile 2813 sayılı Telsiz Kanunu’nun 5 maddesinde yapılan değişiklik ile Telekomünikasyon Kurumu kurulmuştur. Daha sonra ise 5809 sayılı Elektronik Haberleşme Kanunu ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu (BTK) olarak değiştirilmiştir. 2813 sayılı Telsiz Kanunu’nun adı da aynı kanunun 67. maddesi ile “Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun” olarak değiştirilmiştir.

³⁹⁸ “Madde 17- Başkanlığın görevleri şunlardır; (Başkanlık aynı yönetmeliğin 3/d hükmüne göre Telekomünikasyon İletişim Başkanlığını ifade etmektedir.)

...b) 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemleri tek bir merkezden yürütmek,”

göre CMK 135 kapsamındaki iletişimi dinleme tedbirleri tek merkez olarak Telekomünikasyon İletişim Başkanlığı (TİB)'nda yapılacaktır³⁹⁹.

CMK 134 ve 135 kapsamında uygulanan tedbirlerin bir yan ürünü olan tesadüfen elde edilen delillerin de dijital verilerden oluşmaları mümkündür. Bu konu ise CMK 138 kapsamında düzenlenmiştir.

Maddenin arama ve elkoymayı ilgilten birinci fıkrası şu şekildedir: “*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.*”

Görüldüğü gibi arama veya elkoyma koruma tedbirlerinin uygulanması sırasında diğer herhangi bir suçun işlendiği şüphesini uyandıran deliller, tesadüfen elde edilen deliller kapsamına girecektir. Bu kapsama giren deliller muhafaza altına alınarak, durum savcılığa bildirilecektir. Bu maddede “arama ve elkoyma tedbirlerinin uygulanması sırasında” kısmının lafzını dar olarak yorumlamamak gerekir. Aksi takdirde sadece genel arama ve elkoyma kararları için geçerlilik olacaktır. Ancak bu maddede bulunan arama ve elkoyma tedbiri içerisine CMK 134 kapsamındaki aramalar da dâhil olacaktır⁴⁰⁰.

Maddenin ikinci fıkrası ise şu şekildedir: “*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.*”

³⁹⁹ Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1502 içerisinde tüm bu işlemin tek merkezden yürütülmesinin kötüye kullanılabileceğine dikkat çekmektedir.

⁴⁰⁰ Yusuf Yaşar/İsmail Dursun, “**Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri**”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 19, Sayı:3, 2013, s. 23; Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1511 içerisinde bu madde kapsamında bulunacak deliller açısından çıplak gözle görülebilme şartının geçerli olması gereğini ortaya koymaktadır. Dolayısıyla veri aramalarında, örneğin olayla ilgisi olmayan dosyaların ya da tüm verilerin bir şey buluruz umuduyla aranması bu noktada bir problem oluşturabilir.

Görüldüğü gibi bu sefer CMK 135 kapsamında yapılan iletişimin denetlenmesi tedbirlerinin uygulanması sırasında tesadüfen elde edilen delillere ilişkin bir düzenleme yapılmaktadır. Ancak bu sefer bir önceki fıkradan farklı olarak CMK 135 içerisinde sayılan katalog suçlardan birisinin işlendiğine dair şüphe bulunması gerektiği sınırlaması getirilmiştir. Bu sınırlamaya uyan tesadüfen elde edilmiş deliller muhafaza altına alınacak, savcıya bu konuda bildirim yapılacaktır.

Son olarak teknik araçlarla izleme tedbirinde (CMK 140) de elde edilen veriler depolandığından, bu tedbirle elde edilen deliller açısından da CMK 134'ün kapsayıcılığından bahsedilebilecektir.

B. Diğer düzenlemeler

CMK öncesindeki dönemde CMUK içerisinde dijital delillere yönelik bir düzenleme bulunmasa da, CMUK dışında dijital delillere ilişkin bazı düzenlemeler bulunmaktaydı. 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu (ÇASÖMK) içerisinde bazı maddeler aracılığıyla düzenlenmiş olan iletişimin tespiti ve dinlenmesi⁴⁰¹, gizli izleme⁴⁰² ile kayıt ve verilerin incelenmesi⁴⁰³ tedbirleri bunlara örnek gösterilebilirler⁴⁰⁴. Ancak bu hükümler sadece ÇASÖMK içerisinde belirlenen suçlara ilişkin olarak uygulanabilmekteydi. CMK içerisinde getirilen yeni hükümler nedeniyle ÇASÖMK kaldırılmıştır⁴⁰⁵.

⁴⁰¹ ÇASÖMK iletişimin tespiti ve dinlenmesi başlıklı 2. maddesi; “*Bu Kanunda öngörülen suçları işleme veya bunlara iştirak yahut işlendikten sonra faillere her ne suretle olursa olsun yardım veya aracılık veya yataklık etme kuşkusu altında bulunan kimselerin kullandıkları telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyalleri, yazıları, resimleri, görüntü veya sesleri ve diğer nitelikteki bilgileri dinlenebilir veya tespit edilebilir...*” şeklinde düzenlenmektedir.

⁴⁰² ÇASÖMK gizli izleme başlıklı 3. maddesi; “*Bu Kanunda öngörülen suçları işlediklerinden kuşku duyulanların mesken, ikametgâh, işyeri veya kamuya açık yerlerdeki her türlü faaliyetleri, teknik araçlarla gizli olarak gözetlenebilir, izlenebilir, ses ve görüntü kaydına alınabilir.*” şeklinde düzenlenmiştir.

⁴⁰³ ÇASÖMK kayıt ve verilerin incelenmesi başlıklı 4. maddesi; “*Bu Kanunda öngörülen suçların veya delillerinin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumdaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenebilir.*” şeklinde düzenlenmiştir.

⁴⁰⁴ Bu düzenlemelerdeki tedbirlere ilişkin daha geniş çaplı bilgi için bkz. Vesile Sonay Evik, **Çıkar Amaçlı Örgütlenme Suçu**, İstanbul: Beta Yayınevi, 2004, ss. 135-139.

⁴⁰⁵ ÇASÖMK, 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şeklinde Kanun'un 18. maddesiyle yürürlükten kaldırılmıştır.

Günümüzde ise dijital delillere ilişkin genel düzenleyici kanun CMK olsa da, CMK dışında bazı düzenlemelerde de dijital delilleri ilgilendiren hükümler bulunmaktadır.

Bunlara ilk örnek olarak elektronik haberleşme başlığı eklenebilir. Nitekim 5809 sayılı Elektronik Haberleşme Kanunu'nun 12. maddesinde de dijital deliller açısından önemli bir madde bulunmaktadır. İşbu maddenin 2. fıkrasında "*Kurum*⁴⁰⁶, *işletmecilere*⁴⁰⁷ *sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojiye meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirebilir.*" denilmiş ve g bendi ile "*Kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması.*" yükümü işletmecilere getirilmiştir. Yine aynı kanunun 51. maddesi de dijital delil konusunu ilgilendirebilecek kişisel verilere ilişkin olup AYM tarafından iptal edilmiştir⁴⁰⁸.

Elektronik haberleşme içerisinde bir başlık olarak ise internet ortamlarında yapılan yayınlar başlığı verilebilir. İşbu başlık içerisindeki düzenlemeler 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun içerisinde bulunmaktadır. Bu kanun içerisinde özellikle internet üzerindeki verilerin elde edilmesi açısından getirilen önemli düzenlemeler mevcuttur. Bu da dijital delil elde etme çalışmasının internete uzandığı haller için gerekli olmaktadır. Bu amaçla öncelikle kanunun 1. maddesinde internet hizmetini sağlayan servis sağlayıcıların erişim, içerik, yer ve toplu kullanım sağlayıcı olmak üzere dörtlü bir ayrımı yapılmış, 2. maddede de bu sağlayıcıların tanımları yapılmıştır⁴⁰⁹. Daha sonra ise tanımı gereği akla ilk olarak

⁴⁰⁶ Aynı kanunun 3/ee hükmüne göre kurum ile kastedilen Bilgi Teknolojileri ve İletişim Kurumu (BTK)'dur.

⁴⁰⁷ Aynı kanunun 3/z hükmüne göre işletmeci ile kastedilen yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirkettir.

⁴⁰⁸ AYM E. 2013/122, K. 2014/74, T. 09.04.2014. İptal edilen madde şu şekildedir: "*MADDE 51- (1) Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir.*". Bu maddenin iptalinin gerekçesi Anayasa'nın 20. maddesini ihlal etmesidir. Kişisel verilere ilişkin hususlar ile ilgili bkz. s. 147 vd.

⁴⁰⁹ Kanunun 2. maddesine göre yapılan tanımlar şu şekildedir:

"...e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

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

internet kafeleri getiren toplu kullanım sağlayıcılar haricindeki üç asli sağlayıcıya çeşitli yükümlülükler getirilmiştir.

Örneğin, 5651 sayılı kanunun 4. maddesinin 3. fıkrasında; “*İçerik sağlayıcı, Başkanlığın⁴¹⁰ bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder...*” denilmektedir. Yine kanunun 5. maddesinin 3. fıkrası; “*Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.*” şeklinde olup yer sağlayıcılara bilgi saklama yükümü getirilmektedir. 5. maddenin 5. fıkrası ile ise saklanan bu bilgiler talep halinde talep edilen şekilde Başkanlığa teslim edilecektir. Erişim sağlayıcılar ise 6. maddenin 1. fıkrasının b bendi ile bilgi saklama ve depolama yükümü altına sokulmuşlardır. Bu düzenleme; “*Erişim sağlayıcı... sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla... yükümlüdür.*” şeklinde yapılmış ve aynı maddenin aynı fıkrasının d bendi olan “*Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle... yükümlüdür.*” şeklinde devam etmektedir.

Bunların yanı sıra 10.09.2014 tarihli 6552 sayılı kanunla değiştirilen 3. maddenin 4. fıkrası ile yine bilgi sağlama yükümüne ilişkin bir diğer hüküm konulsa da bu hüküm haklı gerekçeyle AYM tarafından iptal edilmiştir⁴¹¹.

Daha önce de bahsedildiği üzere CMK 135 kapsamındaki tedbirler 5651 sayılı kanun içerisinde Başkanlık olarak geçen TİB tarafından uygulanmaktadır.

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

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

⁴¹⁰ “b) Başkanlık: Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığını... ifade eder.”

⁴¹¹ İşbu hüküm; “*Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi halinde ilgili mercilere verilir.*” şeklindedir. Bu madde dikkatli bir şekilde okunduğunda herhangi bir suç soruşturması ve kovuşturması dâhilinde bir talep olmadan TİB’in internet servis sağlayıcılarından bilgi almasının önü açılmaya çalışılmıştır. Ancak AYM tarafından 02.10.2014 tarihli ve E. 2014/149, K. 2014/151 karar ile kişisel veri olarak da değerlendirilebilecek bu tür bilgilerin herhangi bir kurala tabi olmadan elde edilebilir olmasının temel hak ve özgürlükleri ihlal edeceği gerekçesiyle iptal edilmiştir. Bkz. Resmi Gazete, Tarih: 01.01.2015, Sayı: 29223.

Böylece bu konuda tek merkez olması hedeflenen TİB, 5651 sayılı kanun ile içerik, yer ve erişim sağlayıcıların tümünden bilgi alabilecek şekilde yetkilendirilmektedir. Dolayısıyla CMK 135 kapsamındaki tedbirlerin interneti ilgilendiren kısımları açısından, internet servis sağlayıcılar ile TİB arasındaki köprü önem kazanmaktadır.

Kişisel verilerin korunması meselesi de dijital delilleri ilgilendirebilecek bir diğer başlık olarak ele alınabilir. Kişisel veri kavramı kendisine en üst ulusal norm olan Anayasada yer bulmuştur. Anayasanın özel hayatın gizliliği başlıklı 20. maddesinin 3. fıkrası verilerle ilgilidir. İşbu maddenin içeriği şöyledir: *“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”*. Görüldüğü gibi kişisel verilerin korunmasına ilişkin esas ve usullerin kanun ile belirleneceği maddede belirtilmekle birlikte henüz ortada bu çerçeveyi belirleyecek bir kanun bulunmamaktadır. Ancak yıllardır tasarı halinde bekleyen bu konu güncel olarak tekrar ortaya çıkan bir Kişisel Verilerin Korunması Kanunu Tasarısı⁴¹² ile tekrar gündeme gelmiştir.

İşbu Tasarı'nın 3. maddesinde kişisel veri; belirli veya kimliği belirlenebilir gerçek kişiye ilişkin bütün bilgiler olarak tanımlanmıştır. Kişisel verilerin hukuka aykırı kaydedilmesini suç olarak düzenleyen 5237 sayılı TCK'nın 135. maddesinin gerekçesinde de bir gerçek kişiyle ilgili her türlü bilginin, kişisel veri olarak kabul edilmesi gereği belirtilmiştir⁴¹³. Böylece kişilere ilişkin bütün bilgilerin kişisel veri kapsamına girebileceği belirtilmiştir.

Kişisel verilerin işlenmesi gerek mal ve hizmet üretimi açısından özel sektöre; gerekse eğitim, sağlık, vergi, sosyal güvenlik, kamu düzeni ve güvenliği açısından kamu sektörüne önemli avantajlar sunmaktadır. Günümüzde kişisel verilerin dijital teknoloji kullanan elektronik aygıtların kullanımı yoluyla işlendiği

⁴¹² Kişisel Verilerin Korunması Kanunu Tasarısı, <http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf>. (Erişim Tarihi: 16.06.2014)

⁴¹³ 5237 sayılı Türk Ceza Kanunu gerekçesi, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc. (Erişim Tarihi: 17.03.2014)

düşünülünce, özellikle ceza yargılamasında bu konunun da dijital deliller bakımından da önemi olabilecektir. Nitekim kişisel verilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Üstelik bu hukuka aykırılığın ceza hukukunda da karşılığı olduğu için, kişisel verilere ilişkin problemlerin de ceza muhakemesi açısından dijital delillerle alakalı olabileceği söylenebilir.

Kanunlar dışında bazı yönetmeliklerde de dijital delilleri ilgilendiren hükümler bulunmaktadır. Suç Eşyası Yönetmeliği⁴¹⁴,nin “Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler” başlıklı 9. maddesi buna örnek gösterilebilir. Maddenin ikinci fıkrası şu şekildedir: *“Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir.”* Aynı maddenin beşinci fıkrası şu şekildedir: *“Yapısı gereği sabit diskler ve diğer elektronik materyaller ısıya, neme ve sarsıntıya karşı hassastırlar. Bu madde ile elkonulan bilgisayar, bilgisayar kütükleri, bu sisteme ilişkin verilerin asıl ya da kopyalarının ve depolama aygıtları gibi eşyaların bozulmalarını engellemek için uygun ortamlarda muhafaza edileceği düzenlenmiştir. Emanet dairesi / deposunda saklanması mümkün olmayan eşyaların sulh hâkiminden, soruşturma sonu bekletilmeksizin satılmasına veyahut uygun görülen farklı bir mercie teslim edilmesine karar verilmesi talep edilir ve neticede verilen karar uygulanır.”* Görüldüğü gibi kanunda bahsedilmeyen çok önemli hususlar, kendilerine bir yönetmelikte yer bulmuşlardır. Dijital delillerin muhafazasını içeren bu hükümlerde dikkat çeken bir nokta, yeterli depolama imkânı olmayan durumlarda ilgili eşyanın satılmasına ilişkin hükümdür. Eğer bu eşya kopyalardan oluşuyorsa içerdikleri verilerin silinmesi halinde bu husus problem yaratmasa da, orijinal eşyanın satılması mülkiyet hakkına ilişkin problem doğurabilir.

Bu konuda bahsedilebilecek bir başka düzenleme ise AÖAY 17’dir. İşbu maddenin başlığı CMK 134 ile aynıdır. Maddenin içeriği de bir cümle hariç 2014 yılında iki kez değişim geçiren CMK 134’ün eski halinin birebir aynısıdır.

⁴¹⁴ Resmi Gazete, Tarih: 01.06.2005, Sayı: 25382.

Yönetmeliğin üçüncü fıkrasına devamında yazılan bu cümle CMK 134'ün üçüncü fıkrasında bulunmamaktadır. İşbu cümle şu şekildedir: “*Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.*”. Burada bahsedilen işlem, yönetmeliğin üçüncü fıkrasından da anlaşılacağı üzere yapılan elkoyma işlemi sırasında verilerin yedeklenmesi işlemidir. Böylece bilgisayar ve bilgisayar kütüklerinin yanı sıra bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımlarına da elkoyulurken verilerin yedeklemesinin yapılması amaçlanmıştır. Ancak özel hayatın gizliliği hakkına müdahale edebilecek böylesine önemli bir hususun kanunda belirtilmeyerek yönetmelik tarafından eklenmesi hukuken son derece sağlıklı bir yaklaşımdır.

ÜÇÜNCÜ BÖLÜM: UYGULAMADA DİJİTAL DELİLLER VE CEZA MUHAKEMESİ BAKIMINDAN KONUYLA İLGİLİ ÇÖZÜM ÖNERİLERİ

Dijital delillere yönelik hukuki düzenlemeleri de inceledikten sonra, hukuki düzenlemelerin uygulamaya nasıl yansıdığı değerlendirilerek ilgili hukuk kurallarının uygulamaya nasıl yansıdığı görülecektir. Bu bölümde mahkeme kararlarının değerlendirmesi yapılacak, böylece uygulamada ne gibi sorunlar veya eksiklik yaşandığı da görülecektir. Hem bir önceki bölümde Türkiye'deki hukuki düzenlemelerin eksikliği hem de mahkeme kararlarında belirlenecek eksiklikler sayesinde ise, gelecekte dijital delillere yönelik ne gibi çalışmalar yapılması gereği de tamamen ortaya çıkacaktır. Böylece ceza muhakemesi hukukunda yapılabilecek yeni düzenlemelerin yol haritasının da çıkarılması mümkün olacaktır.

Bu bölümde öncelikle dijital delillerle ilgili mahkeme kararları incelenecektir. Mahkeme kararları incelemeleri de hukuki düzenlemelerin incelendiği başlıktaki gibi yapılacaktır. Bu durumda öncelikle uluslararası mahkeme kararları incelenecek, daha sonra ise ulusal mahkeme kararları incelenerek karşılaştırmalı inceleme yapılacaktır. Uluslararası mahkeme kararları açısından Türkiye'yi daha yakından ilgilendiren Avrupa İnsan Hakları Mahkemesi (AİHM) ve Avrupa Birliği Adalet Divanı (ABAD) kararları incelenecektir. Ulusal mahkeme kapsamında ise Yargıtay kararları incelenecektir. Tüm bu kararlar incelenirken hem konu ayrımı yapılacak hem de kronolojik sıraya dikkat edilecektir. Böylece konunun daha iyi bir şekilde anlaşılması ve analizi mümkün olacaktır. Ayrıca geçmişten günümüze mahkemelerin verdiği kararlardaki değişim ve özellikle Yargıtay açısından kanunlarda yapılan değişikliklerin yeni kararları ne kadar etkilediği de görülmüş olacaktır.

I. Avrupa İnsan Hakları Mahkemesi kararları

Avrupa İnsan Hakları Mahkemesi (AİHM), uluslararası bir teşkilat olan Avrupa Konseyi'ne bağlı olan, Türkiye'nin de taraf olduğu İnsan Haklarını ve Ana Hürriyetleri Korumaya dair Sözleşme (Avrupa İnsan Hakları Sözleşmesi [AİHS]) ve bu Sözleşme ek protokolleriyle güvence altına alınmış olan temel haklara dair verilen taahhütlerin çiğnenmesi durumunda; bireylerin, bireylerin oluşturduğu toplulukların, tüzel kişilerin⁴¹⁵ ve hatta Sözleşmeye taraf devletlerin⁴¹⁶ belirli usul kuralları⁴¹⁷ dâhilinde başvurabileceği bir yargı merciidir⁴¹⁸. Türkiye'nin de içerisinde bulunduğu Avrupa Konseyi üyesi devletler, AİHM'in yargı yetkisini tanımaktadırlar. AİHM'in içtihadı, Avrupa Konseyi üyesi devletler için temel haklara yönelik asgari standartların belirlenmesi açısından en önemli yol gösterici enstrümanlardan biridir.

AİHM'in dijital delillere yönelik kararlarında dikkat çeken hak ihlalleri, AİHS'in özel hayatın ve aile hayatının korunması başlıklı 8. maddesi⁴¹⁹ ile AİHS'e ek Protokol'ün mülkiyetin korunması başlıklı 1. maddesi⁴²⁰ üzerinedir. 8. madde içerisinde özel yaşam, aile yaşamı ile konut dokunulmazlığı ve haberleşme özgürlüğü

⁴¹⁵ AİHS 34.

⁴¹⁶ AİHS 33.

⁴¹⁷ AİHS 35.

⁴¹⁸ AİHS 19.

⁴¹⁹ Resmi Gazete'de Sözleşme'nin 8. maddesinin Türkçe tercümesi şu şekildedir:

"1. Her şahıs hususi ve ailevi hayatına, meskenine ve muhaberatına hürmet edilmesi hakkına maliktir.

2. Bu hakların kullanılmasına resmî bir makamın müdahalesi demokratik bir cemiyette ancak millî güvenlik, âmme emniyeti, memleketin iktisadi refahı, nizamın muhafazası, suçların önlenmesi, sağlığın veya ahlâkın ve başkasının hak ve hürriyetlerinin korunması için zaruri bulunduğu derecede ve kanunla derpiş edilmesi şartıyla vuku bulabilir.

Sözleşmenin resmi dilleri ingilizce ve fransızca olup Sözleşmenin Türkçe'ye bilgilendirme amacıyla tercüme edilmiş hali AİHM'in resmi internet sitesi "<http://www.echr.coe.int>" içerisinde bulunmaktadır:

"1. Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç şphenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."

⁴²⁰ Ek Protokol 1. maddesinin Resmi Gazete tercümesi:

"Her hakikî veya hükmi şahıs mallarının masuniyetine riayet edilmesi hakkına maliktir. Herhangi bir kimse ancak âmme menfaati icabı olarak ve kanunun derpiş eylediği şartlar ve devletler hukukunun umumi prensipleri dâhilinde mülkünden mahrum edilebilir."

Avrupa Konseyi'nin resmi olmayan çevirisi:

"Her gerçek ve tüzel kişinin mal ve mülk dokunulmazlığına saygı gösterilmesini isteme hakkı vardır. Bir kimse, ancak kamu yararı sebebiyle ve yasadâ öngörülen koşullara ve uluslararası hukukun genel ilkelerine uygun olarak mal ve mülkünden yoksun bırakılabilir."

düzenlenmektedir⁴²¹. Bu noktada kişisel verilerin korunması ile ilgili hususlar ise özel yaşamın mahremiyeti içerisinde kendisine yer bulmaktadır⁴²². Böylece AİHS ile kişisel verilerin korunması hususu, doğrudan olmasa da dolaylı olarak kapsam içerisinde bulunmaktadır. Mülkiyetin korunmasında ise içerik başlığın aynısı olan mülkiyetin korunmasıdır⁴²³.

Bu arada kararları incelemeye geçmeden önce belirtilmesi gereken bir husus vardır. Bu da AİHS'in 8. maddesinden 11. maddesine kadar süren yapısal denetim kurulumudur. Bu kurulum ile bu maddelere yönelik hak ihlalleri AİHM tarafından incelenirken, görüleceği üzere aşamalı bir denetim sistemi kullanmaktadır. Bu noktada mahkemenin uyguladığı beş temel denetim aşaması bulunmaktadır. Burada ilk iki aşama müdahaleyi tespit ederken, diğer üç aşamada müdahalenin hak ihlaline sebebiyet verip vermediği değerlendirilmektedir⁴²⁴.

Bu sistemin işleyişinde, öncelikle başvuruçunun iddiasının madde ile ilgili olup olmadığı, ilgili ise maddede belirtilen özgürlüğe müdahale olup olmadığı ele alınır. Daha sonra ise müdahale varsa bunun kanun tarafından öngörülüp öngörülmediği, müdahale kanunla öngörülmüş ise bunun maddede sayılan meşru amaçlardan birine ya da birkaçına yönelik olup olmadığı ve bu müdahalenin demokratik bir toplum açısından gerekli veya genel olarak orantılı olup olmadığı, değerlendirilir⁴²⁵.

Dijital delillerle ilgili olan AİHM kararlarında hak ihlalleri genellikle bilişim koruma tedbirlerinin uygulanmasında ortaya çıkmaktadır. Dolayısıyla verilen bu gibi mahkeme kararlarının dikkate alınması, dijital delil elde etme faaliyetinin sınırlarının belirlenmesi açısından faydalı olacaktır.

⁴²¹ Philip Leach, **Taking a Case to the European Court of Human Rights**, 3. Edition, Oxford University Press, 2011, s. 314.

⁴²² Pieter van Dijk/Fried van Hoof/Arjen van Rijn/Leo Zwaak, **Theory and Practice of the European Convention on Human Rights**, Fourth Edition, Antwerp: Intersentia, 2006, s. 666 içerisinde özel hayatın gizliliğinin geniş kapsamına kayıtların, tıbbi geçmişin, cinsel tercihlerin, ismin, vücut bütünlüğünün ve kişisel otonominin girdiği belirtilmektedir.

⁴²³ Leach, **a.g.e.**, s. 414.

⁴²⁴ Leach, **a.g.e.**, s. 310 vd. ; Durmuş Tezcan/Mustafa Ruhan Erdem/Oğuz Sancakdar/Rifat Murat Önok, **İnsan Hakları El Kitabı**, 4. Baskı, Ankara: Seçkin Yayıncılık, 2011, s. 276.

⁴²⁵ Leach, **a.g.e.**, ss. 311-313.

Bu noktada kararları incelerken CMK içerisinde yer alan tedbirlere göre bir konu ayrımı yapılarak, kararların Türkiye açısından değerlendirilmesinde bir kolaylık sağlanacaktır. Bu durumda bir önceki bölümde CMK kapsamındaki düzenlemeler başlığında dijital delillere yönelik hukuksal düzenlemeleri incelerken bahsedilen bu yöntemlerden ilki olan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılan arama, kopyalama ve elkoyma tedbirine yönelik birkaç kararla incelemeye başlanabilir.

Bu konudaki dikkat çeken bir karar Petri Sallinen ve diğerleri Finlandiya'ya karşı kararı⁴²⁶dır. Bu olayda bir müvekkilinin sahtecilik suçuna suç ortağı olduğu iddiasıyla avukat olan Sallinen'in bürosunda yapılan arama sonucunda bütün bilgisayar kayıtları incelenmiş ve bir bilgisayara elkoyulurken diğer iki bilgisayardaki veriler ise kopyalanmıştır.

AİHM öncelikle burada bilgisayarlarda bulunan bilgiler nedeniyle özel hayatı ilgilendiren bir müdahale olduğunu tespit etmiştir. Daha sonra yaptığı denetimde ise, iç hukukta düzenleme bulunsa da, bu düzenlemenin kalitesinin AİHS standartlarına uygun olmadığını belirtmiş, kanundaki açık olmayan ifadeler nedeniyle öngörülebilirlik ilkesine uyulmadığını söylemiştir. Ayrıca mevcut olayda müvekkil-avukat güven ilişkisine zarar verildiği ve buna ilişkin koruyucu hükümlerin kanunda düzenlenmediğini tespit etmiştir. Tüm bu nedenlerle AİHS 8. maddenin ihlal edildiğine karar vermiştir⁴²⁷.

Yine bu konudaki bir başka karar Smirnov Rusya'ya karşı kararıdır⁴²⁸. Bu olayda, örgütlü suç işlediği iddiasıyla St. Petersburg barosuna kayıtlı bir avukat olan Smirnov'un bilgisayarında arama yapılmış ve bilgisayarına da elkonulmuştur.

AİHM, konuyla ilgili verdiği kararında Rusya'nın özel hayatın gizliliği başlıklı AİHS'nin 8. maddesi ile mülkiyet hakkı başlıklı AİHS ek Protokolünün 1. maddesini ihlal ettiğine karar vermiştir. Bu ihlal kararlarının gerekçeleri ise 8. madde için, yeterli şüphe sebebi olmadan arama yapılması ve avukatların meslek sırlarının

⁴²⁶ Petri Sallinen and others v. Finland, 50882/99, 27.09.2005.

⁴²⁷ Petri Sallinen and others v. Finland, p. 68 vd.

⁴²⁸ Smirnov v. Russia, 71362/01, 07.06.2007.

saklanmasıyla ilgili olarak kanunda yeterli bir garanti öngörülmemesi iken⁴²⁹; ek Protokol'ün 1. maddesi açısından ise, elkonulan bilgisayarların üzerlerinde yapılan incelemeler sona ermesine rağmen, bilgisayarların adli makamlarca tutulması ve geri verilmemesidir⁴³⁰.

Bu konuda yakın zamanda verilen bir karar olan Prezhdarovi Bulgaristan'a karşı kararı⁴³¹ da bilgisayarlarda yapılan arama ve elkoymalara ilişkindir. Bu olaydaki başvuru evli bir çift olan Rumen Prezhdarov adlı bir Bulgar vatandaşı ile Anna Prezhdarova adlı bir Rus vatandaşıdır. Bu davada mahkeme tarafından incelenen olay, çiftin sahibi olduğu bir bilgisayar topluluğuna yönelik polisin yaptığı arama ve bu arama sonucunda elkoyduğu beş bilgisayara ilişkindir.

İddia makamı tarafından emredilen arama kararı, çiftin müşterilerine kiraladıkları bilgisayarlarında bulunan oyunların, yüklenmesi gerekli olan yazılım lisanslarını almadıkları şüphesi üzerine uygulanmıştır. Soruşturma sırasında bilgisayar programlarını, oyunları ve filmleri içeren beş bilgisayara elkonulmuştur. Prezhdarov bilgisayar programlarının, oyunların ve filmlerin hukuka aykırı bir şekilde dağıtımını yapmaktan ceza almıştır. Bu sırada elkonulan bilgisayarlar, Prezhdarov'un iade talebine rağmen, ceza davası bitene kadar ilgili makamlar tarafından alıkonulmuştur⁴³².

AİHM çiftin iddialarını kabul ederek elkoyulan bilgisayarların kişisel bilgiler içerdiğini ve yapılan elkoymaya karşı etkili bir itiraz yolu veya denetim yolu bulunmadığını tespit etmiş, bunun yanı sıra uygulanan tedbirin orantısız olduğunu ve başvuru sahiplerinin özel hayatına saygı gösterilmediğini belirterek ihlal kararı vermiştir⁴³³.

Mahkeme tarafından bu konuda verilmiş en yeni karar olan Yuditskaya Rusya'ya karşı kararı⁴³⁴ da bilgisayarlarda arama ve elkoymaya ilişkindir. Bu olayda bir rüşvet soruşturmasıyla ilgili olarak yapılan araştırmada bir avukatlık ofisindeki

⁴²⁹ Smirnov v. Russia, p. 41 vd.

⁴³⁰ Smirnov v. Russia, p. 53 vd.

⁴³¹ Prezhdarovi v. Bulgaria, 8429/05, 30.09.2014.

⁴³² Prezhdarovi v. Bulgaria, p. 22 vd.

⁴³³ Prezhdarovi v. Bulgaria, p. 50-51.

⁴³⁴ Yuditskaya v. Russia, 5678/06, 12.02.2015.

tüm bilgisayarlara elkoyulmuş ve bunlardaki bilgiler kopyalanmıştır. Bu bilgisayarlar bir hafta sonra iade edilmişlerdir.

AİHM, konuyla ilgili verdiği kararında Rusya'nın özel hayatın gizliliği başlıklı AİHS'nin 8. maddesini ihlal ettiğine karar vermiştir. Bu ihlal kararının gerekçeleri olarak ise, soruşturmayla ilgisi olmayan bilgilerin kopyalanması yoluyla avukatların meslek sırlarının saklanmasıyla ilgili olarak, aynı Smirnov Rusya'ya karşı davasında olduğu gibi yeterli garantilerin alınmaması⁴³⁵ ve uygulanan tedbirlerin kanun tarafından öngörülmüş olsa da demokratik bir toplum açısından gereklilik sınırlarının ötesine geçtiğini belirtmiştir⁴³⁶.

Dijital delillere yönelik bir diğer bilişim koruma tedbirinin ana başlığı ise iletişimin denetlenmesiydi. Bu tedbirin bilgisayarlarda arama ve elkoymaya göre ilginç yanı, dijital teknolojiler kullanılmadan önceki teknolojilerde de benzer denetimlerin farklı tipte verilerin elde edilmesi hususunda kullanılmasıdır. Bu nedenle bu alandaki içtihat, dijital delillerden daha eskiye dayanmakla birlikte, dijital deliller açısından da kullanılabilir. Zaten iletişim; posta, telefon, faks, e-posta, kişisel internet kullanımı gibi pek çok farklı şekilde yapılabilmektedir. Ancak tüm bu şekiller 8. madde içeriğindedir. Çünkü 8. madde doğrudan haberleşme özgürlüğünü de içermektedir⁴³⁷.

Bu konuda incelenmesi gereken ilk karar bu konuda önemli bir yere sahip Malone Birleşik Krallık'a karşı kararıdır⁴³⁸. Bu olayda yapılan değerlendirmeye göre iletişimin denetlenmesini düzenleyen kanun gizli olamaz. Kanunun kolayca ulaşılabilir olmaması ve detaylı hükümler içermemesi de, yani kalitesinin yetersiz olması da, özel hayatın gizliliğini ihlal eder niteliktedir⁴³⁹.

Konuya ilişkin olarak birlikte incelenmesi gereken Kruslin Fransa'ya karşı kararı⁴⁴⁰ ve Huvig Fransa'ya karşı kararı⁴⁴¹ da önemlidir. Bu iki kararda da sorgu hâkimi kararıyla, şüpheli konumunda olmayan üçüncü bir kişinin konuşmalarının

⁴³⁵ Yuditskaya v. Russia, p. 31.

⁴³⁶ Yuditskaya v. Russia, p. 32.

⁴³⁷ Leach, **a.g.e.**, s. 319.

⁴³⁸ Malone v. UK, 8691/79, 02.08.1984.

⁴³⁹ Malone v. UK, p. 66.

⁴⁴⁰ Kruslin v. France, 11801/85, 24.04.1990.

⁴⁴¹ Huvig v. France, 11105/84, 24.04.1990.

banda kaydedilmesi, özel hayatın gizliliğine müdahale oluşturmıştır. Bu müdahalenin ihlal boyutuna varmasının sebebi ise, o sırada yürürlükte olan kanunun iletişimin denetlenmesine ilişkin gerekli detayları içermemesi olmuştur. Kanunda kimin, hangi koşullar altında iletişiminin denetlenebileceği, denetleme sırasında elde edilen kayıtların nasıl saklanacağı veya nasıl yok edileceği düzenlenmemiştir⁴⁴².

Yine Kopp İsviçre'ye karşı kararında⁴⁴³ kara para aklamaya yönelik bir soruşturma içerisinde avukat olan Kopp ve karısının hukuk firmasının telefon konuşmaları denetlenmiştir. Bu telefon konuşmalarının denetlenmesinde soruşturmaya ilişkin konuşmaların tespiti açısından yapılan dinlemeyi Posta Ofisi'nde görevli bir uzman yapmıştır.

AİHM bu davada AİHS 8. maddesinin açık bir şekilde ihlal edildiğini belirtmiştir. Her ne kadar İsviçre hukuku, avukatların üçüncü kişiler olarak dinlenmesine ilişkin olarak, Kruslin Fransa'ya karşı ve Huvig Fransa'ya karşı kararlarına göre açık ve kaliteli hükümler içerse de, yapılan uygulamanın bu hükümlerle açıkça çeliştiği gerçeği de ortadadır. Ayrıca bu davada ilgili tedbirin uygulanmasında herhangi bir bağımsız hâkim denetiminin olmaması ve tedbirin idarenin bir parçası olan Posta Ofisi'nde görevli bir kişi tarafından uygulanmasının yanlışlığı ortaya konmuştur⁴⁴⁴.

Bu konuda dikkat çeken kararlardan bir diğeri Craxi İtalya'ya karşı kararıdır⁴⁴⁵. Bu olayda, İtalya'nın eski başbakanı olan Craxi aleyhine hakkında yolsuzluk yaptığı iddiasıyla “temiz eller” adıyla bir operasyon başlatılmıştır. Bu soruşturma sırasında yapılan Craxi'nin telefon görüşmelerinin dinlenerek kayıtları tutulmuş, kayıtlar daha sonraki aşamada da mahkemeye savcı tarafından sunulmuştur. Savcı tarafından sunulan ve aleniyet kazanan bu kayıt içerikleri, böylece basında da kendilerine yer bulmuşlardır.

AİHM konuyla ilgili verdiği kararında, İtalya'nın özel hayatın gizliliği başlıklı AİHS 8. maddesini ihlal ettiğine karar vermiştir. Bu ihlal kararının

⁴⁴² Kruslin v. France, p. 36; Huvig v. France, p. 35.

⁴⁴³ Kopp v. Switzerland, 23224/94, 23.03.1998.

⁴⁴⁴ Kopp v. Switzerland, p. 72 vd.

⁴⁴⁵ Craxi v. Italy (No.2), 25337/94, 17.07.2003.

gerekçesinde basının haber verme hakkı ile özel hayatın gizliliğini karşılaştıran AİHM, elde edilen özel ve davayla ilgili olmayan bilişim verileri ile telefon konuşmalarının duruşmada delil olarak okunmasını ihlale neden olarak göstermiş, bunların basında yayınlanmasının basın özgürlüğü kapsamına girmediğini belirtmiştir⁴⁴⁶.

Bu konuda Türkiye’yi ilgilendiren önemli bir karar Ağaoğlu Türkiye’ye karşı kararıdır⁴⁴⁷. Mülga CMUK’un yürürlükte olduğu dönemde dijital delillerin elde edilmesine yarayan hükümlerinin olmadığından daha önce de bahsedilmişti. Bu davadaki olayda, CMUK’un mektup, telgraf vesair mersulelerin zaptı hükümleri kıyasen uygulanmak suretiyle iletişimin denetlenmesi tedbirine başvurulmuştur.

AİHM, söz konusu uygulama ile başvurucunun AİHS 8. madde ile güvence altına alınan özel hayatının gizliliği hakkının ihlal edildiğine karar vermiştir. Buna gerekçe olarak ise, mevcut kanun hükümlerinin gerekli güvenceleri sağlamadığını, dolayısıyla bu yolla elde edilen delillerin hukuka aykırı olacağını belirtmiştir. Ayrıca bu tedbirin uygulanması, kişiler tarafından hukuken öngörebilir değildir denilmiştir⁴⁴⁸.

Kennedy Birleşik Krallık’a karşı kararındaki⁴⁴⁹ olayda başvuru geçmişte pek çok tartışmanın da yaşandığı bir dava süreci sonunda adam öldürmeden ceza alan, ancak bir süre hapis cezasını çektikten sonra serbest bırakılan bir kişidir. Salındıktan sonra adli hatalara karşı mücadelelere yönelik etkinliklere yoğun bir şekilde katılmıştır. Bu durumun sonrasında ise meydana gelen bazı şüpheli durumlardan yola çıkarak, iletişiminin denetlendiğine dair bir kuşku duymuş ve ilgili kurumlara bu konuda bilgi edinmek için başvurularda bulunmuştur. Bu konuda beklediği cevabı alamaması üzerine ise yapılan denetimin hukuka aykırı olduğu gerekçesiyle dava açmıştır.

AİHM bu olayda 8. maddede belirlenen hakka bir müdahale olduğunu, ancak müdahaleye neden olan kanunun ulusal güvenliğin ve ekonomik düzenin korunması

⁴⁴⁶ Craxi v. Italy (No.2), p. 60 vd.

⁴⁴⁷ Ağaoğlu v. Turkey, 27310/95, 06.12.2005.

⁴⁴⁸ Ağaoğlu v. Turkey, p. 53 vd.

⁴⁴⁹ Kennedy v. UK, 26839/05, 18.05.2010.

ile suçların önlenmesi gibi meşru amaçlara sahip olmasının önemine değinmiştir. Bunun yanı sıra konuyu düzenleyen RIPA'nın internet üzerinden erişilebilir olduğunu ve kimin iletişiminin ne zaman denetlenebileceğine ilişkin açık hükümlere sahip olduğunu belirtmiştir⁴⁵⁰. Ayrıca uygulanan RIPA hükümlerinin yasama ve yürütme erkinden bağımsız bir görevli tarafından başbakan ve parlamentoya rapor olarak sunulmasının kanunun doğru şekilde uygulandığına dair iyi bir güvence olduğunu belirtmiştir. Ayrıca tedbirin belirlenen kurallar dâhilinde uygulandığı ve bu uygulamada herhangi bir kusur bulunduğuna dair delil olmadığı için 8. maddeye yönelik bir ihlalin bulunmadığına karar verilmiştir⁴⁵¹.

İletişimin denetlenmesine ilişkin güncel bir karar olan Dragojevic Hırvatistan'a karşı kararında⁴⁵² ise uyuşturucu ticareti yapıldığı şüphesiyle telefonları dinlenen Dragojevic'e dair yapılan dinlemelere ilişkin kararların alınması aşamasında usule uyulup uyulmadığına dair bir tartışma söz konusu olmuştur. Başvurucu Dragojevic davasına temel oluşturan bu kayıtların hukuka aykırı olduğundan bahisle bu kayıtların dosya kapsamı dışında bırakılmasını talep etse de, mahkeme bu kayıtlara da dayanarak başvuru hakkında mahkûmiyet kararı vermiştir.

AIHM, olayda başvurunun AIHS 6. madde ile güvence altına alınan adil yargılanma hakkının ve 8. madde ile güvence altına alınan özel hayatının gizliliği hakkının ihlal edildiğine karar vermiştir. 8. madde ihlaline gerekçe olarak ise, kanunlardaki hükümlerin, uygulamadaki kötüye kullanmalara engel olmaktan uzak olduğunu ve olaydaki iletişimin denetlenmesi sebeplerinde hukuk kurallarına uygunluğun bulunmadığı ifade edilmiştir⁴⁵³.

AIHM tarafından alınmış kararlardan bir diğerinde⁴⁵⁴ bir başka dijital delil elde etme yöntemi olan teknik takip söz konusudur. Ancak bu karar iletişimin denetlenmesi ile teknik takip arasındaki ilişki açısından da önemlidir. Türkiye'de teknik araçlarla izleme tedbiri, yalnızca ses ve görüntü kaydına yönelik tanımlandığı için mobil telefon yeri tespiti gibi bir uygulamanın içerisinde bulunmadığı ve bu

⁴⁵⁰ Kennedy v. UK, p. 159 vd.

⁴⁵¹ Kennedy v. UK, p. 166.

⁴⁵² Dragojevic v. Croatia, 68955/11, 15.01.2015.

⁴⁵³ Dragojevic v. Croatia, p. 101.

⁴⁵⁴ Uzun v. Germany, 35623/05, 02.09.2010.

uygulamanın dolaylı olarak sinyal bilgilerinin değerlendirilmesi tedbiri içerisinde yapıldığı söylenebilir.

Bu olayda terör suçu şüphelisinin kamusal alandaki hareketleri Global Konumlandırma Sistemi (*Global Positioning System [GPS]*) aracılığıyla takip edilmektedir. Öngörülebilirlik ve kanunla belirlenme kriterlerini de dikkate alan AİHM; GPS takibinin, daha sıkı kuralların uygulandığı telekomünikasyon yoluyla iletişimin denetlenmesine göre kişilerin özel yaşamına daha az müdahale eden bir tedbir olduğundan bahisle özel yaşamın gizliliği hakkının ihlal edilmediğine hükmetmiştir⁴⁵⁵.

II. Avrupa Birliği Adalet Divanı kararları

Avrupa Birliği Adalet Divanı (*Court of Justice of the European Union [CJEU]*), AB'nin yargı organıdır. Bu organ Adalet Divanı (*European Court of Justice [ECJ]*), Genel Mahkeme (*General Court*) ve Kamu Hizmetleri Mahkemesi (*Civil Service Tribunal*) olmak üzere üçlü bir yapıdan oluşmaktadır⁴⁵⁶. Adalet Divanı'nın temel amacı, AB hukukunun birlik içerisinde her yerde aynı şekilde yorumlanmasını ve uygulanmasını sağlamaktır. Bu temel amaca ulaşmak için AB hukukunun yorumlanmasında ve uygulanmasında hukuka saygıyı sağlama, ulusal hukuk düzenleri ile AB hukuk düzeni arasındaki ilişkilerin düzenlenmesi, hukuki denetim, yorum, uyuşmazlık çözme, hukuk yaratma ve boşluk doldurma işlevlerini yerine getirir⁴⁵⁷.

AB düzenlemelerinin, AB üyelerinin ceza hukukunda birbirleriyle olan işbirliğine ilişkin kısmında geri kalmasının nedenleri daha önce belirtilmişti⁴⁵⁸. Dolayısıyla ceza muhakemesinde dijital delil konusu da AB içerisindeki düzenlemelerde yeterince yer almamaktadır. ABAD'nin yargı yetkisi de AB düzenlemeleriyle sınırlı olduğu için bu konuya ilişkin pek fazla karara rastlanmamaktadır. Ancak yine de AB'nin dijital delillere yönelik yaptığı çalışmalar

⁴⁵⁵ Uzun v. Germany, p. 77 vd.

⁴⁵⁶ Court of Justice of the European Union, http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm. (Erişim tarihi: 11.03.2015)

⁴⁵⁷ Avrupa Birliği Bakanlığı, **Avrupa Birliği: Kurumlar**, http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_2_kurumlar/ab_kurumlar.pdf. (Erişim tarihi: 11.03.2015)

⁴⁵⁸ Bkz. s. 69.

içerisinde de belirtildiği üzere, bu konuyu ilgilendiren bazı düzenlemeler de mevcuttur⁴⁵⁹. İşbu düzenlemelere ilişkin başvurularda, AB'nin bu konudaki en üst yargı makamı olan ABAD bazı önemli kararlar vermiştir. Ancak bu düzenlemelere yönelik kararlar içerisinde dijital delillerle en ilişkili kararlar, AB hukuku kapsamında da temel hak olarak görülen özel hayata saygı ve kişisel verilerin korunması kapsamında verilmiştir. ABAD'ın dijital deliller konusunda AİHM kadar yoğun bir gündemi ve çok sayıda kararı bulunmasa da bu konudaki az sayıdaki kararının da incelenmesi gerekir.

ABAD tarafından verilen kararlara genel olarak bakıldığında, AB hukuku kapsamında bulunan mahremiyete yönelik hakların AİHM'e göre daha geniş kapsamda korunduğu söylenebilir. Nitekim AİHM özel hayatın gizliliği ve ulusal güvenlik meseleleri arasındaki denge açısından AİHS'e taraf devletlere bir takdir payı (*margin of appreciation*) bırakabilmektedir⁴⁶⁰. Bu nedenle ABAD'ın daha özgürlük yanlısı kararlar verdiği belirtilmektedir.

Özel hayata saygı ve kişisel verilerin korunması kapsamında ABAD'ın verdiği kararlara göz atıldığında ilk olarak dikkat çeken karar⁴⁶¹ 2003 yılında verilmiş bir karardır. Bu karar ABAD'ın 1995 tarihli Veri Koruma Direktifi kapsamında olup, verilerin internet üzerindeki hareketlerine ilişkin verdiği ilk karardır.

İşbu karar içerisindeki olaylar şu şekilde gerçekleşmiştir: İsveçli bir vatandaş olan Lindqvist, yaptığı gönüllü işe ilişkin bir internet sitesi kurmuş ve içerisinde kendisi ile birlikte bu işi gönüllü yapan diğer kişilerin de bazı kişisel bilgilerini paylaşmıştır. İzin almadan yaptığı bu eyleme ilişkin olarak kişisel bilgileri paylaşılan kişilerden de gelen tepkiler üzerine, Lindqvist ilgili internet sitesini tamamen kaldırmıştır. Ancak ilgili kurumlar tarafından yapılan araştırmalar sonucunda, bu durumun izinsiz bir şekilde kişisel verilerin işlenmesi fiilini oluşturmasından yola çıkılarak Lindqvist yargılanmıştır. Bu noktada ABAD'ın önüne gelen dosyada, çeşitli kişilerin internet üzerinden isimleri veya kendilerine ilişkin kişisel veri niteliğindeki

⁴⁵⁹ Bu düzenlemeler için bkz. s. 69 vd.

⁴⁶⁰ Federico Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.", Tilburg Law School Research Paper No. 15/2014, ss. 5-6.

⁴⁶¹ C-101/01 – Lindqvist.

herhangi bir veriye atıfta bulunulmasının AB hukuku ve Veri Koruma Direktif'i kapsamında bulunacağına, dolayısıyla bu kapsamda da korunacağına dair önemli bir karar verilmiştir.

ABAD'ın bu konuda verdiği bir diğer önemli karar⁴⁶² ise telekomünikasyon sektörüne ilişkin olarak özel hayatın korunması ve kişisel verilerin işlenmesine ilişkin olarak 1997 yılında çıkarılan Direktif'e aykırı düzenleme yapılmasına ilişkindir. Bu kararda Hollanda tarafından yapılan Telekomünikasyon Kanunu'nun, Direktif'in trafik ve faturalama verileri başlıklı 6. maddesi ile istisnalar başlıklı 9. maddesi içeriğine uygun olarak düzenlenmediği kararına varılarak, Hollanda'nın AB hukukundan doğan yükümlülüklerini yerine getirmediğine ve ihlal ettiğine karar verilmiştir.

Yine bu konuda verilen bir başka kararda⁴⁶³ bu sefer Almanya'daki hukuki düzenlemeler tartışma konusu olmuştur. Almanya'da 3 aydan fazla süredir ikamet eden gerek AB vatandaşı gerek AB vatandaşı olmayan tüm yabancıların belli kişisel verileri (Bu veriler isim, doğum yeri, doğum zamanı, cinsiyeti, uyruğu gibi sıradan bilgilerin yanı sıra ciddi suçlara ilişkin sabıka kaydı gibi bilgileri de içermektedir.) bir merkezi sistemde kayıtlı tutulmaktadır. Bu verilerin ikametle ilgili, istatistiksel ve suçla mücadele amaçlı tutulduğu belirtilse de Alman vatandaşlarına ilişkin böyle bir uygulama bulunmamaktadır. Bu durumun ayrımcılık yarattığını düşünen bir Avusturya vatandaşı olan Huber, kendisi ile ilgili verilerin sistemden silinmesini talep etmiştir. Bu talebi kabul görmeyince dava açan Huber'in dosyası ABAD önüne kadar gelmiştir. ABAD bu davadaki değerlendirmesini kişisel verilerin depolanmasındaki üç amaç üzerinden yapmıştır.

Verilerin ikametle ilgili olarak tutulmasına ilişkin yapılan değerlendirmede, AB vatandaşı da olsa her yabancının başka bir ülkede ikamet hakkına sahip olması için bazı kısıtlamalara tabi tutulabileceğini ve bunun Veri Koruma Direktifi'nde belirtilen gerekliliği oluşturabileceğini belirtmiş, bu kısıtlamanın ulusal çapta ve kanunla yapılmasının amaca uygun olduğunu ortaya koymuştur. Ancak verilerin istatistiki olarak tutulmasının Veri Koruma Direktifi'nde belirtilen gereklilik kapsamını aştığını, elde edilen bilgilerin nüfus hareketlerini gözlemlemekten daha

⁴⁶² C-350/02 – Commission v Netherlands.

⁴⁶³ C-524/06 – Huber.

fazlasını içerdiğini belirtmiştir. Suçla mücadeleyle ilişkin olarak ise, yabancıların ceza adaletine ilişkin hususlarda ülkenin kendi vatandaşlarından farklı bir muamele görmeleri gereği ortaya koyularak, benzer yükümün Alman vatandaşlarından istenmemesinin vatandaşlığa bağlı ayrımcılık yaratabileceği belirtilmiştir. Bu hususun ise doğrudan Maastricht Antlaşması'nın ayrımcılık yasağına ilişkin 12. maddesine aykırılık oluşturacağına hükmedilmiştir.

Bu konudaki bahsedilmesi gereken bir önemli konu da Veri Koruma Direktifi'nin 28. maddesinin 1. fıkrası gereği kurulması zorunlu tutulan kişisel verilerin işlenmesi ve korunmasını denetleyen kurumlara ilişkin kararlardır⁴⁶⁴. Üç kararda da ilgili denetim kurumlarının işleyişlerinin bağımsız yapıya sahip olması gereği üzerinde durulmuştur. Almanya'da bu durum eyaletlere kurulan ilgili kurumların kanunlar aracılığıyla devlet denetimine tabi olması nedeniyle, Avusturya'da ilgili kurumun hizmet açısından yürütmeye olan yakın ilişkisi nedeniyle, Macaristan'da ise ilgili kurumun başkanının görev süresi bitmeden parlamento tarafından değiştirilmesi nedeniyle Direktif'e ve dolayısıyla AB hukukuna aykırılık oluşmuştur.

Bir başka kararda⁴⁶⁵ ise ABAD, Hollanda vatandaşı olan Rijkeboer'in kendisine ilişkin kişisel verileri kayıt altında tutan kurumdan, bu verilere dair öğrenmek istediği bilgiye geç ve tam olarak ulaşamaması üzerine, Veri Koruma Direktifi'nin kişilerin kendilerine ait verilere erişim hakkını düzenleyen 12. maddesinin ihlal edildiğine hükmetmiştir.

ABAD'ın yine dijital delilleri ilgilendirebilecek ses getiren bir kararı⁴⁶⁶ ise unutulma hakkına (*right to be forgotten*)⁴⁶⁷ ilişkin olarak verilmiştir. 2010 yılında bir İspanyol vatandaşının şikâyeti üzerine açılan davada; Google arama motoruna şikâyetçinin ismi yazılınca, geri alma yoluyla yeniden mülkiyetine sahip olduğu bir malın açık arttırma ilanının Google arama sonuçları içerisinde çıkmasının kendisinin mahremiyete ilişkin haklarını etkilediğini belirtmiştir. Yıllar önce halledilmiş bir

⁴⁶⁴ Bu konuda verilmiş üç karar bulunmaktadır.

C-518/07 - Commission v Germany

C-614/10 - Commission v Austria

C-288/12 - Commission v Hungary

⁴⁶⁵ C-553/07 – Rijkeboer.

⁴⁶⁶ C-131/12 - Google Spain and Google.

⁴⁶⁷ Veri Koruma Direktifi'nin 12. maddesi bu hakkın yasal kaynağını oluşturmaktadır.

meseleye yönelik ilanının ilgili gazetenin sayfasından çıkarılmasının yanı sıra Google arama sonuçlarından da kendisiyle ilgili kişisel verilerin çıkarılması istemi davanın konusunu oluşturmaktadır.

Burada İspanyol yargı makamları tarafından konu ABAD'a taşınmıştır. ABAD yaptığı inceleme sonunda verdiği kararda öncelikle bu konunun AB hukukunun ilgilendirdiğini tespit etmiştir. Nitekim sunucusu fiziksel olarak AB içerisinde bulunmasa da Google şirketinin AB içerisinde bulunan şubeleri aracılığıyla AB içerisinde işlem yapma kabiliyeti bulunduğu belirtilmiştir. Ayrıca internet arama motorları doğrudan kişisel verileri kontrol etme üzerine kurulu bir sistem olduğu için, bu konudaki sorumluluktan da kaçamayacaklardır. Bunlara ek olarak kişilerin kendilerine ait kişisel verilerin unutulma hakkı kapsamında kaldırılmasını talep etmelerinde bir sıkıntı bulunmamaktadır. Ancak bu durumda kaldırılması istenen bilginin verilerin işlenmesi açısından yanlış (*inaccurate*), eksik (*inadequate*), ilgisiz (*irrelevant*) veya aşırı (*excessive*) olması gereklidir⁴⁶⁸. Nitekim unutulma hakkının da sınırları ifade ve medya özgürlüğü gibi temel haklarla olan dengesine göre çizilecektir⁴⁶⁹.

Sonuç olarak görüldüğü üzere bu karar ile internet arama motorlarının kişisel verileri işlemeden dolayı sorumlulukları bulunduğu belirtilmiştir. Arama sonucunda ekrana gelecek sayfaların belirlenmesinde, üçüncü kişilere ait sayfalarda bulunan kişisel verilerin işlenmesi ile bir sıralama oluşturulduğuna karar verilmiştir. Bu nedenle aynı şekilde ilgili bağlantıların arama motorunda çıkmamasından da yine internet arama motorları sorumlu olacaklardır. Bu durumda kişisel veri içeren bağlantıların yayından çıkarılması için internet arama motoruna doğrudan başvurulabilecektir.

Konuyla ilgili bir diğer kararda⁴⁷⁰ ise, pasaportlarda parmak izi bulunması zorunluluğu getiren düzenleme tartışma konusu olmuştur. ABAD tarafından yapılan değerlendirmede bu hususun, her ne kadar özel hayata saygı ve kişisel verilerin korunması haklarına bir müdahale teşkil etse de sahte pasaport kullanımının engellenmesi açısından gerekçelendirilebileceğini belirtmiştir. Bu nedenle AB'ye

⁴⁶⁸ C-131/12 - Google Spain and Google, p. 93.

⁴⁶⁹ C-131/12 - Google Spain and Google, p. 85.

⁴⁷⁰ C-291/12 – Schwarz.

hukuka aykırı bir şekilde girmeyi engelleyecek bu tedbirin, amacına uygun yoğunlukta olduğunu belirtmiştir.

Bir başka kararda⁴⁷¹ ise vatandaşların kendileri ile ilgili olarak tutulan kişisel verilere ilişkin kayıtlara dair alacakları dökümlerin ücretlendirilmesi tartışılmıştır. Bu konuda ücretlendirmeye dair herhangi bir yasak olmadığını belirten ABAD, yine de belirlenen ücret miktarının da kişilerin verilere erişimini engelleyecek derecede yüksek olmaması gerektiğini belirtmiştir.

Yine konuyla ilgili bir diğer kararda⁴⁷² ise, Veri Koruma Direktifi'nin evlere güvenlik amaçlı yerleştirilen ve kamusal alanı video olarak kaydeden görüntülere uygulanıp uygulanamayacağı tartışılmıştır. Bu noktada öncelikle görüntülenen kişilerin tanınmasına yol açtığı için görüntülerin kişisel veri niteliği taşıdığı belirlenmiştir. Daha sonra ise özel mülkiyete konu alan açısından alınacak görüntülerin istisna oluşturabileceğini, ancak kamusal alana yönelik çekimlerin bu kapsamda sayılamayacağını tespit etmiştir.

Bu konuda ABAD tarafından yakın dönemde verilen ve dijital çağda özel hayatın ve verilerin korunması açısından adeta sembol karar haline gelen bir karardan⁴⁷³ da mutlaka bahsetmek gereklidir. Nitekim bu karar; insan hakları alanında çağımızın en çok konuşulan konularından biri olan ve yapılan düzenlemelerde ilk olarak aranan özgürlük-güvenlik dengesinin özgürlük lehine bozulmasını sağlayacak önemli bir karardır⁴⁷⁴.

Kararın konusu, 2012 yılında İrlanda Yüksek Mahkemesi ve Avusturya Anayasa Mahkemesi'nin başvurusu üzerine değerlendirilen, iletişimin kaydedilmesi kapsamında internet servis sağlayıcılarına belli trafik verilerini saklama yükümü getiren Veri Saklama Direktifi'nin AB Temel Haklar Bildirgesi'nin 7, 8 ve 11. maddelerine aykırı olup olmadığı üzerinedir.

⁴⁷¹ C-486/12 – X.

⁴⁷² C-212/13 – Ryneš.

⁴⁷³ Joined Cases Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others.

⁴⁷⁴ Fabbrini, **a.g.e.**, s. 19.

Aralık 2013'te Türkçe'ye Umumi Vekil (*Advocate General*) olarak çevrilebilecek, kendisi ne avukat ne de hâkim olan, ama davaya ilişkin hukuki görüşünü mahkemeye sunmakla görevli kişi olan davanın Umumi Vekili Cruz Villalón'un görüşleri mahkemeye sunulmuştur. Bu görüşler karar vermede mahkemeyi bağlayıcı olmasalar da dikkate alınmaktadırlar⁴⁷⁵. Villalón öncelikle AB Temel Haklar Bildirgesi'ndeki özel hayata saygı ile verilerin korunması arasındaki farka değinerek, özel hayata saygı hakkının olayla ilgili olarak daha geniş bir perspektif sunduğunu belirtmiştir. İşbu hakların kısıtlanmasının şartlarını içeren AB Temel Haklar Bildirgesi'nin 52. maddesi ile Veri Saklama Direktifi'nin birbirine aykırılık içerdiğini, bu nedenle Direktif'in özel hayata saygı hakkını ihlal ettiğini görüş olarak sunmuştur⁴⁷⁶.

Kararın verilme aşamasında ABAD'ın yaptığı incelemede AB Temel Haklar Bildirgesi'nin 7, 8 ve 11. maddelerinin Veri Saklama Direktifi'nin geçerliliği ile ne açılardan çatışabileceğini dikkate almıştır. Davada Veri Saklama Direktifi'nde özel hayata müdahale sebepleri olarak yer alan kamu yararı, ciddi suçların önlenmesi ve terörle mücadelenin orantısının tartışıldığı görülmüştür. Sonuç olarak verilen karara göre, Veri Saklama Direktifi'nin yapılmasında AB yasama erkinin orantılılık sınırlarını aşmış olduğu, bu nedenle Direktif'in hükümsüz olduğu belirtilmiştir⁴⁷⁷. ABAD'a göre bu Direktif; AB Temel Haklar Bildirgesi ile garanti altına alınan kişisel verilerin korunması ve özel hayata saygı haklarına ciddi bir müdahalede bulunmaktadır. Üstelik bu müdahale gerçekleşirken ne yargı erki tarafından yapılan yargısal bir denetimin, ne de bağımsız bir idari otoritenin idari bir denetimin bulunduğu söylenebilecektir. Bu nedenle Direktif başlangıcından itibaren (*ab initio*) hükümsüz olup, Direktif'i hukuk sistemlerine aktaran üye devletlerin ABAD'ın kararına uymalarının beklendiği belirtilmiştir⁴⁷⁸.

Bu arada son dönemde epeyce tartışılan hususlardan biri olan AB'nin AİHS'e taraf olması meselesi de AB yürütme organı olan Avrupa Komisyonu'nun başvurusu

⁴⁷⁵ Fabbrini, **a.g.e.**, s. 14.

⁴⁷⁶ Fabbrini, **a.g.e.**, s. 14.

⁴⁷⁷ Joined Cases Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, p. 69.

⁴⁷⁸ Joined Cases Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, p. 71.

üzerine, ABAD tarafından değerlendirilmiştir⁴⁷⁹. İşbu görüş bildiriminde ABAD, AB'nin, kendisini oluşturan üye ülkelerden ayrı bir yapı olarak AİHS'ye taraf olmasının AB'nin kendi yasalarına aykırı olduğuna hükmetmiştir. Buna ek olarak AİHS'ye taraf olmanın AB'nin temelindeki dengelere ve AB yasalarının özerk yapısına zarar vereceğini belirtmiştir. Bu görüş sadece dijital deliller açısından değil hukukun her alanı açısından son derece önemlidir. Nitekim ABAD tarafından mevcut düzenin devamına ilişkin bir görüş bildirilmiştir. Böylece ABAD ile AİHM arasında oluşabilecek yargı yetkisi tartışmasının da geçici bir süre için önüne geçilmiştir.

III. Türkiye'deki mahkeme kararları

Dijital delillere ilişkin Avrupa İnsan Hakları Mahkemesi ve Avrupa Birliği Adalet Divanı kararlarını inceledikten sonra, Türkiye'de gerek Yargıtay'ın gerekse Anayasa Mahkemesi'nin dijital delillere karşı nasıl bir hukuki yaklaşım gösterdiği değerlendirilecektir. Türkiye'deki mahkemeler açısından dijital delillerin yeni bir konu olmasıyla birlikte, yine de bu konuda inceleme yapabilmek için yeterli düzeyde içtihat bulunduğu da yadsınamaz.

Türkiye'de dijital delillerin tartışma konusu yapıldığı pek çok dava bulunmakla birlikte, bu konu Balyoz güvenlik harekât planı davası ile kamuoyu gündeminde daha geniş bir biçimde yer bulmuştur. O yüzden öncelikli olarak Balyoz güvenlik harekât planı davası, daha sonra ise diğer başka örnek davalar incelenecektir.

A. Balyoz güvenlik harekât planı davası

Türkiye'de daha önce pek çok davada dijital delillere yönelik kararlar verilmiş olsa da kamuoyunda en büyük yankıyı uyandıran ve belki de bu alandaki tartışmaları yeniden alevlendiren dava hiç kuşkusuz ki budur. Hükümete karşı işlenen suç⁴⁸⁰ iddiası üzerine temellendirilerek açılan davada ceza hukuku açısından pek çok tartışmalı kısım olsa da, konu dışına çıkmamak adına, bu davaya ilişkin olarak yalnızca dijital delillere yönelik tartışmalar incelenecektir.

⁴⁷⁹ Opinion 2/13, Opinion pursuant to Article 218(11) TFEU.

⁴⁸⁰ 5237 sayılı TCK 312, 765 Sayılı TCK 171.

İlk derece mahkemesinde dava görülürken dijital delillere ilişkin pek çok tartışma su yüzüne çıkmıştır. Bu tartışmalar davayla ilgili Yargıtay kararı ve Anayasa Mahkemesi kararı ile özetlenmiş bulunmaktadır. Bu yüzden konuyu uzatarak detaylandırmak yerine Yargıtay kararı ve Anayasa Mahkemesi kararının dijital delillere yönelik değerlendirmeleri üzerinden bir inceleme yapılacaktır.

Yargıtay kararında⁴⁸¹ usul yönünden yapılan incelemenin delillere ilişkin kısmı, davada delil tartışmasının yapılmadığı ve bir kısım tanıkların dinlenmediği iddiaları üzerinedir.

Kararda usul tartışmasının yanı sıra dijital delillere yönelik genel bir değerlendirmeye de yer verilmiştir. Yargıtay, yaptığı genel değerlendirmeye şu şekilde başlamaktadır: “*Dijital delillerin yapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital deliller de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestisinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, ceza muhakemesi hukukunda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi hususlar gözetilip, özel olarak da; delilin temsil ettiği olayın niteliği, ele geçiriliş yeri, şekli ve zamanı, bu delilin sair karakteristik özellikleri gibi hususlar göz önünde bulundurulmalıdır.*” Burada dijital delillere ilişkin yapılan güzel tespitler bulunmaktadır. Dijital delillerin kolaylıkla değiştirilebildiği, ancak sonuç olarak delil özelliklerine sahip dijital delillerin de delil olarak kabul edilmesinde delil serbestisini benimseyen bir sistem açısından sorun olmadığı belirtilmiştir. İspat açısından ise delilin öncelikle ceza muhakemesinde belirtilen genel özelliklere sahip olup olmadığı araştırıldıktan sonra, kendine has özelliklerinin değerlendirilmesi gerektiği ortaya konulmuştur. Böylece dijital delillerin de ceza yargılamasında aynı klasik deliller gibi normal olarak kullanılabileceği ortaya konmak istenmiştir.

Değerlendirmenin devamında; “*...Dijital deliller de, kimyasal, biyolojik ve benzeri diğer tüm deliller gibi sanıklar ya da başkaları tarafından çeşitli şekillerde*

⁴⁸¹ Yargıtay 9. CD, E. 2013/9110, K. 2013/12351, T. 09.10.2013.

gizlenmeye, değiştirilmeye, bozulmaya elverişlidir. Sanıklar veya başkaları tarafından delillerin yok edilme, silinme, gizlenme, değiştirilme veya bozulmak istenmesi o kadar olağandır ki; yasa koyucu maddi gerçeğin ortaya çıkarılabilmesi bakımından büyük bir tehlike oluşturan bu fiilleri ayrı bir suç olarak veya nitelikli hal olarak düzenlemiştir...” denilmiştir. Böylece dijital delillerin değişime, bozulmaya ve yok edilmeye bu kadar elverişli olmalarının, delillerin rahatlıkla karartılabilmesini de mümkün kıldığı ortaya konulmuştur. Bu noktaya kadar dijital delillere ilişkin yapılan değerlendirmelerde herhangi bir sıkıntı bulunmamaktadır.

Sonra yapılan değerlendirme ise, “...Ancak, dijital delillerin değiştirilebilme kolaylığı ve sanal oluşundan hareketle hükme esas alınamayacak olduğunun ileri sürülmesi delil olgusuna aykırıdır. Kaldı ki, dijital deliller Türk ceza muhakemesi sisteminde ilk kez bu dava ile gündeme gelmiş olmayıp, geçmişte de pek çok davada tartışılmış ve hükme esas alınmıştır...” şeklindedir. Böylece dijital delillerin de hükme esas alınabileceği belirtilmiştir. Hatta bu kısmın devamında bu konuya örnek olarak bazı Yargıtay kararları örnek gösterilmiştir.

Verilen örneklerde dijital delillerin sahteliğine yönelik ileri sürülen itirazların, nasıl değerlendirildiği şu cümle ile ortaya konulmuştur: “*Bu davalarda da, dijital delillerin içeriğine, içerik çelişkilerine, saklanma biçimine ve teknik yönüne dair ileri sürülen itirazlar, delillerin ele geçiriliş şekli, bütünlüğü, birbirlerini doğrulaması, somut olgulara karşılık gelmesi, hayatın olağan akışı ve tüm dosya kapsamı ile birlikte değerlendirilmiş ve dijital deliller mevcut halleriyle ve taşıdıkları delil değerleri ölçüsünde hükme esas alınmıştır.*”

Daha sonra konuyla ilgili mevcut olaya dönülerek, dijital delillere ilişkin sahtecilik iddiaları iki ana başlık altında toplanmıştır. Dijital delillerle ilgili olarak ileri sürülen iddiaların, kolluk veya adli makamlarca bu delillerin ele geçirilmesinden önceki aşamaya ve sonraki aşamaya ilişkin olmasına göre bu ayırım yapılmıştır. Sonraki aşamaya ilişkin olarak iki iddia değerlendirilmiştir.

Bunlardan ilki; “*Gazeteci tarafından teslim edilen CD'lerden 9 nolu CD'nin 29.01.2010 tarihli teslim alma ve el koyma tutanağına "Vatandaşlık Taslak" ve yeşil kalemle 67 yazılı Sony marka CD ibaresiyle kayda geçirilmiş olmasına rağmen,*

CD'lerin bilirkişiyeye teslimine ilişkin 01.02.2010 tarihli tutanakta aynı CD'nin markasız marka ve "İrticai Unsurlar Aşırı Sol Unsurlar" CD no 67 olarak kayda geçirildiği ve bu hususun 9 nolu CD'nin Cumhuriyet savcılığı aşamasında değiştirilmiş olduğunu gösterdiği iddiasının gerçeği yansıtmadığı, bu iddianın, CD'lere el konulması sırasında 9 nolu CD'nin plastik muhafaza kabı üzerinde yazılı olan marka ve isimlendirme ile kayda geçirilmesi, CD'lerin bilirkişiyeye teslimine ilişkin tutanakta ise kapsız haldeki 9 nolu CD'nin üzerinde yazılı olan isimlendirmenin kayda geçirilmiş olmasından kaynaklandığı, bu durumun 9 nolu CD'nin kendisi ve muhafaza kabı üzerinde yapılan basit bir incelemeyle anlaşıldığı, iddia konusu hususun gazeteci tarafından teslim edilen 19 adet CD'nin tamamı için de geçerli olduğu, kaldı ki; 9 nolu CD içeriğinin sanıklara yüklenen suçlamalarla ilgisinin bulunmadığı..." şeklinde değerlendirilmiştir.

İkinci iddia ise şu şekilde değerlendirilmektedir: "Gazeteci tarafından 21.01.2010 tarihinde yapılan yayınların dayanağını oluşturan disklerin Cumhuriyet savcılığına teslimine ilişkin tutanakta 4 adet DVD yazılmasına karşın emanete alınan disklerin 3 adet DVD ve 1 adet CD olduğunun anlaşılması ve bu hususun 4 nolu DVD'nin adli makamlar elinde başka bir CD ile değiştirildiği anlamına geldiği iddiasının gerçeği yansıtmadığı, diskleri teslim eden gazetecinin teslim tutanağında yer alan beyanında da bu durumun "üzerinde 4 yazılı VCD de ise bu belgelerle ilgili muhtelif fotoğraflar vardır" şeklinde ifade edilmiş bulunduğu, Dairemizce yapılan incelemede de bu ifadenin doğrulandığı, üzerinde "4" yazılı diskin DVD olmayıp CD olduğunun açıkça anlaşıldığı, tutanaktaki teslim edilen disklerin dördünün de DVD olduğuna ilişkin yazımın tutanağın düzenlenmesi sırasında oluşan maddi hatadan kaynaklandığı, kaldı ki; bu 4 nolu disk içeriğinin de sanıklara yüklenen suçlarla ilgisinin bulunmadığı, keza bu 4 adet diske kopyalanmış 19 adet CD'nin orijinal halde aynı gazeteci tarafından sonradan Cumhuriyet Başsavcılığına teslim edildiği ve incelemelerin de orijinal CD'ler üzerinden yapıldığı, Böylelikle; dijital delillerin ele geçirilmesinden sonra kolluk veya adli makamlar elinde değiştirilmiş olduğuna ilişkin iddiaların gerçeği yansıtmadığı açıkça anlaşılmaktadır."

İki iddia bir arada değerlendirdiğinde; soruşturma aşamasında tutulan ilk tutanaklarla, bilirkişiyeye teslim edilen eşyayı içeren tutanakların birbirleriyle basit maddi hatalardan oluşan çelişkiler içinde bulunduğu görülmektedir.

Önceki aşamaya ilişkin iddialar ise; *“Dijital delillerle ilgili olarak ileri sürülen diğer iddiaların, kolluk veya adli makamlarca bu delillerin ele geçirilmesinden önceki aşamaya, delillerin bir kısım sanıklarda bulunduğu veya askeri mahallerin kontrollü evrak bürosu gibi ya da Donanma Komutanlığının İstihbarata Karşı Koyma birimi gibi ilgili görevlilerden başkası tarafından girilmesi mümkün olmayan kısımlarında gizlendiği döneme münhasır kaldığı görülmektedir.”* şeklinde özetlenmiştir.

Üstelik kararda, *“Arama ve el koyma işlemlerine ilişkin ihbar içerikleri, Donanma Komutanlığı İstihbarata Karşı Koyma biriminde yapılan aramaya esas ihbarın sanıklara yüklenen suça ilişkin olmaması, arama yapılan askeri ve sivil mahallerin özellikleri, dijital delilleri muhafaza eden sanıklar Hakan Büyük ve Kemalettin Yakar'ın istihbarat sınıfından yetişmiş ve bu tür manipülasyonlara karşı oldukça tecrübeli kimseler olması, tanık beyanları, aramalarda ele geçen delillerin birbirini ve başka mahallerde ele geçen delilleri doğrulaması, belgelerin tutarlılığı, arama işlemlerini gerçekleştiren görevliler, bu görevlilerin sayısı, aramanın icra ediliş şekli, aramada ele geçen diğer malzemeler, Dairemizce de izlenen arama işlemlerine ilişkin kamera kayıtları ve delillerin başkaları tarafından bu mahallere konulduğuna ilişkin savunmaların soyut bırakılmış olması karşısında; anılan delillerin sanıklar dışındaki kimseler tarafından bu mahallere konulmuş olduğuna dair savunmalar dosya kapsamına ve hayatın olağan akışına uygun görülmemiştir.”* denilerek arama işlemleri açısından da hukuki bir sıkıntı bulunmadığı belirtilmiştir.

Ayrıca daha sonra, çeşitli AİHM kararlarına atıflarda bulunularak delillerin inandırıcılığının ulusal yargı organlarına ait bir değerlendirme olduğu belirtilmiştir. Ayrıca AİHS'in, iç hukukun ve ulusal yargının yetki alanına giren delillerin kabul edilebilirlikleri veya bunların değerlendirilmeleriyle ilgili konularda bir kural koymadığı da bu değerlendirmelere eklenmiştir. Bu değerlendirmeler sonucunda, *“...dosya kapsamında yer alan ve hükme esas alınan dijital delillerin esasını korudukları, ilişkin oldukları olayları temsil niteliklerinin ortadan kalkmadığı, ulaşıma, elde ediliş ve muhafaza şekillerinin usule uygun olduğu, açıklanan kabule göre; hayatın olağan akışına, akla ve mantığa uygun bulunduğu ve böylelikle de hukuka uygun deliller olarak hükme esas alınmalarının isabetli olduğu neticesine varılmıştır.”* kanaatine ulaşılmıştır.

Sonuç olarak Yargıtay dijital delillerin mevcut halleriyle hükme esas alınamayacağına ilişkin temyiz itirazlarını yerinde bulmamıştır. AİHM gibi objektif bir gözlemciyi bile suçun işlenmiş olabileceğine dair ikna edebilecek nitelikte delillerin bulunduğunu belirtmiştir. Bu delillerin diğer deliller ve tüm dosya kapsamı göz önünde bulundurularak, hükme esas alınmasında problem olmadığına hükmedilmiştir. Bu konuda Anayasa Mahkemesi kararı, hukuki inceleme yapılmaya daha uygun ve detaylı bilgiler içerdiği için Yargıtay'ın bu kararı üzerinde fazla bir inceleme yapılmamıştır. Dolayısıyla davaya ilişkin detaylı inceleme Anayasa Mahkemesi kararı içeriği üzerinden yapılacaktır.

İlk derece mahkemesinin kararı ile Yargıtay'ın verdiği bu karar, sanıklar tarafından yargılama sürecinde adil yargılanma hakları ile özgürlük ve güvenlik haklarının ihlal edildiği gerekçesiyle Anayasa Mahkemesi'ne başvurulması üzerine Anayasa Mahkemesi tarafından da incelenmiştir⁴⁸². Bu başvurunun içeriği de çok geniş olmakla birlikte konunun bütünlüğü açısından başvurunun delillere ilişkin kısımları ortaya konacaktır.

Başvurucuların delillere yönelik iddiaları, dijital deliller üzerinde yapılan bilirkişi incelemesinin yeterli olmadığı ve tekrarlanmasına ilişkin taleplerin reddedildiği; bilirkişi raporları arasındaki çelişkiler nedeniyle ortaya çıkan delillerin sıhhati konusundaki tereddütlere rağmen mahkûm edildikleri; kendilerine isnat edilen suçun işlenmesine anılan tarihte görevde olan Genelkurmay Başkanı ve Kara Kuvvetleri Komutanı tarafından engel olunduğunun kabul edilmesi nedeniyle bu kişilerin tanıklık yapmak üzere davet edilmeleri taleplerinin reddedildiği; delillerin ortaya konulması ve tartışılması safhasının usulünce yerine getirilmediği; hukuka aykırı olarak elde edilen gerçek dışı delillere dayanılarak mahkûm edildikleri; haklarında yeterli somut delil bulunmaksızın kolektif gerekçelere dayanılarak mahkûm edildikleri; darbe planlarının sunulduğu plan seminerine katılmadıkları veya o tarihlerde yurtdışında görevde olmak vb. engelleyici nedenlerinin olduğu, dijital verilerin kendileri ile illiyet bağlarının ispatlanamadığı; başvurucular tarafından

⁴⁸² AYM 18.06.2014 tarih ve 2013/7800 başvuru numaralı kararı; Resmi Gazete, Tarih: 05.07.2014, Sayı: 29051 (Buradan sonra AYM Balyoz Kararı olarak anılacaktır.), <http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/de3fd0d1-cced-4a35-8377-750ed661dd6b?wordsOnly=False>. (Erişim tarihi: 30.01.2015)

alınan bilirkişi raporları ile başvuruçuların isteği üzerine dinlenen bilirkişi beyanlarının mahkûmiyet kararının dayanağı olan dijital delillerin manipülasyona açık olduğunu ortaya koymasına rağmen bu delillere dayanarak mahkûmiyet kararı verildiği üzerine yoğunlaşmıştır⁴⁸³.

Başvuruçuların dijital delillere ilişkin şikâyetleri karar içerisinde başlıklar halinde özetlenmiştir⁴⁸⁴.

Bu noktada ilk başlık, eski tarihli olarak nitelendirilen dijital delil içeriklerinin, iddia edilen tarihlerden daha sonra oluşturulmasına ilişkindir. Bu iddia “*Bilirkişi raporları ile mahkûmiyet kararının dayanağı olan Eskişehir’de ele geçirilen flaş bellek, Gölcük Donanma Komutanlığında ele geçirilen CD’ler ve harddisklerin 2003 yılında oluşturulduğu iddia edildiği halde bu depolama araçlarında yer alan verilerin 2007 yılına ait bir program olan Microsoft Office 2007 programı ile yazılmış olmasının belgelerin sahteliğini kanıtladığı...*” şeklinde ortaya konulmaktadır.

Diğer bir başlık ise yargılamada sunulan dijital delillere ilişkin bilirkişi raporlarının değerlendirilmesinde iddia-savunma dengesinin sağlanmadığı iddiasıdır. Bu iddia ise, “*Savunma tarafınca yurtiçi ve yurtdışındaki çeşitli üniversite ve bağımsız kuruluşlardan alınan bilirkişi raporlarının mahkûmiyet kararının temel dayanağı olan dijital verilerdeki manipülasyonları ortaya koyduğu ve dijital veriler üzerinde ikibine yakın çelişkiyi ortaya çıkardığı halde İlk Derece Mahkemesi ve Yargıtayca bu raporların dikkate alınmayarak dijital belgelerin ilk oluşturuldukları gibi orijinal olduğu şeklindeki TUBİTAK raporuna dayandığı...*” denilerek ortaya konmuştur.

Bir diğer başlık ise hükme konu edilen dijital delil içeriklerinin kolaylıkla değiştirilebileceği ortadayken, bu delillerin yeterli inceleme ve değerlendirme yapılmadan hukuka uygun olduğunun kabulünün adil yargılanma hakkını ihlaline neden olduğuna ilişkindir. Bu husus “*Mahkeme tarafından itibar edildiği gerekçeli hükmünde kabul ve ifade edilen TUBİTAK görevlilerince düzenlenmiş raporlarda ve mahkemeye sunulan uzman raporlarında ortak görüş olarak ifade edilen; dijital bir*

⁴⁸³ AYM Balyoz Kararı, p. 17.

⁴⁸⁴ AYM Balyoz Kararı, p. 27.

verinin kullanıcı dosya yollarının, oluşturulma ve son kaydedilme tarihlerinin kolaylıkla değiştirilebileceği veya manipüle edilebileceği ya da eski tarihli olarak sonradan düzenlenebileceği gerçeği karşısında, bir gazeteci olan M.B. tarafından savcılığa teslim edilen 11, 16 ve 17 no.lu CD'ler içerisinde yer alan imzasız dijital verilerin, verilerde isimleri yazılı kişi veya sanıklar bakımından hukuka uygun şekilde elde edilmiş bir delil olarak kabul edilmesinin adil yargılanma hakkının ihlali niteliğinde olduğu...” şeklinde açıklanmaktadır.

En son başlık olarak ise dijital delillerin sağlamlığı, bütünlüğü ve güvenilirliği için gerekli olan incelemelerin yapılmasının davaya katkı sağlamayacağı gerekçesiyle reddinin savunma hakkını kısıtladığı hususudur. Bu husus ise “*Delil olarak ileri sürülen tüm dijital materyaller ile ilgili olarak kapsamlı bir bilirkişi incelemesi yaptırılması taleplerinin davaya bir katkı sağlamayacağı gerekçesiyle reddedilmiş olmasının savunma hakkının kısıtlanması niteliğinde olduğu, ileri sürülmüştür.*” şeklinde ortaya konulmuştur.

İlk derece mahkemesinin başvuruçuların şikâyetleri kapsamındaki dijital delillere ilişkin iddialara yönelik değerlendirmeleri ise şu şekilde olmuştur. Mahkeme değerlendirmesinde, üç ayrı yerden elde edilen dijital delillerin birbirlerini doğrular içeriklere sahip olduğu; belgelerde zaman çelişkilerinin bulunduğu ve 2003 yılından sonraki tarihlerdeki olaylara ilişkin bilgilerin olduğu doğru ise de 2003 yılından sonra oluşturulmuş olan belgelerin Balyoz Harekât Planı, Eylem Planları ve ses kayıtlarında yer alan bilgilerin güncelleneceği yönündeki talimatların yerine getirilmesinden ibaret olduğu ve 2003 yılından sonra da plan, bilgi ve listelerin güncelleştirildiği; Balyoz Planında yazışma kurallarına riayet edilmediği, evraklarda imla hataları ile askeri yazışma ilkelerine aykırılıklar bulunduğu, bu nedenle de Balyoz Harekât Planının sahte olduğu iddiasına karşın insan unsurunun bulunduğu her yerde yazım hatası ya da imla yanlışlıklarının olabileceği, hukuk dışı bir yapılanma içerisinde yazışmaların bir düzen ve intizam içerisinde olmasının, askeri yazışma ilkelerinin geçerli olmasının beklenemeyeceği; Balyoz Harekât Planı kapsamındaki cunta yapılanmasının elinde bulunan dijital belgelerin veri yollarında, yazar bilgilerinde uygunsuzluk olmasının, dijital verilerin delil olma niteliğini tek başına ortadan kaldırmayacağı, sanıkların birçok konuyu öngördükleri ve bu kapsamda mevzuat çalışmaları yaptıkları, hata kod tabloları ve ihtimalat planları

hazırladıkları, gerek sanıkların belgelerin oluşturulma aşamasında gerekse sanıkların ve cunta yapılanmalarının güncellenmesi çalışmalarında dijital verilerde bugünkü savunmaların temelini oluşturabilmek amacıyla birçok çelişkinin yakalanmaları halinde kullanılmak üzere bizzat sanıklar tarafından bilerek yapılmış olma ihtimalinin bulunduğu; davanın esasını oluşturan CD'lerin 2007-2008 yıllarına kadar plan odasında kaldığı ve daha sonra bir şekilde buradan çıkartıldığı sabit olmakla birlikte plan odasının herkesin girip çıkmasına açık, kontrolünün zayıf bir yer olduğu; dijital belgelerden bazıları 2007 yılına ait Microsoft Office programı ile yazılmış olmakla birlikte, Microsoft Office'in önceki versiyonları kullanılmak suretiyle bir veri hazırlandıktan sonra, hazırlanan verinin yeni tarihli bir program ile açılmaya çalışıldığında bilgisayarın eski tarihli veriyi sanki açılma tarihindeki yeni versiyonu ile yazılmış gibi dönüştürerek açabileceği, bu nedenle de somut olarak 2003 yılında yazılmış olan bir word belgesinin 2007 yılında yeni versiyon yüklü bir bilgisayarda açıldığında bu 2003 tarihinde yazılmış olan belgenin sanki 2007 yılında hazırlanmış ve yazılmış gibi görünebileceği; 2003 yılında tanzim edildiği iddia edilen keşif ve plan krokilerindeki sokak isimlerinden bazılarının resmi olarak 2007 yılından sonra verilmesi nedeniyle krokilerin, sokaklara resmi olarak bu isimler verildikten sonra çizildiği iddia edilmiş ise de bu sokakların isimlerinin halk arasında, açık kaynaklarda da görüleceği üzere, değişiklikten önceki isimleriyle 40-50 yıldır kullanıldığı; 2005-2006 yıllarında fiilen Türk Silahlı Kuvvetleri bünyesine katılan bir geminin adının 2003 yılında hazırlanan bir CD içerisinde olmasının CD'nin sahteliğine işaret ettiği ileri sürülmüş ise de, bir geminin isminin inşa ve satın alma sözleşmesinin kesinleşmesine müteakip verilmiş olabileceği; sanıkların, kendilerince hazırlanan bir darbe çalışmasında şu veya bu şekilde, bilerek veya bilmeyerek yaptıkları yanlışlar ve çelişkilerin, tüm dosya göz önüne alındığında teşebbüs edilen darbe suçunun sübutunu etkilemeyeceği şeklinde açıklamalarda bulunmuştur⁴⁸⁵.

Anayasa Mahkemesi değerlendirmesinde öncelikle, ilk derece mahkemesinin mahkûmiyet kararını verirken gerek iddia makamı, gerekse savunma makamı tarafından sunulan rapor ve mütalaalarda üzerinde kolayca manipülasyon yapılma ihtimali bulunan ve bir gerçekliği kesin olarak temsil ettiğinin söylenemeyeceği ifade edilen dijital deliller üzerine kurulmadığı; dolayısıyla mahkemenin dijital delillerle

⁴⁸⁵ AYM Balyoz Kararı, p. 43.

birlikte başka delillerin varlığıyla başvuruçuların mahkûmiyetlerine karar verdiği belirtilmiştir⁴⁸⁶.

Ancak dosya dijital delillere ilişkin iddialar göz önüne alınıp incelendiğinde birçok sıkıntı göze çarpmaktadır. Bu noktada öncelikle başvuruçuların iddialarının ilk başlığı olan, eski tarihli olarak nitelendirilen dijital delil içeriklerinin, iddia edilen tarihlerden daha sonra oluşturulmasına ilişkin değerlendirilmelerde bulunulmuştur. Aslında bu başlık içerisindeki tartışmalar diğer başlıklara ilişkin sorunları da doğuran hususlardır. Bu nedenle tartışmanın merkezinin bu başlık olduğu söylenebilir.

Bu değerlendirmelerden ilki şu şekildedir: *“İlk Derece Mahkemesine sunulan bilirkişi raporlarında, 17 no’lu CD’nin 04/03/2003 tarihinde saat 23:52:02’de, 11 no’lu CD’nin 05/03/2003 tarihinde saat 23:50:42’de, 16 no’lu CD’nin ise 14/10/2003 tarihinde saat 12:14:34’de oluşturulduğu görülmektedir. Aynı raporlarda, CD’lerde yer alan dosyaların oluşturma ve son kaydetme tarihleri CD’lerin yazdırıldığı tarih olan 04/03/2003, 05/03/2003 ve 14/10/2003 tarihinden önceye ait olmakla birlikte pek çok belgenin aslında bu tarihlerden sonra üretildiği, 2003 yılı sonrasına ait programların kullanıldığı veya belge içeriklerinde 2003 yılı sonrasına ait bilgilerin yer aldığı tespit edilmiştir. Bu tespitler üzerine bilirkişiler, söz konusu belgelerin bir defada, sistem saati güncel olmayan bir bilgisayarda CD’lere yazdırıldığı görüşünü bildirmişlerdir. İlk Derece Mahkemesi, 2003 yılından sonra oluşturulmuş belgelerin plan, bilgi ve listelerin güncelleştirildiğini gösterdiğini kabul etmiştir. Bununla birlikte Mahkeme, 2003 yılı sonrası “güncelleştirilmiş” olarak kabul ettiği belgelerin, nasıl olup da CD’lerin yazdırılma tarihlerinden önceki tarihleri gösterdiğini cevaplamamıştır.”*⁴⁸⁷ Bunun yanı sıra *“İlk Derece Mahkemesinin kararında dayanak aldığı İstanbul Cumhuriyet Başsavcılığınca görevlendirilen Emniyet Müdürlüğü uzmanlarınca hazırlanan bilirkişi raporunda (gerekçeli karar, s.887); 11 nolu CD’nin oluşturulma tarihi ve saati "05/03/2003, 23:50:42" olduğu, CD içerisinde 68 adet klasör içerisinde toplam 287 adet dosya bulunduğu ve tüm dosyaların "08.04.1996 16:39:44" ila "04.03.2003 13:01" tarihleri arasında oluşturulduğu, bu noktadan hareketle bütün dosyaların oluşturulma tarihlerinin CD’nin oluşturulma tarihinden önce olduğu ve son düzenlenme tarihi en geç olan dosyanın, "04.03.2003, 22:07" tarihinde düzenlenen*

⁴⁸⁶ AYM Balyoz Kararı, p. 44,45.

⁴⁸⁷ AYM Balyoz Kararı, p. 46.

"EK-M LAHİKA-İ BİRLEŞTİRİLMİŞ LİSTE.doc" isimli MS Word dosyası olduğu, bu dosyanın son düzenlenme tarihinin de yine CD'nin oluşturulma tarihinden önce olduğu belirtilmiştir." ortaya konulmuştur⁴⁸⁸.

1. Ordu Komutanlığı Askeri Savcılığı tarafından görevlendirilen bilirkişi heyetince hazırlanan 28/06/2010 tarihli rapora göre; "...esaslı belgelerden biri olan *"BALYOZ Güvenlik Harekat Planı"* olarak adlandırılan dokümanın en son kaydedilme tarihi olarak görülen 02/12/2002 tarihinden sonraki tarihlerde oluşturulan ve rapor ekinde gösterilen belgelerden, takdimlerden ve konuşma metinlerinden alıntıların Doküman Metni içerisinde yer aldığı, 2006 yılında kurulan bir Sivil Toplum Kuruluşunun adının doküman metninde geçtiği gösterilmiştir. Bir başka önemli belge olan *"milli mutabakat hükümeti programı"* adlı dokümanın ise en son kaydetme tarihi olarak görülen 03/03/2003 tarihinden sonra, Bağımsız Türkiye Partisi Genel Başkanı tarafından 27/11/2005 tarihinde yapılan bir Uluslararası Milli Ekonomi Modeli Kongresi Kapanış Konuşma metninden 25 paragraftan alıntıları içerdiği ve bu durumun ise dokümanın 2005 yılından sonra oluşturulduğunu gösterdiği..." tespit edilmiştir⁴⁸⁹.

Yine Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Fakültesi Öğretim Üyeleri Prof. Dr. A. Coşkun Sönmez ve Dr. Ö. Özgür Bozkurt'tan alınan 28/03/2011 tarihli uzman mütalaasına göre, "...11, 16 ve 17 no'lu CD'lerde toplam 80 adet dosyanın, CD'lerin hazırlanma tarihinden sonraki yıllarda kullanıma sunulan programlarla hazırlandığı veya CD'lerin hazırlandığı tarihlerde bulunmayan olanaklar içerdiği..." tespit edilmiştir⁴⁹⁰.

Bunlara ek olarak Arsenal Consulting isimli firmadan alınan raporlarda, 11 ve 17 numaralı CD'lerde bulunan en az 76 dokümanın tarih ve zamanlarında çelişki bulunduğu saptanmıştır⁴⁹¹. Yine benzer zaman ve içerik çelişkileri uzman kişi Tevfik

⁴⁸⁸ AYM Balyoz Kararı, p. 47.

⁴⁸⁹ AYM Balyoz Kararı, p. 49.

⁴⁹⁰ AYM Balyoz Kararı, p. 50.

⁴⁹¹ AYM Balyoz Kararı, p. 51, "...Arsenal Consulting'e göre son kayıtlarının yapılmasının akabinde 2003 yılında CD'ye kaydedilmiş gibi görünen dokümanların Microsoft Office 2007 programından önce mevcut olmayan XML şemalarına ve Calibri yazı karakterlerine referanslar taşıması mümkün değildir ve 11 ve 17 numaralı CD'lerin oluşturulma tarihi, en erken 2006 ortası olabilir. Arsenal, Gölcük'ten elde edilen 5 no'lu Samsung marka sabit diske, tarihi geriye çekilmiş (en az) 120 dosya ve klasörün kopyalandığını belirtmiştir. Arsenal'in DATA MFT'de tespit ettiği tarih ve zaman aykırılıklarından biri, Samsung Sabit Disk'e en son yazılan 120 dosya ve klasörün, 8 Nisan 2004 'de

Koray Peksayar ve uzman kişi Türker Gülüm'ün rapor ve mütalaalarında da tekrar edilmektedir⁴⁹².

Başvurucular tarafından ileri sürülen önemli bir iddia da davaya konu belgelerin üstveri bilgilerinde güncelleme yapıldığının görülmediğidir. Bu hususa ilişkin bilirkişi raporları ve uzman mütalaalarına göre (örneğin Prof. Dr. Ahmet Coşkun Sönmez'in mütalaası); *"...2003 yılında yazılmış olan bir belgenin 2007 yılında üretilmiş bir programla açılması tabiidir. Ancak bu durumun belgenin üstveri bilgilerine muhakkak kaydedildiği ancak dava konusu belgelerde bunun görülmediği iddia edilmiştir. Başka bir deyişle başvuru, derece mahkemelerinde "2003 yılında üretilmiş ve 2007 yılına ait bir yazılım ile açılmış" bir belge ile "2007 yılında üretilmiş belgenin" farklı olduğunu, 2003 yılında üretilmiş bir belge 2007 yılına ait bir yazılım ile açıldığında söz konusu belgenin özgün halinin de 2007 yılına ait hale gelmeyeceğini ileri sürmüşlerdir..."* böyle bir iddia ortaya konulmaktadır⁴⁹³.

Yine AYM kararında başvuru, derece mahkemelerinde "2003 yılında üretilmiş ve 2007 yılına ait bir yazılım ile açılmış" bir belge ile "2007 yılında üretilmiş belgenin" farklı olduğunu, 2003 yılında üretilmiş bir belge 2007 yılına ait bir yazılım ile açıldığında söz konusu belgenin özgün halinin de 2007 yılına ait hale gelmeyeceğini ileri sürmüşlerdir..."⁴⁹⁴.

oluşturulmuş gibi görünmesidir. Arsenal'e göre bu husus, Samsung sabit diski 28 Temmuz 2009 'a kadar kullanımda olduğu için mümkün değildir. Arsenal ayrıca Gölcük'ten elde edilen 1 nolu CD'de bulunan en az 65 dokümanın tarih ve zamanlarında çelişki bulunduğu sonucuna da varmıştır. Arsenal'e göre son kayıtlarının yapılmasının akabinde 2003'de 1 nolu CD'ye kaydedilmiş gibi görünen dokümanların Microsoft Office 2007 programından önce mevcut olmayan ClearType yazı karakterlerine ve XML şemalarına referanslar taşıması mümkün değildir. Gölcük 1 nolu CD, en erken 2006 yılı ortasında oluşturulmuş olabilir..."

⁴⁹² AYM Balyoz Kararı, p. 52.

⁴⁹³ AYM Balyoz Kararı, p. 56.

⁴⁹⁴ AYM Balyoz Kararı, p. 57.

Tüm bu çelişkiler mahkeme tarafından da, hem ileride yeni bir darbe yapmak amacıyla kısmen veya tamamen güncellenmiş olma hem de bizzat sanıklarca daha sonra yargılanma ihtimallerine karşın bilinçli olarak oluşturulmuş olma ihtimallerine binaen⁴⁹⁵, karara gerekçe yapılmıştır. Mahkemenin bu konudaki özeti şu şekildedir: *“Mevcut dijitalerde yer alan belgelerin 5-7 Mart 2003 1. Ordu Plan Seminerinden önce oluşturuldukları, belgelerin yazılı ve ıslak imzalı olarak ilgili birimlere ulaştırıldığı, bu belgelerden sanık Yüksel Gürcan imzalı olan bir tanesinin ele geçirildiği, daha sonraki tarihlerde belgeler üzerinde güncellemeler yapıldığı, bir kısmının oluşturma tarihlerinin değiştirildiği bu şekilde belgelerin ele geçme ihtimaline karşı mevcut çelişkiler ortaya atılarak savunma imkanı hazırlanılmaya çalışıldığı, diğer yandan da Ağustos 2003 tarihinden sonra devam eden cunta yapılanmalarının bu belgeleri kullanılmaya hazır halde tuttukları anlaşılmaktadır.”*⁴⁹⁶.

Mahkeme tarafından bu belgelerin mahkûmiyet kararının dayandığı belgeler olmadığı belirtilse de⁴⁹⁷, ilgili belgelerin mahkûmiyet kararının dayanağını oluşturduğu Anayasa Mahkemesi tarafından ortaya konulmaktadır⁴⁹⁸.

Bu nedenle AYM bu konuda, *“...söz konusu CD’lerin sistem saati güncel olmayan bir bilgisayarda 2003 yılından sonra ve muhtemelen 2007 yılından sonraki bir tarihte oluşturulduğu kabul edilse bile CD’lerin oluşturulduğu tarihe kadar sanıkların ya da dava dışı bazı kimselerin elinde bulunan ve Mahkemenin kabulüne göre güncellenen bir kısım dokümanın oluşturulma tarihinin hangi surette CD’lerin oluşturulduğu tarihten önce üretildiği hususunun, Mahkemece şüpheyi yer bırakmayacak ve ikna edici bir şekilde açıklanması gerekmektedir...”* şeklinde değerlendirme yapmıştır⁴⁹⁹. İşbu değerlendirmeye şu şekilde devam etmiştir: *“...Tarafsızlığı, keyfiliği, denetimden kaçmayı ve perdelemeyi önlemek için mahkemeler, kararın verilmesine neden olan temelleri yeterince açık olarak belirtmekle yükümlüdürler. Mahkemelerin yargılama süresince kendilerine iletilen her iddia ve talebi gözetme zorunda olmadıkları biçimindeki serbesti, kararın*

⁴⁹⁵ AYM Balyoz Kararı, p. 54.

⁴⁹⁶ AYM Balyoz Kararı, p. 53.

⁴⁹⁷ AYM Balyoz Kararı, p. 48.

⁴⁹⁸ AYM Balyoz Kararı, p. 55.

⁴⁹⁹ AYM Balyoz Kararı, p. 55.

*verilmesine neden olan temellere asgari açıklıkta değinilmesi görevini ortadan kaldıracak şekilde yorumlanamaz...*⁵⁰⁰.

Buna ek olarak başvuruçular tarafından mahkemeye sunulan rapor ve uzman mütalaalarının hükme esas alınmadığı görülmektedir. Bunun gerekçesi olarak, söz konusu rapor ve mütalaalarda mahkemenin yerine geçerek delil değerlendirmesi yapılması hususu gösterilmiştir. Mahkemeye göre bu rapor ve beyanlarda “dijital verilerin delil olamayacağı yönünde ve adeta müdafî gibi ayrıntılı tespitlerde” bulunulmuş ve uzman kişiler “tüm çabaları ile bu delilleri çürütmeye çalışmışlardır”. Bu durumun da bu kişilerin tarafsız olmadıkları yönünde kanaat oluşturduğunu belirtmiştir ve bu raporlara itibar etmemiştir⁵⁰¹. AYM ise bu konuda, “...*İlk Derece Mahkemesi, bilirkişi rapor ve uzman mütalaalarında bulunan ve hakim tarafından yapılması gereken hukuki değerlendirmelerin neler olduğunu belirtmemiş, sunulan rapor ve mütalaaların oldukça karmaşık teknik sorunların ele alındığı teknik bilgi içeren kısımlarına da hangi sebeple itibar edilmediğini kararında göstermemiştir...*” şeklinde bir değerlendirme yapmıştır⁵⁰².

AYM bireysel başvurularda mahkemelerin gerekçelerinin niteliği, ancak açık bir keyfilik veya takdir hatası oluşturduğu ya da makul ve ikna edici açıklamalar içeren bir gerekçe gösterilmediği, iddia olunan eylem ile hüküm arasında “uygun illiyet bağı” kurulmadığı durumlarda denetlenebileceğini belirtirken; mahkeme kararlarının adalet gereksinimini giderecek ölçü ve nitelikte yeterli gerekçe ile açıklanıp açıklanmadığı hususunun da adil yargılanma hakkının ihlali iddiasıyla yapılan bireysel başvurular kapsamında yer aldığını belirtmiştir⁵⁰³. Bu nedenle bu dosyayı anlatılan kapsam içerisinde incelediğini belirtmiştir.

İnceleme sonucunda yapılan değerlendirmede ise ilk olarak “...*Savunmaların dayanağını oluşturan ve dijital verilerin güvenilirliğine ilişkin ciddi kuşkular uyanmasına neden olan bilirkişi raporları ve uzman mütalaaları gözetildiğinde, önemli ölçüde, dijital veri ve içeriklerine dayanan İlk Derece Mahkemesince verilen kararın gerekçesi, adalet gereksinimini giderecek ölçü ve nitelikte, yeterli ve makul*

⁵⁰⁰ AYM Balyoz Kararı, p. 58.

⁵⁰¹ AYM Balyoz Kararı, p. 62.

⁵⁰² AYM Balyoz Kararı, p. 63.

⁵⁰³ AYM Balyoz Kararı, p. 59.

olarak değerlendirilemez. Bu sebeple “gerekçeli karar hakkı”⁵⁰⁴ ihlal edilmiştir...” sonucuna varılmıştır⁵⁰⁵. Ayrıca AİHM içtihadı ile bağlantı kurarak⁵⁰⁶, “...Kural olarak, bilirkişilerin sunduğu rapor ve mütalaalar derece mahkemeleri açısından bağlayıcı olmamakla birlikte, İlk Derece Mahkemesi tarafından esasa ilişkin değerlendirmeler yapılırken Cumhuriyet Savcısı tarafından sunulan bilirkişi raporlarının belirleyici bir etkisi olmuştur. Başka bir deyişle somut davada İlk Derece Mahkemesi, yalnızca Cumhuriyet Savcısı tarafından sunulan bilirkişi raporlarına itibar etmiş, bu raporlara karşı başvuru sahiplerinin savunmalarının bir parçası olarak sundukları bilirkişi rapor ve uzman görüşleri ise dikkate alınmamıştır. Mahkeme ayrıca başvuru sahiplerinin, mahkumiyet kararının dayanağı olan dijital verilerin gerçeği yansıtmadığı iddialarını değerlendirmek üzere mahkemenin bilirkişi heyeti tayin etmesi ve rapor aldırması yönündeki taleplerini de yeterli olmayan gerekçe ile reddetmiştir. Böylece başvuru sahiplerinin, haklarında yöneltilen suçlamaların dayanağı olan delillere karşı kovuşturmanın genişletilmesini isteme hakları kısıtlanmış, ceza yargılamasının, maddi gerçeğin ortaya çıkartılması amacına yönelik olarak “silahların eşitliği” ilkesi ihlal edilmiştir...” sonucuna ulaşmıştır⁵⁰⁷.

Böylece dijital delillerin değerlendirilmesine ilişkin şikayetler yönünden, mahkemenin kararının “gerekçeli karar hakkına” ve “silahların eşitliği” ilkesine aykırılığından dolayı, başvuru sahiplerinin Anayasa’nın 36. maddesinde güvence altına alınan adil yargılanma haklarının ihlal edildiğine hükmetmiştir⁵⁰⁸.

AYM kararının da açık şekilde gösterdiği üzere gerek ilk derece mahkemesi gerekse Yargıtay aşamasında karar verilirken birçok husus değerlendirilmemiştir. Sonuç olarak AYM başvuru sahiplerinin adil yargılanma hakkı kapsamında dijital delillerin değerlendirilmesine ilişkin şikâyetlerinin giderilmediğine dair iddialarının ve dönemin Genelkurmay Başkanı Hilmi Özkök ve Kara Kuvvetleri Komutanı Aytaç Yalman’ın tanık olarak dinlenmesi taleplerinin reddi nedeniyle tanık dinletme

⁵⁰⁴ AYM Balyoz Kararı, p. 38, “...Zira bir davada tarafların, hukuk düzenince hangi nedenle haklı veya haksız görüldüklerini anlayıp değerlendirebilmeleri için usulüne uygun şekilde oluşturulmuş, hükmün içerik ve kapsamı ile bu hükme varılırken mahkemenin neleri dikkate aldığı ya da almadığını gösteren, ifadeleri özenle seçilmiş ve kuşkuyla yer vermeyecek açıklıktaki bir gerekçe bölümünün ve buna uyumlu hüküm fıkralarının bulunması “gerekçeli karar hakkı” yönünden zorunludur...”, ayrıca gerekçenin makul olması vs. 34 vd. bir bak

⁵⁰⁵ AYM Balyoz Kararı, p. 61.

⁵⁰⁶ AYM Balyoz Kararı, p. 64 vd.

⁵⁰⁷ AYM Balyoz Kararı, p. 70,71.

⁵⁰⁸ AYM Balyoz Kararı, p. 72.

hakkına ilişkin şikâyetlerinin⁵⁰⁹ kabul edilebilir olduğuna karar vermiştir. Görüldüğü üzere yapılan değerlendirmeler sonucunda mevcut yargılamada Anayasa ile güvence altına alınan adil yargılanma hakkının ihlal edildiği hüküm altına alınarak, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasına yönelik bir karar verilmiştir.

B. Askeri casusluk ve şantaj davası

Balyoz güvenlik harekât planı davasından sonra, yine Türkiye kamuoyunda yankı uyandıran bir başka dava olan Askeri casusluk ve şantaj davası da dijital deliller yönünden incelenecektir.

İlk derece mahkemesinde dava görülürken ve Yargıtay aşamasında dijital delillere ilişkin yapılmış tartışmalar Anayasa Mahkemesi kararı⁵¹⁰ ile özetlenmiş bulunmaktadır. Bu yüzden aynı Balyoz güvenlik harekât planı davasında olduğu gibi konu hakkında daha çok Anayasa Mahkemesi kararı üzerinden bir inceleme yapılacaktır.

Olayda TSK içerisinde yer alan bir fuhuş çetesinin yurt dışından getirdiği kadınlara fuhuş yaptırdıkları ihbarı üzerine başlatılan bir soruşturma içerisinde, başvuru sahiplerinin ev ve işyerlerinde yapılan aramalar sonucunda bulunan dijital delillere elkonulmuştur⁵¹¹.

Soruşturma aşamasında tutuklanan başvuru sahipleri, tutuklanmalarına neden olan, TÜBİTAK ve Genelkurmay Başkanlığı gibi kurumların gönderdiği ve kolluk tarafından dijital delillere ilişkin olarak düzenlenen tüm bilirkişi inceleme tutanağı örneklerinin verilmesi için İstanbul Cumhuriyet Başsavcılığına talepte bulunmuşlardır. Savcılığın ret cevabı üzerine İstanbul 9. Ağır Ceza Mahkemesine yapılan itiraz üzerine, Cumhuriyet Savcılığı mütalaasında; "*Genelkurmay Başkanlığı ile diğer kurumlardan gelen raporlar ile emniyet tarafından hazırlanan inceleme*

⁵⁰⁹ AYM'nin bu konudaki değerlendirmeleri için bkz. AYM Balyoz Kararı p. 73-91.

⁵¹⁰ AYM 09.01.2015 tarih ve 2014/253 başvuru numaralı kararı; Resmi Gazete, Tarih: 12.05.2015, Sayı: 29353 (Buradan sonra AYM Askeri Casusluk Kararı olarak anılacaktır.), <http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/3820ebf9-5872-483d-b088-791694cadbb8?wordsOnly=False>. (Erişim tarihi: 20.05.2015)

⁵¹¹ AYM Askeri Casusluk Kararı, p. 11.

tutanakları bilirkişi raporu niteliğinde olmadığından ve özellikle ilgili kurumlardan gelen raporların şüpheli müdafilerine verilmesi halinde 'Devletin güvenliğine ilişkin belgelerin' inceleme yetkisi olmayan kişilerin eline geçmesi ihtimali bulunduğundan şüpheli müdafilerin taleplerinin CMK. 153. maddesi kapsamında görülmediğinden reddine karar verilmesi" talep edilmiş⁵¹², İstanbul 9. Ağır Ceza Mahkemesi Nöbetçi Hâkimi, bu mütalaa doğrultusunda talebin reddine karar vermiştir⁵¹³.

Bir kısım başvuruçuların bu karara itirazı üzerine İstanbul 9. Ağır Ceza Mahkemesi heyet halinde, talebin kesin olarak reddine karar vermiştir⁵¹⁴.

Pek çok suç iddiasının yer aldığı ve elde edilen dijital delillerden elde edilen bilgilere dayandırılan iddianame ile başvuruçular hakkında kamu davası açılmıştır.

Kamu davası açıldıktan sonra başvuruçular bu kez kovuşturma evresinde, davanın açılmasına neden olan TÜBİTAK, Genelkurmay Başkanlığı ve diğer kurumların gönderdiği ve kolluk tarafından düzenlenen tüm bilirkişi inceleme tutanağı örneklerinin kendilerine verilmesini, CD, flaş bellek, DVD ve hard diskler üzerinde bilirkişi incelemesi yaptırılmasını ve bunların imajlarının verilmesini talep etmiş, başvuruçuların bu talepleriyle ilgili olarak davanın 1. celsesinde *"...adli emanette bulunan dijital materyaller ve diğer belgelerle ilgili iddianamede bu belgelerin devlet sırrı kapsamında kaldığı ve yine askeri belgelerle ilgili soruşturma aşamasında T.C. Genel Kurmay Başkanlığından gelen yazı cevabında da bu belgelerin devlet sırrı niteliğinde gizli belgeler olduğu belirtildiği buna karşılık bu belgelerin on binlerle ifade edilen sayıda olduğu göz önüne alınarak, sanıklarda ele geçirilen ve adli emanette bulunan dijital verilerin imajlarının ve diğer tüm belgelerin yukarıdaki kapsamda devlet sırrı niteliğinde ve aleniyet kazanmaması gereken gizli belgeler olup olmadığı hususunda değerlendirme yapıldıktan sonra sanık ve müdafilerine verilip verilmemesi hususunun karara bağlanmasına, bu aşamada bu yöndeki tüm taleplerin reddi..."* kararı verilmiştir⁵¹⁵. Başvuruçuların

⁵¹² AYM Askeri Casusluk Kararı, p. 15.

⁵¹³ AYM Askeri Casusluk Kararı, p. 16. Karar gerekçesinde yer alan ifade şöyledir: *"İstenen raporlar CMK kapsamında bilirkişi raporu niteliğinde olmadığından bu konudaki taleplerin reddine."*

⁵¹⁴ AYM Askeri Casusluk Kararı, p. 17. Karar gerekçesinde yer alan ifade şöyledir: *"Şüpheliler müdafilerin taleplerinin CMK.153 maddesi kapsamında olmadığı dikkate alınarak, Mahkeme Nöbetçi Hâkimliğinin vermiş olduğu kararda usul ve yasaya bir aykırılık bulunmadığından şüpheliler müdafilerinin itirazlarının reddine."*

⁵¹⁵ AYM Askeri Casusluk Kararı, p. 18.

davanın 5. celse ve 9. celsesinde dijital materyallerin verilmesi hususundaki talepleri "sanıklarda ele geçen dijital verilerle ilgili bilirkişi incelemesi yaptırılacağı" gerekçesiyle reddedilmiştir⁵¹⁶.

Yine davanın 9. celsesinde başvuruclardan bir kısmının suçlamaların dayanağı olan dijital verilerle ilgili uzman kişi sıfatıyla dinlettikleri M.T.'nin uzman kişi sıfatıyla verdiği görüşü; "...üst veri bilgileri (dosyanın adı, kimin oluşturduğu, ne zaman oluşturduğu ve son tarihte ne zaman değiştirildiği gibi bilgiler) tek başına bir güvenlik bilgisi içermediği için güvenilir bir bilgi değildir. Bu veriler bilgisayarı kullanan herkes tarafından değiştirilebilir..." şeklindedir⁵¹⁷.

Başvuruclanın, dijital verilerle ilgili inceleme raporları hazırlayan görevli polislerin huzurda dinlenilmesi talepleri de esasa etkili bir katkısının bulunmayacağı nedeniyle reddedilmiştir⁵¹⁸. Ayrıca başvurucları hakkında mahkûmiyete neden olan dijital kayıtlar üzerinde usulüne uygun olarak bilirkişi incelemesi yaptırılması talebi de ilk derece mahkemesinin "Dijital delillerin sanıkların ev veya iş yerlerinde usulüne uygun yapılan ve kamera görüntüleri ile desteklenen aramalar sonucunda ele geçirilmiş olması nazara alındığında delillere sonradan ilave yapıldığı ya da olay yerine daha önceden konulduğu ile ilgili iddiaları destekleyen bir bulgu bulunmadığından bu savların dayanaksız olduğu sonucuna varılmıştır. Ceza yargılamasında hâkim (mahkeme) önüne gelen delilleri serbestçe takdir eder. Ceza Muhakemesi Kanunu anlamında da bilirkişi kesin delil olarak sayılmamıştır. Bu nedenle CMK. 161. maddesi anlamında Adli Kolluk sayılan Emniyet Müdürlüğü mensubu olan polislerin soruşturma safhasında Bilişim Şubesi aracılığıyla elde edilen dijital delillere ilişkin yukarıda yine dijital delillere ilişkin teorik anlatımda sözü edilen yazılımları kullanarak el konulan dijital delillerin çözümlemesini ve raporlamasını yapmış olmaları karşısında ulaşılan sonuç mahkememizce diğer dosya kapsamındaki deliller bir bütün olarak değerlendirilip dijital delil zinciri göz önünde bulundurularak, ayrıca Yargıtay 9. Ceza Dairesi'nin 2012/1750 esas sayılı 20/06/2012 tarihli onama kararına konu İzmir 10. Ağır Ceza Mahkemesi'nin TCK. 136. maddesinden mahkûmiyete ilişkin örgüt mensubu sanıklardan elde edilen dijital verilerle ilgili benzeri kapsamdaki değerlendirmesi de dikkate alınarak yeterli kabul

⁵¹⁶ AYM Askeri Casusluk Kararı, p. 19 ve 20.

⁵¹⁷ AYM Askeri Casusluk Kararı, p. 21.

⁵¹⁸ AYM Askeri Casusluk Kararı, p. 22.

edilmiş, bu sebeple bir kısım sanıklar müdafisinin 16/12/2011 tarihli celsede beraberlerinde hazır bulundurdıkları ve bilirkişi olarak dinlenmesini istedikleri M.T.'nin duruşma sırasındaki beyanında genel olarak bilgisayarlar da oluşturulan word belgelerinin üst ve alt veri yollarına rahatlıkla müdahale edilebildiğini, bunu önlemenin yolunun bilgisayarların bulunduğu mekanların uygun kontrol araçları ile takibi olduğunu ifade etmiş olması karşısında mahkememizin yukarıda sözü edilen delillerin serbestçe takdire dayalı olduğuna yönelik genel ceza hukuku kabulü dışında bir yenilik getirmediğinden hükme etkili sayılmamış ve yine aynı nedenlerle yeniden bilirkişi incelemesine başvurmaya gerek duyulmamıştır" şeklindeki gerekçesiyle reddedilmiştir⁵¹⁹.

Temyiz yoluyla Yargıtay'a taşınan davada Yargıtay 9. Ceza Dairesi, ilk derece mahkemesinin bilirkişi incelemesi yaptırılması talebini reddetmesine ilişkin temyiz itirazlarını "*Askeri Yargıtay 4. Dairesinin 10.01.2007 gün ve 2007/1-1 sayılı kararında da işaret edildiği gibi, sanıklarda ele geçen ve Türk Silahlı Kuvvetleri ile Türkiye Bilimsel Teknik Araştırma Kurumuna ait bilgilerin TCK'nın 326 ve devamı maddeleri bakımından niteliğini tespit eden bu kurumlarca görevlendirilmiş kişilerin verdikleri mütalaaların, anılan maddelerde aranan evraka, bilgiye ve gizliliğe ilişkin koşullar ile bunlar arasındaki ayrıma ilişkin ölçütlere ve dosya kapsamına uygun biçimde hazırlandığı ve yine sanıklarda ele geçen bilgilerin sayısı, içeriği ve dosya kapsamına göre belirlenen ele geçiriliş amacı dikkate alındığında; niteliklerinin belirlenmesi bakımından özel veya teknik bilgi gerekmediği, nitekim Askeri Yargıtay 1. Dairesince de aynı suç tipine ilişkin bir inceleme sonucunda 18.06.2008 gün ve 2008/1890-1886 sayılı kararı ile aynı sonuca varıldığı anlaşıldığından, dava konusu bir kısım bilgilerin niteliğine ilişkin belirlemenin bilirkişilere yaptırılması gerektiğine dair temyiz itirazları yerinde görülmemiştir"* gerekçesiyle reddetmiş; başvuru haklarında verilen mahkûmiyet kararını onamıştır⁵²⁰.

Bu sürecin ardından Anayasa Mahkemesi önüne gelen dosyada başvuru haklarında dijital delillere yönelik iddiaları, dijital delillerin sıhhati konusunda herhangi bir bilirkişi incelemesinin yapılmadığı ve buna ilişkin taleplerinin reddedildiği, kolluk tarafından hazırlanan teknik raporlara dayanarak karar verildiği, dijital delillerin kopyalarının talep edildiği ancak bunların verilmediği; delillerin

⁵¹⁹ AYM Askeri Casusluk Kararı, p. 23.

⁵²⁰ AYM Askeri Casusluk Kararı, p. 26.

ortaya konulması ve tartışılması safhasının usulünce yerine getirilmediği; hukuka aykırı olarak elde edilen, gerçek dışı delillere dayanılarak mahkûm edildikleri ve haklarında yeterli somut delil bulunmaksızın kolektif gerekçelere dayanılarak mahkûm edildiklerini, dijital verilerin kendileri ile illiyet bağlarının ispatlanamadığı üzerine yoğunlaşmıştır⁵²¹.

Anayasa Mahkemesi dijital deliller konusundaki esas incelemesine başlamadan önce, adil yargılanma hakkının ihlal edildiği şikâyetlerine ilişkin başvurunun usul yönünden kabul edilebilir olduğuna karar vermiştir⁵²².

Başvurunun esas yönünden⁵²³ ilk başlığı silahların eşitliği ilkesinin ihlal edildiği iddiasıdır. Başvurucular bu başlık çerçevesinde, davanın temeli ve hükme esas alınan dijital kayıtlar hakkında sadece kolluk tarafından yapılan teknik tespitlerle yetinilmesi ve bu inceleme tutanaklarının kendilerine verilmesi yönündeki talebin İstanbul Cumhuriyet Başsavcılığınca reddedilmesi, Başsavcılığın ret kararına karşı yapılan itirazların da reddedilmesi, kendilerine ait olduğu iddia edilen dijital verilerin imajlarının verilmesine ilişkin taleplerin kabul edilmemesi, dijital verilerin sıhhati konusunda herhangi bir bilirkişi incelemesi yapılmamasının savunma hakkının kısıtlanması niteliğinde olduğu; delil olarak ileri sürülen tüm dijital materyaller ile ilgili olarak kapsamlı bir bilirkişi incelemesi yaptırılması taleplerinin devlet sırrı olduğu gerekçesiyle reddedilmiş olmasının silahların eşitliği ilkesine aykırı olduğu; mahkeme tarafından itibar edildiği gerekçeli hükümde kabul ve ifade edilen dijital bir verinin kullanıcı dosya yollarının, oluşturulma ve son kaydedilme tarihlerinin kolaylıkla değiştirilebileceği veya manipüle edilebileceği ya da eski tarihli olarak sonradan düzenlenebileceği gerçeği karşısında, ele geçirilen CD, flash bellek ve hard diskler içerisinde yer alan imzasız dijital verilerin, verilerde isimleri yazılı kişi veya sanıklar bakımından hukuka uygun şekilde elde edilmiş bir delil olarak kabul edilmesinin adil yargılanma hakkının ihlali niteliğinde olduğu; hükme esas alınan dijital kayıtlar hakkında Dz.K.K.lığı'nın 6/4/2011 tarih ve ADMÜŞ.:2011/2016 (50984) sayılı yazısı ile bildirilen görüşe mahkemece neden itibar edilmediğinin gerekçesinin bulunmadığı hususlarını ileri sürmüşlerdir⁵²⁴.

⁵²¹ AYM Askeri Casusluk Kararı, p. 33.

⁵²² AYM Askeri Casusluk Kararı, p. 46 vd.

⁵²³ AYM'nin başvuruysu esas yönünden inceleyebileceğine yönelik olarak verilen AİHM kararı örnekleri için bkz. AYM Askeri Casusluk Kararı, p. 68, 69.

⁵²⁴ AYM Askeri Casusluk Kararı, p. 55.

AYM bu iddiaların ilki olan dijital verilerin sıhhati konusunda herhangi bir bilirkişi incelemesi yapılmamasının savunma hakkının kısıtlanması niteliğinde olduğu konusunda, ilk derece mahkemesinin "*Dijital delillerin sanıkların ev veya iş yerlerinde usulüne uygun yapılan ve kamera görüntüleri ile desteklenen aramalar sonucunda ele geçirilmiş olması nazara alındığında delillere sonradan ilave yapıldığı ya da olay yerine daha önceden konulduğu ile ilgili iddiaları destekleyen bir bulgu bulunmadığından bu savların dayanaksız olduğu sonucuna varılmıştır*" gerekçesine gönderme yaparak⁵²⁵; sanıklara isnat edilen eylemlerin esas olarak bilgisayar programlarıyla oluşturulmuş belgelere (CD, DVD, flash bellek, harici disk gibi) dayanması, bu belgelerin içeriklerinin maddi olay ve olguları yansıttığının ve gerçek olduklarının mahkemece kabul edilmesi, 16/12/2011 tarihli celsede dinlenen uzman beyanında, bu verilerin müdahale edilebilir nitelikte olduğunun belirtilmiş olması nedenlerine göre bilirkişiye başvurulmasının ve bir heyet tarafından verilecek raporların maddi gerçeğe ulaşmada önemsiz olduğunun söylenemeyeceğini belirtmiştir⁵²⁶.

AYM, ikinci iddia olan delil olarak ileri sürülen tüm dijital materyaller ile ilgili olarak kapsamlı bir bilirkişi incelemesi yaptırılması taleplerinin devlet sırrı olduğu gerekçesiyle reddedilmiş olmasının silahların eşitliği ilkesine aykırı olduğu konusunda ise "*Dijital deliller üzerinde yapılacak teknik incelemenin suçların sübutu ve sanıkların bu suçlarla ilgisinin tespiti bakımından belirleyici olabileceği açıktır. Başvurucunun, dijital delillerin içindeki belgelerin kendisi tarafından oluşturulmadığı ve temin edilmemiş olduğu iddiası karşısında bu iddialarla ilgili olarak etkili bir şekilde savunma yapmaya imkân verecek bir erişimin sağlanmış olması ya da yargılama makamınca bu amaca uygun bir incelemenin yaptırılmış olması gerekir.*" tespitinde bulunarak⁵²⁷ savunma hakkının zedelenmiş olabileceğini ortaya koymuştur. Daha sonra ise adil yargılanma hakkı kapsamındaki bu konuyu "*Sözleşmenin 6. maddesi çelişmeli yargılama ve silahların eşitliği ilkesi yanında, iddia makamının bütün maddi delilleri açıklamasını gerektirir. Fakat suçlamaya konu delillere erişim hakkı mutlak bir hak değildir. Ulusal güvenlik, tanıkların korunması vb. gibi tedbirlerle ve ancak zorunlu olduğu ölçüde savunma hakkı kısıtlanabilir. Bu amaçlarla bazı delillerin savunmadan saklı tutulması gerekebilir.*"

⁵²⁵ AYM Askeri Casusluk Kararı, p. 70.

⁵²⁶ AYM Askeri Casusluk Kararı, p. 71.

⁵²⁷ AYM Askeri Casusluk Kararı, p. 72.

Ancak savunma hakkını kısıtlayan bu yola kesinlikle gerekli olması halinde başvurulabilir. Böyle bir durumun varlığında bu sınırlamadan kaynaklanan zorlukların yargı makamlarınca başka usullerle mutlaka dengelenmesi gerekir. Bu usuller silahların eşitliği ilkesinin gereklerine uygun olmalı ve gerekli güvenceleri de içermelidir. Bu imkânların sağlanamadığı ve gizlenen delilin belirleyici bir kanıt olduğu durumda silahların eşitliği ilkesi ihlal edilmiş olabilir.” şeklinde özetlemiştir⁵²⁸.

Ayrıca AYM’ye göre: “İsnatların esasını oluşturan delillerle ilgili savunmanın etkisiz kalmasını doğuracak şekilde erişim ve inceleme imkânının sağlanmaması, ceza yargılamasının temel işlevinin yerine getirilmemesi sonucunu doğurur. Suçlamaların temelini oluşturan delillerin suçun sübutu bakımından uygun yöntemlerle ve uzman kişilerce incelenmemesi savunmanın faydasız ve gereksiz olması durumunu ortaya çıkarmaktadır”⁵²⁹.

Kararın devamı şu şekildedir: “Kural olarak, bilirkişinin sunduğu rapor ve mütalaalar derece mahkemeleri açısından bağlayıcı olmamakla birlikte, İlk Derece Mahkemesi tarafından esasa ilişkin değerlendirmeler yapılırken Cumhuriyet Savcısı tarafından yaptırılan incelemelerin belirleyici bir etkisi olmuştur. Başka bir deyişle somut davada İlk Derece Mahkemesi, yalnızca dijital deliller üzerinde Cumhuriyet Savcısı tarafından yaptırılan çözümleme ve incelemeler ile kurumlardan gelen çizelgelere itibar etmiş, bu raporlara karşın başvuruçuların, mahkûmiyet kararının dayanağı olan dijital verilerin gerçeği yansıtmadığı iddialarını değerlendirmek üzere mahkemenin bilirkişi heyeti tayin etmesi ve rapor aldırması yönündeki talepleri ile bu belgelerin imajlarının verilmesi talebini reddetmiştir. Somut olayda, dijital deliller içindeki bilgi ve belgelere dayanarak başvuruçuların mahkûmiyetine karar verilmiştir. Başvuruçuların dijital verilerin gerçeği yansıtmadığı yönündeki iddialarının araştırılması amacıyla bu deliller üzerinde bilirkişi incelemesi yaptırılması veya bunlara ilişkin imajların verilmesi taleplerinin, dijital belgelerin içeriklerinin devlet sırrı kapsamında kaldığından ve dijital delillerin usulüne uygun aramalar sonucu ele geçirildiğinden bahisle reddedilmesi yargılamanın bütünü yönünden adil yargılanma hakkını ihlal eder niteliktedir”⁵³⁰.

⁵²⁸ AYM Askeri Casusluk Kararı, p. 73.

⁵²⁹ AYM Askeri Casusluk Kararı, p. 74.

⁵³⁰ AYM Askeri Casusluk Kararı, p. 75.

Üstelik mahkûmiyet kararına konu olan delillerin mahkemece bu şekilde gizlenmiş olmasının başvuruçuların dijital delillerin sıhhati konusundaki iddialarını tam olarak ileri sürmesini imkânsız kıldığı üzerinde durulmuş; silahların eşitliği ilkesinin gereklerine uygun olmayan bu durumun, başvuruçunun menfaatlerini yeterince koruyan bir güvence içermediği belirtilmiştir⁵³¹.

Sonuç olarak AYM kararına göre; başvuruçuların adil yargılanma hakkı kapsamında kendilerine yöneltilen suçlamaların dayanağı olan delillere karşı savunma yapma imkânı ve kovuşturmanın genişletilmesini isteme hakkı kısıtlanmış, ceza yargılamasının, maddi gerçeğin ortaya çıkartılması amacına yönelik olarak "silahların eşitliği" ilkesi ihlal edilmiştir⁵³². Bu nedenle ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasına yönelik bir karar verilmiştir.

C. Diğer kararlar

Balyoz güvenlik harekât planı davası ile askeri casusluk ve şantaj davası etkileri bakımından kamuoyunda sıklıkla tartışılmakta iken, dijital delillere ilişkin olarak pek de göz önünde olmayan bazı önemli Yargıtay kararları verilmiştir. Ancak Yargıtay'ın bu konudaki kararları sınıflandırılırken, bazı davalarda dijital delillere yönelik kısımdan daha çok, bilişim alanındaki suçlara yönelik kısım öne çıkartılmaktadır. Bu da bilişim alanı açısından üst sınıflandırma yapılırken henüz ceza muhakemesi hukuku problemleri ile suç teorisi problemleri ayrımının Yargıtay tarafından bile yeterince yapılamadığının göstergesidir. Gerçi Türkiye'de Yargıtay kararlarının düzeni ve erişilebilirliği hukukun her alanı açısından problemli bir husustur. Bu yüzden bunun dijital delillere özgü bir problem olmadığı da söylenebilir. Bu bölümde Yargıtay kararları geçmişten geleceğe giderek incelenecek ve sonuçta da bu kararlara yönelik bir değerlendirme yapılacaktır. Bu bölümde konuyla ilgili Yargıtay kararları kronolojik olarak verilerek hem bu konuda öne çıkan problemlerin zamana göre değişimi görülecek, hem de Yargıtay'ın mevcut olaylara zamana göre bakış açısı değerlendirilecektir.

⁵³¹ AYM Askeri Casusluk Kararı, p. 76.

⁵³² AYM Askeri Casusluk Kararı, p. 77.

Yargıtay'ın verildiği dönemde ses getiren bir kararında⁵³³, sanığın kendisine zayıf not veren öğretim görevlisi, mağdur ile birkaç kişiye gönderdiği "e-posta" iletiliyle mağdura sövme eylemi gerçekleştirmesi değerlendirilmektedir. Bu değerlendirmede, internette e-posta yolu ile yapılan hakaret ve sövmeye yönelik elde edilecek dijital delillerin, suçun ispatı açısından sahip olduğu güç, çok ilginç bir değerlendirmeye konu olmuştur. İşbu kararda Yargıtay; *“E-Posta yolu ile yapılan hakaret ve sövmeye; sözü edilen iletiyi internet servis sağlayıcısından gönderen bilgisayarın (I.P) numarasının sorulması, bu yolla bilgisayarın kime ait olduğunun saptanması sonucuna göre; 1- İnternet kafe gibi umuma açık yerlerde bulunan bir bilgisayardan ileti gönderilmiş ise sanığın beraatine, 2- Sanığın evi ya da işyerinde bulunan kişisel bilgisayarından gönderilmiş ise mahkumiyetine, 3- Olayla ilgisi bulunmayan bir üçüncü kişinin kişisel bilgisayarından gönderilmiş ise, bu şahsın tanık olarak dinlenmesi ve sonucuna göre karar verilmesi gerekir.”* değerlendirmesinde bulunmuştur. Yargıtay'ın olaydaki değerlendirmesine göre suçun ispatı açısından iletinin gönderildiği IP numarasının, sanığın kişisel bilgisayarı ile eşleşmesi yeterli olacaktır. Ancak günümüz teknolojisinin kullandığı yöntemler ile IP numaralarının tek başına faili göstermeyeceği söylenebilir⁵³⁴. Nitekim kişilerin IP numaraları kendilerinden habersiz olarak bile kullanılabilir. Bu nedenlerle IP numarasının tespiti ile doğrudan ispat açısından net bir sonuca ulaşılmamalı, bu tespit araştırmanın ilerlemesinde kullanılmalıdır. Bu kararda Yargıtay'ın IP numarası araştırılmadan hüküm kurulmasını yanlış bulması doğru olsa da, sadece IP araştırmasının sonucuna göre bir mahkûmiyet hükmü kurulması ise pek doğru görünmemektedir.

Bu konuda dikkat çeken bir başka Yargıtay kararında⁵³⁵ sanığın kendi adına kayıtlı e-posta adresinden virüs göndererek başkasının bilgisayar sistemine zarar verdiği iddiasına yönelik olarak Yargıtay 11. Ceza Dairesi; *“Gerçeğin kuşkuyla yer vermeyecek şekilde belirlenebilmesi için; öncelikle e-posta yoluyla virüs gönderilerek sistemine zarar verilmiş bir bilgisayarda incelemenin olaydan hemen sonra yapılması yada inceleme yapılacak bilgisayarın olaydan sonra inceleme anına kadar hiç kullanılmamış olması; bilgisayarda virüslü dosya üzerinden inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir yedeğinin alınması, ikinci*

⁵³³ Yargıtay 4. CD, E. 2004/8763, K. 2005/21445, T. 05.12.2005.

⁵³⁴ Dülger, **a.g.e.**, s. 733.

⁵³⁵ Yargıtay 11. CD, E. 2005/6376, K. 2007/2551, T. 16.04.2007.

olarak birebir yedeğin değiştirilip değiştirilmediğinin tespitine 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, daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin talep edilmesi, bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılarak tespiti gerekir.” değerlendirmesini yapmıştır. Bu karar Yargıtay’ın dijital deliller konusunda verdiği belki de en kaliteli karar olarak değerlendirilebilir. Karar içerisinde dijital delillerin elde edilmesi sürecinin sırasıyla hangi işlemler yoluyla yapılacağı açık bir şekilde anlatılmaktadır. Üstelik daha önce verilen kararın aksine burada, IP numarası üzerinden kesin ispatın mümkün olamayacağı hususu da ele alınmıştır. Ayrıca karar konusu olay incelendiğinde, verilerin bilirkişi aşamasına geldiği sırada şirket tarafından değiştirilebilecek durumda olduğu yani inceleme yapılacak bilgisayarın olaydan sonra inceleme anına kadar şirket tarafından kullanılmış olması nedeniyle, bilirkişi tarafından konuyla ilgili bilgilerin internet servis sağlayıcılardan sağlanmasının daha doğru olacağı da belirtilmiştir.

Yargıtay 2009 yılında verdiği bir kararda⁵³⁶ sanığın suçluluğun tespiti açısından IP numarası ile bağlantısının önemini yanı sıra bu bağlantının da araştırılması gereğini bir kez daha belirtmiştir. Yargıtay bu kararda; “*Sanığın savunması ve tüm dosya kapsamı dikkate alındığında, dosyada mevcut Türk Telekomünikasyon A.Ş.’nin yazısından hesaplara gelen paraların internette 85.97.000.000 IP numarası kullanılarak aktarıldığının anlaşılması karşısında, bu numaranın kullanım bilgileri istenerek EFT’nin yapıldığı anda anılan numaranın bu şirket tarafından hangi kullanıcıya atandığının ilgili kurumdan araştırılıp tespit edildiğinde sanık ile irtibatı olup olmadığının saptanması gerektiğinin gözetilmemesi sonucu eksik soruşturmaya dayanarak yazılı şekilde hüküm kurulması nedeniyle hükmün bozulması gerekir.”* değerlendirmesini yapmıştır. Yargıtay burada daha önce IP numaralarına ilişkin verdiği kararın⁵³⁷ izinde giderek, IP numarasının tespiti ile sanığın bu IP numarası arasındaki bağlantısının da araştırılması gereğini bir kez daha ortaya koymuştur.

⁵³⁶ Yargıtay 11.CD, E. 2008/16570, K. 2009/101, T. 28.01.2009.

⁵³⁷ Bkz. s. 163.

Yine bir başka Yargıtay kararı⁵³⁸ örnek bir bilişim suçunda yapılacak araştırmalarda kullanılması gereken usul yöntemlerini gayet güzel bir şekilde özetlemektedir. Karar göre; “*Müştekiye ait hesaptan internet bankacılığı kullanılarak başka bir hesaba para transfer edilmesi şeklinde gerçekleştirilen eylemde; müzekkere yazılarak SMS doğrulama mesajının müştekiye ait hangi GSM hattına gönderildiği; SMS doğrulama mesajı olmadan internet bankacılığına giriş yapıp yapılamayacağının öğrenilmesi; diğer yandan, internet bankacılığına girilen IP numarasının müştekiye ait internet erişim sistemine ait olması karşısında, dosyanın uzman bir bilirkişiye tevdi edilerek, internet bankacılığına yapılan yetkisiz erişimin müştekinin IP adresinden bağlanılarak yapılmasının teknik olarak mümkün olup olmadığı hususunda bilirkişi raporu alınması, ATM cihazından çekilmesine ilişkin görüntülerin saklanıp saklanmadığının ilgili bankadan sorularak, temin edilmesi halinde parayı çeken şahıslar arasında sanıkların bulunup bulunmadığının belirlenmesi; Alışveriş mail order sistemi ile telefon veya internet üzerinden yapılmış ise ilgili iş yerlerinden kullanılan telefon ya da internet IP adresinin temin edilerek buna ilişkin araştırma yapılması ve ayrıca iş yeri çalışanlarının tanık olarak beyanlarına başvurularak söz konusu alışverişlerin sanıklar tarafından yapıp yapılmadığına ilişkin yüz yüze, mümkün değilse fotoğraf üzerinden teşhis işleminin yaptırılması, Adı geçen sanığın kartının usulsüz olarak kullanıldığını tespit etmesi üzerine ilgili bankaya ve yetkili mercilere kayıp ya da çalıntı başvurusu yapıp yapmadığının araştırılarak varsa buna ilişkin kayıt ve belgelerin dosya içerisine celp edilmesi gerekir. Suça yönelik kastın; var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması nedeniyle sanıkların fiilinin nitelikli hırsızlık suçunu oluşturduğu gözetilmelidir. Ek savunma hakkı tanınmadan iddianamede tavsifi yapılmayan bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama suçundan mahkumiyet kararı verilmesi hukuka aykırıdır.” değerlendirmesi yapılmaktadır. İşbu karardaki analiz dijital delil elde etme sürecinin ve bilişim suçlarına yönelik araştırmaların detayı konusunda bilgi edinilebilecek güzel bir karardır. Bu yüzden konuyla nispeten daha az ilgili bu kararı da burada paylaşmak yararlı olacaktır.*

Konuyla ilgili bir başka Yargıtay kararı⁵³⁹ ise bilgisayarlarda yapılan aramalara ilişkin güzel bir örnektir: “*Sanığın kullandığı bilgisayar üzerinde usulince*

⁵³⁸ Yargıtay 13. CD, E. 2012/14783, K. 2013/28348, T. 10.10.2013.

⁵³⁹ Yargıtay 8. CD, E. 2012/21817, K. 2013/25428, T. 24.10.2013.

imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tesbit edilmemiş bulunması, IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden m...-k12.com adresine bağlantı yapıldığının tespit olunamaması "hack" programına rastlanmasının şikayetçiye ait siteye müdahale edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılmamıştır.” Bu kararda CMK 134 ile uygulanan tedbir açısından imaj alma işlemi ve hash değerinin önemi ortaya konulmaktadır. Yine IP numarasına ilişkin araştırmanın yanı sıra bilgisayar kütüğünden yapılan araştırmanın sonucunda suçun işlendiğine dair kesinlik içermemesi nedeniyle olayda kesin delil bulunmadığına dair isabetli bir karar verilmiştir.

IV. Ceza muhakemesi hukuku bakımından konuyla ilgili çözüm önerileri

Ceza muhakemesi hukuku bakımından dijital delillere yönelik hukuki düzenlemelerin ve uygulamadan bazı örneklerin de ortaya koyduğu tek bir sonuç vardır. O da ceza muhakemesi hukukunda dijital delillere yönelik düzenlemelerin bulunduğu, ancak bu düzenlemelerin geliştirilmesi gereğidir. Dijital teknolojinin giderek gelişmesi ile hayatın akışını takip eden hukukun da bu yönde düzenlemelere en azından fikren hazır bulunması gerekecektir.

Bu bölümde ceza muhakemesi hukukunda dijital delillere yönelik problemlere çözüm önerileri ele alınacaktır. Böylece konuyla ilgili hukuki düzenlemelere yönelik fikri bir altyapı hazırlanacaktır.

A. Uluslararası uyum ve işbirliğinin arttırılması

Günümüzde hukuki düzenlemelerin yapılmasında uluslararası toplumun rolü artmıştır. Hukukun her alanında artan uluslararası etkileşimin, uluslararası yaygınlığa sahip dijital deliller açısından da önemli belirleyiciliği olacaktır.

Zaten uluslararası platformlarda uzunca bir süreden beri dijital delillere yönelik düzenlemeler, sınır aşan suçlarla mücadele ve siber güvenlik konuları

içerisinde tartışılmaktadır. Ancak bu konuda hala yapılması gereken hususlar mevcuttur. Bu hususların temeli ise ceza muhakemesinde bulunan uluslararası uyumsuzlukların giderilmesi ve devletler arası işbirliğinin arttırılması ile mümkün olacaktır⁵⁴⁰. Dijital delillerin uluslararası niteliği ve yaygınlığı göz önüne alındığında hukuk alanında işbirliğine yönelik çalışmaların yapılması gereği tartışmasıdır.

Uluslararası hukukun temel kaynakları uluslararası sözleşmelerdir⁵⁴¹. Bu nedenle ceza muhakemesinde uluslararası uyumsuzlukların giderilmesi de uluslararası sözleşmeler yoluyla yapılabilir. Günümüzde dijital delillere ilişkin en kapsamlı düzenleme SSS'dir. Türkiye'de bu Sözleşme'yi onaylamış olduğundan artık Türkiye'de dijital delillere ilişkin yapılacak çalışmalarda, ulusal hukuk düzenlemelerinin SSS'ye uyumlu hale getirilmesi ana hedef olmalıdır⁵⁴².

SSS alanındaki boşlukları dolduran önemli bir uluslararası kaynak olsa da güncellemeye ihtiyaç duyduğu belirtilmektedir. Bu durumda, uluslararası alanda bu konuda çalışmalar yapan Birleşmiş Milletler ve Avrupa Konseyi gibi örgütlerin çalışmaları takip edilmelidir. Ayrıca bu çalışmalara devlet kurumları ve sivil toplum örgütlerinin birlikte çalışmalarıyla, ortaya çıkarılacak benimsenebilir ortak ilkelere ilişkin fikirlerle destek sağlanmalıdır⁵⁴³. Ayrıca adli kolluk teşkilatının INTERPOL ve EUROPOL gibi uluslararası kuruluşla uyumlu bir şekilde çalışması sağlanmalıdır.

Bunlara ek olarak ve uluslararası uyum ve işbirliğinin arttırılması açısından en önemli alan uluslararası adli yardımlaşmadır. SSS 23 ile sözleşmenin tarafı olan devletlere, bilgisayar sistemleri ve verileri ile ilgili ceza soruşturma ve kovuşturmalarında, dijital delillerin toplanabilmesi açısından bir uluslararası işbirliğine gitmeleri gereğinden bahsedilmiştir. Nitekim dijital delillerin soyut nitelikleri ve depolanma yöntemleri göz önünde bulundurulduğunda, bu delillerin dünya çapında bir alana dağılmış olabilecekleri gerçeği ortadadır. Bu nedenle, yapılan suç soruşturmaları veya kovuşturmalarında ülkesel yetki alanlarında yapılan araştırmalar yeterli olmayabilmektedir. Ülke yetki alanı dışındaki yerlerde dijital

⁵⁴⁰ Cevat Özel/Gökhan Ahi, “**Bilişim Suçları’nda Usul ve Sorumluluk Sistemi Üzerine Öneriler**”, Kazancı Hukuk Eserleri Bilgi Bankası, <http://www.kazanci.com/kho2/hebb/files/makale-cevatozel-mgokhanahi-1.htm>. (Erişim tarihi: 22.02.2015)

⁵⁴¹ Hüseyin Pazarcı, **Uluslararası Hukuk**, 12. Baskı, Ankara: Turhan Kitabevi, 2013, s. 37.

⁵⁴² Bkz. s. 169 vd.

⁵⁴³ Özel/Ahi, **a.g.e.**

delil elde etmeye yönelik araştırma yapılması büyük bir sorun teşkil etmektedir. Zira ülkesel sınırların aşıldığı hallerde, yetki sahibi olan diğer ülkeden yeterli yardımın alınamadığı durumlar söz konusu olabilmektedir.

Bunun dışında internet gibi anonim kaynaklar aracılığıyla büyüyen uluslararası karakterli bir yapının üzerinden işlenen suçların hangi ülkenin topraklarında işlendiğinin belirlenmesi bakımından gerek teknik yetersizlikler, gerek bu yeni hukuk alanındaki hukuki tanımların ve kabullerin farklılığı nedeniyle bazı zorluklar mevcuttur⁵⁴⁴.

Bu konuda devletler arasındaki farklı yaklaşımlardan doğan bir sıkıntı, bir ülkede suç kabul edilen eylemin, diğer bir ülkede suç sayılmayabileceği konusu üzerinden doğabilmektedir. SSS içerisinde, 2. maddesi ile 10. maddesi arasında sayılan suç tipleri ile özellikle bilişim yöntemleri kullanılarak işlenecek suçların bir ortak katalog haline getirilmesi ve taraf devletlere bu konuda ceza hukuku düzenlemeleri yapılması zorunluluğu getirmek yoluyla, bu sorunun önüne geçilmeye çalışılmaktadır.

Yine suç konusunda ortak bir düzenleme bulunsa da bazı durumlarda, sanığın vatandaşlığı ile mağdurun vatandaşlığının farklı olması da, hangi devletin ceza kanununun uygulanacağına ilişkin problem yaratabilmektedir. Bu gibi sorunlar ise ancak uluslararası sözleşmeler yoluyla çözülebilecektir⁵⁴⁵.

B. Yeni hukuki düzenlemeler yapılması

Uluslararası uyum ve işbirliğinin önemi yüksek olmakla birlikte, konu ile ilgili ceza muhakemesi hukuku alanında bazı yeni ulusal düzenlemelere de ihtiyaç olacaktır. Mevcut düzenlemelerin günümüz koşullarını karşılamaktan uzak olduğu, yapılan pek çok eleştiri ile ortaya konulmaktadır. Türkiye’de dijital deliller, hukuki anlamda ve delil teorisinde neyi ifade ettikleri tam olarak bilinmeden ve anlaşılmadan, pek çok ceza yargılamasında bir şekilde kullanılmaktadırlar. Üstelik dijital deliller alanındaki gelişmelerle birlikte, bu konudaki tartışmalarda

⁵⁴⁴ Özel/Ahi, **a.g.e.**

⁵⁴⁵ Özel/Ahi, **a.g.e.**

çoğalmaktadır. Dolayısıyla mevcut düzenlemelerdeki yapılacak değişikliklerde bu yeni gelişmelerin bulunması mantıklı olacaktır. Hatta bu konunun bir gereklilik oluşturduğu bile ileri sürülebilir. Bu konuda yapılması gereken ise, önceden üzerinde durulan hukuki düzenlemelerin eksik yanlarını doldurabilecek yeni düzenlemelerin hayata geçirilmesi olacaktır. İşbu başlık altında da ilgili düzenlemelerin eksik yanlarının tespiti ile bu eksikliklerin ne şekilde doldurulabileceklerine ilişkin öneriler yer almaktadır. Bu noktada sadece CMK içerisindeki düzenlemelerde değil, konuyu doğrudan veya dolaylı olarak etkileyen bazı diğer düzenlemelerde de değişiklikler yapılmalıdır.

1. CMK hükümlerinin SSS ile uyumlandırılması

Daha önce de bahsedildiği üzere Türkiye SSS'yi 2010 yılında imzalamış ve 2014 yılında da onaylamıştır⁵⁴⁶. İmzalama ile sözleşmeye aykırı davranmama yükümü edinen Türkiye için, işbu sözleşmenin onaylanmasıyla birlikte sözleşme hükümleri bağlayıcılık kazanmıştır⁵⁴⁷. Dolayısıyla sözleşmeye taraf olan Türkiye açısından mevzuatını SSS'ye uyumlandırma gibi bir yüküm ortaya çıkmıştır⁵⁴⁸.

Bu yükümün gerçekleştirilmesi yolunda ilk önemli adım, SSS'nin 16. maddesi ile 21. maddesi arasında sayılan bilişim koruma önlemlerinin ulusal hukuka uyarlanmasıdır.

Öncelikle CMK 134 kapsamında düzenlenmiş olan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirini ele alacak olursak, bu tedbirin bilgisayar temelli kurulmuş bir yapısı olduğu görülecektir. SSS'de 19. maddede tedbir, depolanmış bilgisayar verilerinin aranması ve bunlara elkoyma olarak düzenlenmiştir. Burada ilk dikkat çeken husus, SSS'nin bu tedbiri düzenlerken veri odaklı bir yaklaşım sergilemesidir⁵⁴⁹. Benzer bir yaklaşım CMK'de gösterilmemiş, düzenlemenin odak noktası bilgisayar olarak alınmıştır. Bu maddenin bu durum göz önüne alınarak bir kez daha gözden geçirilmesi yerinde olacaktır.

⁵⁴⁶ İlgili bilgi için bkz. s. 75.

⁵⁴⁷ Anlaşmaların bağlayıcılığı üzerine görüşler için bkz. Pazarcı, **a.g.e.**, s. 57 vd.

⁵⁴⁸ Türkiye'nin sözleşmeye dair çekinceleri için bkz. s. 75.

⁵⁴⁹ Bkz. s. 76 vd.

Yine arama tedbiri sonrasında verilere elkoyma ya da verilerin kopyalanması hususları CMK 134 içerisinde düzenlenmiş olsa da, bu konudaki eleştiriler⁵⁵⁰ ve çağın gerekleri yerine getirilerek maddenin düzeltilmesi gereklidir. Elkonulan dijital delillerin muhafaza altına alınması hususu Suç Eşyası Yönetmeliği'nin 9. maddesinin 2. ve 5. fıkraları ile düzenlenmiş olsa da bu düzenlemenin hakkında yapılan eleştiriler⁵⁵¹ de dikkate alınarak kanuna taşınması yerinde olabilir.

Bunlara ek olarak SSS 19'a göre CMK 134 içerisinde en dikkat çeken eksiklik verilerin erişilemez hale getirilmesi veya kaldırılmasına yönelik düzenlemelerin madde içerisinde yer almamasıdır. Bu denli önemli bir husus konusunda da doğrudan bir düzenleme bulunmaması önemli bir eksikliktir.

CMK 135 kapsamında düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri ele alınacak olursa, madde içerisinde iletişimin tespiti, iletişimin dinlenmesi, iletişimin kayda alınması, sinyal bilgilerinin değerlendirilmesi ve mobil telefon yeri tespiti gibi tedbirler bulunmaktadır.

Daha önceki bölümde belirtildiği üzere CMK 135 kapsamındaki iletişimin tespiti tedbiri ile telefon görüşmelerine yönelik arama, aranma, yer bilgisi ve kimlik bilgilerinin tespiti yapılmaktadır. Sinyal bilgilerinin değerlendirilmesinde ise sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemleri yapılmaktadır. Ancak her iki tedbir uygulanırken iletişim içeriğine müdahale edilmemektedir. Bu durumda iletişim içeriğine müdahalenin yalnızca iletişimin dinlenmesi ve kayda alınması tedbiri yoluyla gerçekleşeceği söylenebilir. Ancak bu işlem yapılan dinlemenin kayda alınması şeklinde gerçekleştiği için içerik verisinin takibinin yapılması sadece belirlenen çerçevede mümkün olmaktadır. Bu nedenle Türk hukuku açısından SSS 20. maddesindeki trafik verilerinin gerçek zamanlı olarak toplanması bilişim koruma önlemini karşılayabilecek bir tedbirin varlığından söz edilebilirken⁵⁵²; SSS 21. maddesindeki içerik verilerinin denetlenmesi tedbirini karşılayacak bir tedbirin asgari olarak bulunmadığı sonucuna varılacaktır.

⁵⁵⁰ Bkz. s. 108 vd.

⁵⁵¹ Bkz. s. 122.

⁵⁵² Serap Keskin Kızıroğlu, “**Ceza Muhakemesi Hukukunda Bilişim Koruma Tedbirleri**”, Kazancı Hukuk Eserleri Bilgi Bankası, <http://www.kazanci.com/kho2/hebb/files/makale-serapkeskinkiziroglu-3.htm>. (Erişim tarihi: 22.02.2015)

Mobil telefon yeri tespiti ise delil elde etmeye yönelik bir tedbir değildir. Yakalamaya yönelik düzenlenen bu tedbire SSS içerisinde de yer verilmemiştir. Bu nedenle belki de daha başka bir başlık altında düzenlemesi daha doğru olabilir. Ayrıca bu hükmün delil elde etmeye yönelik olarak değiştirilerek teknik takip içerisine alınması da mümkün olabilir.

SSS kapsamında kabul edilen bir diğer bilişim koruma önlemi olan 17. maddedeki trafik verilerinin hızlı şekilde korunması ve kısmen açıklanması işlemi ise 5651 sayılı kanun ile kısmen karşılanmaya çalışılmaktadır. Erişim ve yer sağlayıcılara getirilen trafik bilgilerini saklama ve bildirim halinde bilgi verme yükümleri bu kanun içerisinde yer almaktadır⁵⁵³.

Bu noktada SSS'ye göre eksik kalan diğer düzenlemeler depolanan bilgisayar verilerinin hızlı şekilde korunması ile üretim emridir. Nitekim CMK 134, depolanmış bilgisayar veri içeriklerinin, ileride yapılacak elkoyma işleminin amaca uygun olabilmesi için veri saklayıcılar tarafından özgün niteliğiyle önceden korunmasını sağlayıcı bir düzenleme değildir. Aynı şekilde üretim emrine ilişkin ayrı bir düzenleme de yoktur. Dolayısıyla SSS'nin 16 ve 18. maddelerini kapsayan bu tedbirler ceza muhakemesi hukuku sistemine eklenmelidir.

Ancak özellikle üretim emrini karşılayacak düzenlemeler yapılırken, üretim emrinin aslında bir delili teslim etme ve delil elde edilmesine katkıda bulunma yükümü olduğu unutulmamalıdır. Bu durumda ilgili düzenlemelere şüpheli veya sanığa ve tanıklıktan çekinebilecek kişilere bunun uygulanmaması yönünde istisna hükümleri konulması gerekecektir. Aksi halde kişinin kendisi ve yakınları aleyhine delil vermeye zorlanması yasağı ihlal edilmiş olur. Yine bu konuda savcının veya kolluğun etkili araştırma yapabilmesi için delile ulaştırabilecek şifrelerin edinilmesi gerekli olsa da, bu şifreler bazen gerektiğinden fazla olarak bütün bilgileri ortaya serebilir. Bu nedenle bu hükümlerin karşılıklı menfaatlere göre ciddi bir biçimde değerlendirilip düzenlenmeleri gerekecektir⁵⁵⁴.

⁵⁵³ Bkz. ss. 119-120.

⁵⁵⁴ Ulrich Sieber, “**Enformasyon Toplumu, Siber Suçlar ve Reform**”, Siber Suçlar: Olgular, Önleme, Cezalandırma Konferansı, İstanbul, 12.04.2013.

2. Kişisel verilerin korunmasına ilişkin kanunun çıkartılması

Daha önce de belirtildiği üzere, kişisel verilerin dijital yöntemlerle işlendiği günümüz dünyasında, bu verilerin korunmasına ilişkin ayrı bir mevzuatın olması gereği açıktır⁵⁵⁵. Nitekim kişisel verinin anlamı, hangi gerekçelerle korunması gerektiği, bu korumayı sağlayacak ilkelerin ve istisnaların neler olduğu, verileri işleyenlerin sorumlulukları ve veri öznelinin yani bireylerin hakları açısından açık bir şekilde bir düzenleme içinde bulunmayınca, çeşitli kanunlarda konuya ilişkin mevcut bulunan haklardan da düzgün şekilde yararlanılamamaktadır⁵⁵⁶. Ayrıca bu düzenleme yapılırken, CMK’de bulunmayan kişisel verilerin delil elde etmek amacıyla incelenmesi konusundaki istisna maddesi de bu düzenlemeye eklenebilir⁵⁵⁷.

Buna ek olarak bu düzenlemenin Anayasa’nın 20. maddesi gereği bir anayasal hak olduğu da söylenebilir. AB ile uyum kapsamında da kişisel verilere ilişkin yapılacak düzenlemenin getireceği olumlu etkiden bahsedilebilir. Üstelik bu çalışmada da görüleceği üzere kişisel verilerin korunmasına verilen önem ABAD kararlarına da yansımış durumdadır. Türkiye’nin bu konuda çalışma yapmadığı söylenemese de gelişen sürece bakıldığında kişisel verilerin korunmasına ilişkin düzenleme yapılması sürecinin ağırdan alındığı da açıktır.

3. Adli bilirkişilik kurumu kurulması ve bu konuda kanun çıkartılması

Türkiye’de mevcut durumda dijital delillere yönelik adli bilişim incelemeleri Adli Tıp Kurumu bünyesinde bulunan Fizik İhtisas Dairesi Başkanlığı tarafından yapılmaktadır⁵⁵⁸. Daha önce de bahsedildiği üzere adli tıp, adli mercilerin sadece tıp bilimi konusunda yardım alması gereken bir alandır. Tıp biliminin dışındaki alanların adli tıp içerisine yamanarak⁵⁵⁹ 2659 sayılı Adli Tıp Kurumu Kanunu ve Adli Tıp

⁵⁵⁵ Bkz. s. 121.

⁵⁵⁶ Elif Küzeci, “Anayasal Bir Hak: Kişisel Verilerin Korunması”, s. 145, <http://www.bilisimdergisi.org/s128/pdf/142-149.pdf>. (Erişim tarihi: 19.02.2015)

⁵⁵⁷ Kunter/Yenisey/Nuhoglu (2013), *a.g.e.*, s. 1325.

⁵⁵⁸ Bu görev, Adli Tıp Kurumu Kanunu Uygulama Yönetmeliği’nin fizik ihtisas dairesi başlıklı 14. maddesi ile belirlenmiştir. Nitekim ilgili madde içeriğinde de belirtildiği üzere, ses ve görüntü inceleme şubesi ile bilişim ve teknoloji suçları şubesi işbu daireye bağlı bulunmaktadır.

⁵⁵⁹ Servet Yetim, “Dijital Kanıt Araştırma Yöntemleri”, İstanbul Barosu Dergisi, Cilt: 82, Sayı: 3, 2008, s. 1202 içerisinde Adli Tıp Kurumu Kanunu’nun ilk düzenlemesinde sadece tıbbi alanlarda bilirkişilik ihtiyaçlarının giderilmesi amacıyla Adalet Bakanlığı’na bağlı bir kurum olarak kurulmuş iken daha sonra birimin ana yapısı içinde yer alan ihtisas Kurullarına İhtisas Daireleri de eklenerek morg, fizik, kimya, gözlem, trafik, biyoloji vb. ihtisas daireleri kurulduğuna ve kurumun sadece tıbbi

Kurumu Kanunu Uygulama Yönetmeliği⁵⁶⁰ içerisine katılması yerine, adli bilirkişilik üst kavramı üzerinde birleşilmesi gereklidir.

Dolayısıyla öncelikle bu konu ile ilgili bir düzenleme yapılmak suretiyle Adli Tıp Kurumu Kanunu, Adli Bilirkişilik Kurumu Kanunu olarak değiştirilmelidir⁵⁶¹. Yeni isme sahip bu kurum içerisinde dijital delillere yönelik incelemelerin sağlıklı bir şekilde yapılabilmesi amacıyla adli bilişimin her boyutunu içine alacak bir Adli Bilişim İhtisas Kurulu'nun kurulması gerekmektedir. Üstelik kurulacak bu birimde çalışacak adli bilişim uzmanlarının öncelikle delil konusunu temel alacak şekilde hukuk konusunda ve adli bilişim alanında eğitilmiş olmaları gerekmektedir. Üstelik bu eğitimin belli bir sertifika ya da akreditasyon sistemine bağlanması gereklidir⁵⁶².

Bu birimde çalışacak olan adli bilişim uzmanlarının diğer ihtisas daireleri ile iletişim içerisinde bulunmalarına, hatta farklı ihtisas dairelerinin birbirleriyle olan iletişimine yönelik hususlar düzenlenmelidir. Yine Adli Bilişim İhtisas Kurulu'na bağlı olacak ve bu birimde çalışacak olan adli bilişim uzmanlarının, olayların çözümünde istifade edecekleri ileri düzey laboratuvarlar kurulmalıdır. Bu laboratuvarlarla birlikte nitelikleri gereği kopyaların uzun süre saklanması gereken dijital delillerin depolanmasına yönelik uygun imkânlar sağlanmalıdır⁵⁶³.

Tüm bunlara ek olarak adli bilirkişiliğin sadece bir kurumun kontrolüne bırakılması da çok doğru görünmemektedir. Bu nedenle gerektiğinde üniversitelerin adli bilişim ile ilgili bölümlerinde uzman olan kişilerin görüşlerine de başvurulabilmelidir. Hatta eğer Adli Bilirkişilik Kurumu ve üniversite bünyesinden uzman bilirkişi sağlanmasının mümkün olmadığı hallerde, adli bilişim konusunda çalışan sivil toplum örgütlerinin liyakata göre bildireceği uzmanlara da bilirkişilik görevi verilebilmelidir⁵⁶⁴. Ancak tüm bu kişiler açısından da, adli birimlerin eğitimi başlığında da belirtilecek bir husus olan, konunun uzmanı olduklarını bildiren sertifika ya da akreditasyon belgelerinin bulunması aranmalıdır. Üstelik bu sertifika ve akreditasyon belgelerinde, ilgili uzmanın bilişim alanındaki son gelişmelere

alanlarda bilirkişilik yapma fonksiyonundan hızla uzaklaşmış olmasına rağmen adının değiştirilmesi gerektiği yönünde bir girişimde bulunulmadığına dikkat çekmektedir.

⁵⁶⁰ Resmi Gazete, Tarih: 31.07.2004, Sayı: 25539.

⁵⁶¹ Yetim, **a.g.e.**, s. 1202.

⁵⁶² Bkz. Yetim, **a.g.e.**, s. 1202.

⁵⁶³ Özel/Ahi, **a.g.e.**

⁵⁶⁴ Özel/Ahi, **a.g.e.**

yönelik eğitim aldığını gösterir bilgi bulunmalı, belli tarihten öncesine yönelik belgeler kabul edilmemelidir⁵⁶⁵.

HSYK de 2012 yılında yaptığı değerlendirmede bilirkişilik ve Adli Tıp alanında yaşanan sıkıntılara yönelik bir durum analizi yapmıştır⁵⁶⁶. Bu rapora göre, bilirkişilik hizmetlerinde yapılacak düzenlemeler ve kurumsallaştırma çalışmaları ile bilirkişi raporlarındaki kalite artacaktır. Bu artış ile yargı sisteminin daha sağlıklı, etkin ve hızlı işlemesi temin edilmiş olacak, böylece davaların makul sürede sonuçlanmasına, adil yargılamanın ve adaletin etkin ve sağlıklı işlemesine katkıda bulunulacaktır. Bunların yanı sıra bilirkişi raporlarının tarafsız ve kaliteli bir şekilde hazırlanması yargıya güveni olumlu yönde etkileyecektir. Özellikle bu husus Balyoz güvenlik harekât planı davası içerisindeki en büyük problemlerden birini oluşturmaktadır.

Yukarıda belirtilen tüm hususların gerçekleştirilebilmesi için Adli Tıp uzman sayısı artırılmalı, adli tıp uzmanlığı özendirilmeli, Adli Tıp Grup Başkanlıkları donanımlı hale getirilmeli, grup başkanlıklarında ihtisas dairelerinin tüm birimlerinin kurulması sağlanmalı, adli tıp şube müdürlükleri tüm illere yaygınlaştırılmalı ve son olarak Adli Tıp Kurumu'na olan bağımlılığın kaldırılması için üniversite ve ihtisas hastanelerinin raporları yeterli olmalıdır⁵⁶⁷.

HSYK'nin raporundaki tespitler genellikle doğru olmakla birlikte eksiktir. Nitekim daha önce de bahsedildiği üzere adli bilirkişilik üst kavramı, adli tıp üst kavramına göre daha doğru olacaktır.

C. Dijital delillere ilişkin (hem CMK hem de SSS içerisinde yer almayan) bazı yeni düzenlemelerin uygulanabilirliğinin tartışılması

Ceza hukuk sisteminin geleceği açısından, çeşitli hukuk sistemlerinde yeni olarak denenmiş veya denenmesi tartışılan bazı düzenlemelerin de tartışılması gerekmektedir. Nitekim yeni ulusal düzenlemelerin yapılmasının ardından, mevcut

⁵⁶⁵ Bu konuda bkz. s. 173.

⁵⁶⁶ HSYK, **Yargıda Durum Analizi Toplantıları Sonuç Raporu**, Ocak 2012, ss. 60-61, <http://www.hsyk.gov.tr/dosyalar/Yargida-Durum-Analizi-Toplant%C4%B1lari-Sonuc-Raporu.pdf>. (Erişim tarihi: 20.02.2015)

⁵⁶⁷ HSYK, **Yargıda Durum Analizi Toplantıları Sonuç Raporu**, s. 61.

problemler üzerinden üretilmiş diğer düzenlemelerin de yapılmasının uygunluğuna dair tartışmalar yapılacaktır. Bu nedenle bu başlık altında bu düzenlemelerden bazıları ortaya konarak, tanıtılacaktır.

Bu konuda önerilen düzenlemelerden biri DNA veri tabanının oluşturulmasıdır⁵⁶⁸. Bu konuda Adalet Bakanlığı tarafından 2007 yılında hazırlanan DNA Verileri ve Milli DNA Veri Bankası Kanunu Tasarısı, Başbakanlık tarafından 2008 yılında iade edilmiştir. Adalet Bakanlığı, 2012 yılında tasarımı görüşleri alınmak üzere ilgili kurum ve kuruluşlara tekrar göndermiştir⁵⁶⁹. Kişilerin DNA verilerinin vücuttan alınan örneklerle saptanan ve bir takım genetik incelemeler sonucu elde edilen kişisel veriler oldukları söylenebilir. Suçla mücadele konusunda olumlu olabilecek bu hususun, özel hayatın gizliliği ve kişisel verilerin korunması hakkına müdahale eden bir niteliği olduğu açıktır. Bu nedenle AİHM’de de tartışılmış olan⁵⁷⁰ bu konuda düzenleme yapılırken titizlikle çalışılmalıdır. Hele ki ortada bir Kişisel Verilerin Korunması Kanunu yokken, bu konu ikinci planda kalmaya mahkûmdur.

Bu düzenlemelerden bir diğeri ise verilerin karşılaştırmasıdır. Verilerin karşılaştırılmasında değişik veri tabanlarından⁵⁷¹ elde edilen bilgilerin bir havuza toplanarak, ceza soruşturmasında şüpheli veya şüphelilere ulaşılmaya çalışılır⁵⁷².

Bu düzenlemelerden bir diğeri ise çevrimiçi (uzaktan) aramadır. Çevrimiçi arama soruşturma sırasında üçüncü kişilere ait bilişim sistemine dışarıdan girip

⁵⁶⁸ Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1328; Tanrıkulu, **a.g.e.** , ss. 333-335.

⁵⁶⁹ Adalet Bakanlığı Kanunlar Genel Müdürlüğü, **Aylık Faaliyet Raporu** (01.01.2012-31.01.2012), <http://www.kgm.adalet.gov.tr/Faaliyetler/AyFaliyet/2012%20y%C4%B1%C4%B1/ocak2012/avr.pdf>. (Erişim tarihi: 13.03.2015)

Adalet Bakanlığı Kanunlar Genel Müdürlüğü, **Aylık Faaliyet Raporu** (01.03.2012-31.03.2012), <http://www.kgm.adalet.gov.tr/Faaliyetler/AyFaliyet/2012%20y%C4%B1%C4%B1/Mart2012/avr.pdf> (Erişim tarihi: 13.03.2015)

⁵⁷⁰ S. and Marper v. United Kingdom, 30562/04 and 30566/04, 04.12.2008 kararında AİHM, DNA verilerinin suç soruşturmalarında kullanılacak bile olsa, sınırı belli olmayan bir zaman için depolanmasını demokratik toplumdaki gereklilik ilkesini karşılamaması açısından AİHS 8. maddesinin ihlali olarak değerlendirmiştir.

⁵⁷¹ Türkiye’de bu konuda yapılan çalışmalar hakkında bkz. Selma Arslantaş-Toktaş/Mutlu Binark/Ergin Şafak Dikmen/Işık Barış Fidaner/Elif Küzeci/Alkım Özaygen, **Türkiye’de Dijital Gözetim**, İstanbul: Alternatif Bilişim Derneği Yayınevi, 2012, s. 67 vd. (Örneğin, nüfus ve vatandaşlık işlerine ilişkin kayıtlar, e-devlet şifresi, mobil imza, elektronik imza ve T.C. kimlik kartı gibi; ayrıca sınırlarda yapılan kontrollere ilişkin kayıtlar ile satın alınmış biletler, ödenmiş faturalar gib elektronik ortamda yapılan ticari kayıtlardan da bu noktada bahsedilmesi yerinde olacaktır.) Yine bu konuda bkz. Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.** , s. 1325.

⁵⁷² Tanrıkulu, **a.g.e.** , s. 304.

içerideki verileri öğrenmek olarak tanımlanabilir⁵⁷³. Bu yöntem ile eski yöntemlerle takip edilemeyen kişilerin takibinin mümkün hale geleceği belirtilmektedir. Nitekim modern teknoloji ile kolluğun bilişim sistemine dışarıdan girip ne var ne yok incelemesi ve bu sistemde ne tür işlemler yapıldığını denetlemesi teknik olarak mümkündür.

Bu noktada nitelik olarak çevrimiçi aramaya yakın olan ancak genel anlamda farklı ayrıntılar içeren klavye hareketlerinin kayda alınması (*keylogging*) ve ekranın denetlenmesi ile ilgili düzenlenmeler de dikkate alınabilir⁵⁷⁴.

Son olarak bahsedilmesi gereken düzenleme ise ses ve görüntü kayıtlarının denetlenmesi üzerinedir. CMK'de mevcut olan teknik takip tedbirine karar verildikten sonra kişilerin kamuya açık yerlerdeki faaliyetlerinin denetlenmesi mümkün olsa da, böyle bir kararın olmadığı hallerde kişilerin görüntü ve ses kayıtlarının alınmasının TCK 134 kapsamında özel hayatlarının gizliliğinin ihlaline yol açacağı söylenebilir.

Bu durumda her ne kadar güvenlik amaçlı konulsa da kamuya açık yerlere ilişkin ilgili kayıtları yapan gerek özel gerek kamuya ait güvenlik kameraları⁵⁷⁵ tarafından yapılan tüm kayıtların hukuka aykırı nitelik taşıdığı açıktır. Nitekim haklarında hiçbir düzenleme bulunmamaktadır.

Bunun dışında kamuya açık yerlerde güvenlik kameralarının kullanılması meselesi, kamu yararını oluşturan kamu güvenliği açısından önemi ve özellikle suç soruşturmalarında delil elde edilmesi konusunda yaratacağı geniş imkânlar nedeniyle bu konuda düzenleme yapılması mümkün olabilir.

D. Adli birimlerin konuyla ilgili eğitimi

Gerek uluslararası alanda, gerek ulusal alanda çeşitli çalışmalar yoluyla yeni düzenlemeler yapılsa da, bu düzenlemelerin uygulayıcılarının, düzgün uygulama

⁵⁷³ Kunter/Yenisey/Nuhoğlu (2013), **a.g.e.**, s. 1323.

⁵⁷⁴ Sieber.

⁵⁷⁵ Buna örnek olarak MOBESE sistemi verilebilir. Böylesine yaygınlaşmış bir sistemin hala yasal dayanaktan yoksun şekilde çalışmaya devam ettiği görülmektedir.

yapabilmeleri için, düzenlemelerde neyin amaçlandığını anlamaları gereklidir. Aksi takdirde yapılan uygulamalar hukuki yanlışlıklar doğurabilir.

Arada bazı değişiklikler yapılsa da CMK'nin dijital delillere yönelik düzenlemelerinin kanunlaşmasının üzerinden 10 yıllık bir süre geçmiştir. Bu süre içerisinde bu düzenlemelerin uygulaması açısından belli bir temel oluşmasına rağmen, günümüzde bile alanla ilgili bilgi sahibi olan hukukçu sayısının yetersiz olduğu söylenebilir. Dijital deliller alanının hukuk açısından yeni yeni oturmaya başlayan bir alan olması nedeniyle alan içerisinde süregelen pek çok hukuki tartışma ile birlikte, alan konusunda hukukçuların yeterli bilgiye sahip olmaması, uygulama aşamasında yapılan yanlışlıkları da beraberinde getirmektedir⁵⁷⁶. Bu nedenle öncelikli olarak hukukçuların dijital deliller konusunda bilgi edinmesi sağlanmalıdır.

Eğitim konusunda hukukçular içerisinde ilk olarak değinilmesi gereken kişiler hâkimlerdir. Daha önce de bahsedildiği üzere hâkimlerin bilgi birikimleri, ellerindeki dosya sayısının getirdiği iş yükü ağırlığından dolayı kendilerini geliştirmeye zamanları kalmadığından, sadece dava tecrübesi eksenli gelişmektedir.

Bir görüşe göre, bu durumun çözümü bilişim suçlarına özel ihtisas mahkemelerinin kurulması ile gerçekleşebilir⁵⁷⁷. Böylece bu ihtisas mahkemelerinde görevli hâkimlerin konuya ilişkin teknik bilgilere daha hakim olması sağlanacaktır. Zaten hâkimin bilişim konusunda sahip olması gereken bilgi, olayı hukuken değerlendirmeye ve konuyla ilgili bilirkişi raporunu anlamaya yetecek ölçüdedir. Nitekim dijital delillerin sağlamlığı ve güvenilirliği açısından mutlaka bilişim konusunda teknik bilgilere sahip olan bilirkişilerin yardımından yararlanılması gerekir.

Adli bilişim konusunda yapılacak bilirkişilik sisteminin kanunen nasıl kurulması gerektiğinden daha önemli olan husus, bilirkişiliğe kabul konusundaki

⁵⁷⁶ Mason, **a.g.e.** , ss. xxxv-xxxvi.

⁵⁷⁷ Bilgi çağında bilgiye ulaşmak kolaylaşsa da artan bilgi birikimi hukukun her alanda daha da derinleşmesi sonucunu doğurmuştur. Artık hukukun her alanı eskiye göre çok daha geniş ve kapsamlıdır. Buna dayanarak günümüzde pek çok mahkemenin konu açısından bölümlere ayrılarak ihtisas mahkemelerine dönüştüğü görülmektedir. Hukuk davaları açısından aile mahkemeleri, iş mahkemeleri, kadastro mahkemeleri, fikri ve sınai haklar hukuk mahkemeleri, icra hukuk mahkemeleri ile ceza davaları açısından fikri ve sınai haklar ceza mahkemeleri, icra ceza mahkemeleri bunlara örnek gösterilebilir. Ayrıca bkz. Özel/Ahi, **a.g.e.**

eğitim gereklilikleri olacaktır. Bu eğitim programlarında hukuk, bilişim sistemleri, kriminoloji ve kriminalistik konuları ağırlıklı olarak bulunmalıdır⁵⁷⁸. Böylece bilişim suçlarının nasıl işlendiği, dijital delillerin nasıl elde edileceği, dijital delillerin zarar görmeden ve orijinalliğini bozulmadan ne şekilde inceleneceği ve bu incelemeler sonunda ortaya çıkan sonuçların adli makamlara nasıl sunulacağı öğrenilecektir. Üstelik tüm bu eğitim düzeninin belli bir sertifika ya da akreditasyon sistemine bağlanması gereklidir.

Adli bilişim konusunda aldığı eğitim sonucunda, bu alanda uzmanlık sertifikası ya da akreditasyonu alan kişilerin, bilirkişilik faaliyetlerini yürütebilmeleri için, düzenli olarak mesleki gelişim eğitimlerine de tabi tutulmaları gerekir. Nitekim bilişim ve dijital teknoloji alanındaki gelişmelerin takip edilip edilmediği ancak bu yolla denetlenebilecektir⁵⁷⁹.

Günümüzde Türkiye’de bazı üniversitelerde açılan adli bilişim yüksek lisans programlarının yanı sıra Adli Bilişim Mühendisliği lisans programları da bulunmaktadır. Adli bilişim alanındaki eleman eksikliğinin giderilmesi açısından, bu tip programların üniversite bünyelerinde kurulması olumlu bir gelişmedir.

Tüm bu gelişmelerin yanında, sadece özel ihtisas mahkemelerinin kurulması, bu konudaki eksikliği gidermek açısından yeterli değildir. Nitekim bu ihtisas mahkemelerinin düzgün bir şekilde işleyebilmesi için, savcılar ve kolluk görevlilerinin de ihtisaslaşması gerekecektir⁵⁸⁰. Nitekim bilişim aygıtları aracılığıyla suçların soruşturma ve kovuşturma aşamasındaki adli işlemler, bu alanda bilgi sahibi olan savcılar ve dijital deliller konusunda eğitilerek bu konuda özel olarak görevlendirilmiş kolluk görevlilerinin mevcudiyetinde daha rahatlıkla yapılacaktır. Özellikle kolluk görevlileri açısından, açılacak eğitimler sonunda verilecek sertifikalar yoluyla dijital delillerin elde edilmesi konusunda uzmanlaşan birimler kurulmalıdır⁵⁸¹.

⁵⁷⁸ Adli Bilişim İhtisas Kurulu’nda çalışacak kişilerin yazılımdan, donanımdan, veri tabanı yönetiminden, veri kurtarmadan ve ağ bağlantıları yönetiminden anlayan uzmanlar olması gerektiği konusunda bkz. Özel/Ahi, **a.g.e.**

⁵⁷⁹ Yetim, **a.g.e.**, s. 1202.

⁵⁸⁰ Özel/Ahi, **a.g.e.**

⁵⁸¹ Özel/Ahi, **a.g.e.**

Bunların yanı sıra bilişim suçları alanında ihtisaslaşan hâkim, savcı ve kolluk birimlerinin bir araya gelecekleri, teknolojik imkânların son durumuna ilişkin güncel bilgilerin paylaşıldığı seminerlerden ve dijital delillere ilişkin süreçlerin nasıl işlediğine dair yapılacak çalışma ziyaretlerinden oluşan bir farkındalık eğitimi programı oluşturulması da yararlı olacaktır⁵⁸². Nitekim Türkiye’de bilgi probleminin daha büyük bir farkındalık problemi oluşmaya başlamıştır. Adli kurumların birbirlerinin çalışmaları hakkında farkındalığının oluşması açısından bu tür programların önemi büyüktür.

Avukatların da adli bilişim ve dijital deliller konusunda bilgi sahibi olabilmeleri açısından barolar aracılığıyla seminerler ve konferanslar düzenlenmesi de yararlı olacaktır.

Sonuç olarak önerilen ideal çözüm olarak bilişim suçlarına yönelik ihtisaslaşma olgusunun önemi ön plana çıksa da, yargılamanın dijitalleştiği bu çağda adli birimlerin hepsinin belli oranda dijital teknoloji bilgisine sahip olması gereklidir. Özellikle hâkim ve savcılarının bu konularda temel bir eğitim almaları şarttır⁵⁸³. Nitekim artık ceza muhakemesi işlemleri bile dijital bir platform olan UYAP aracılığıyla gerçekleştirilmektedir. Dolayısıyla ihtisaslaşmanın sağlanması ile bile sorunlar tamamen çözülemeyebilir.

⁵⁸² HSYK, **Hukuki Müzakere Toplantıları Ceza Hukuku Grubu Raporu**, Denizli, 08.11.2013-10.11.2013, s. 5, <http://hmt.hsyk.gov.tr/toplantilar/2013/adli-yargi/guz/denizli/raporlar/5grup.pdf>.

⁵⁸³ **Hâkimler ve Savcılar İçin Siber Suç Eğitimi: Bir Kavram**, AK Siber Suç Projesi ve Lizbon Şebekesi, Strasbourg, 2009, s. 12, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09_TUR.pdf.

SONUÇ

Günümüzün önemli bir gerçeği haline gelen dijital delillerin ceza muhakemesi sistemindeki yerini gösteren bu çalışmada, sıklıkla kavram ve terimlerin anlamlarının üzerinden değerlendirmeler yapılmıştır. Nitekim hukuk, delil ve ispat sistemlerinin tarihçesi düşünüldüğünde daha çok yeni olan bu alanda öncelikli dikkat çeken problem, hukukçuların konuya yabancı olmaları nedeniyle yaşadıkları kavram kargaşasıdır. Nitekim ceza muhakemesinde dijital deliller başlığı tezin konusunu açıkça belirtse de; henüz başlıkta belirtilen dijital delil teriminin bile tartışmalı olduğunu söylemek gerekir. Hukuk düzenlemeleri içerisinde daha çok elektronik terimi kullanılsa da, elektronik delil olarak kastedilen delillerin içerik olarak dijital delilleri oluşturduğu söylenmelidir.

Her bilim gibi hukuk da kendi dilini oluşturabilen bir bilim alanı olsa da, hayatla doğrudan bağlantılı bu alanın içerisindeki kavramların da hayatla ve diğer bilim alanlarıyla olan ilişkisi önem kazanmaktadır. Nitekim hukuk düzenlemelerindeki lafzi yanılsamalar, uygulamada yapılacak yanlışlıkların da kapısını aralamaktadır. Neticede hukukçular da insandır ve insan yanılır. Önemli olan bu yanılgılardan ders çıkarmaktır. Bu nedenlerle kavramsal tartışmalar ve dijital delilin yerinin mevcut ceza muhakemesi hukukundaki delil teorisi içerisindeki yerinin tespit edilmesi bu çalışmanın öncelikli sorunsalı olmuştur.

Ancak dijital deliller sadece hukuk alanını içermeyen, bilgisayar ile ilgili alanları ve bilişim bilimini ilgilendiren çok yönlü bir konudur. Bu nedenle çalışma içerisinde karşılaşılan en büyük sıkıntılardan biri, konu ile doğrudan ilgisi olan ama hukuk ile doğrudan ilgisi olmayan bir alana ilişkin yapılacak değerlendirmelerde yanılgıya düşme ihtimalinin artmasıydı. Bu nedenle bilişim alanına ilişkin değerlendirmeler mümkün olduğunca kısa bir özet olarak tutulup, konunun ana omurgası olan hukuk alanına daha çok yer ayrılmıştır.

Hukuka ilişkin incelemeler yapılırken uluslararası, yabancı ve ulusal düzenlemeler ayrı olarak incelenmiştir. Böylece her bir sistem birbirinden ayrı olarak daha rahat olarak görülebilecek duruma gelmiştir. Bu incelemeler sonucunda henüz hiçbir hukuk düzenlemesi açısından mükemmeliyetin yakalanamamış olduğu ve her düzenlemenin kendince bazı eksikliklerinin bulunduğu tespit edilmiştir. Bu noktada dijital delillerin uluslararası yaygınlığı da dikkate alındığında, bu konuda yapılan uluslararası düzenlemelerin öneminin de biraz daha fazla olduğu gerçeği de ortaya çıkmaktadır. Zaten dijital deliller konusunda yapılan düzenlemelerin uluslararası hukuk temelli çalışmalar sonucunda ortaya çıkmakta olduğu gerçeği de ortadadır. Nitekim bu konudaki en önemli örnek Avrupa Konseyi tarafından hazırlanmış olan Siber Suçlar Sözleşmesi'dir.

Siber Suçlar Sözleşmesi günümüz açısından yeterli görünmese de, iyi bir başlangıç noktası olarak kabul edilebilir. Türkiye de bu Sözleşme'yi onaylayarak bu konudaki iradesini ortaya koymuştur. Bu noktada artık ulusal hukuk düzenlemeleri yapılırken, Sözleşme'nin bilgisayar verisi odaklı anlayışı ve hukuki değer olarak veriyi temel almasına dikkat edilmesi gerekir. Bunun dışında yabancı hukuk düzenlemelerindeki olumlu örneklerin takip edilebilmesi açısından, bu konuyu ilgilendiren yabancı hukuk düzenlemeleri de incelenmiştir.

Yapılan incelemeler sonucunda Türkiye'de dijital delilleri ilgilendiren düzenlemelerin belli temellerinin bulunduğu, ancak bu temellerin kendilerinin ve üstlerinin sağlam bir şekilde doldurulmadığı tespit edilmiştir. Bu konudaki eksikler tespit edilerek eleştirilmiştir.

Daha sonra ise kuralların hayata yansımaları ve uygulamasının aynası olan mahkeme kararlarının dijital delilleri ilgilendiren kısımları incelenmiştir. Bu konudaki hak ihlallerini ve asgari standartları belirleme açısından Avrupa İnsan Hakları Mahkemesi kararlarının her zaman için dikkatle takip edilmesi gereklidir. Nitekim bu kararlar, bilişim koruma tedbirleri olarak da adlandırılan dijital delil elde etme yöntemlerinin temel haklar ile çatıştığı noktaların çözümlerini içermektedir. Avrupa Birliği Adalet Divanı ise bu konuda daha çok kişisel verilerin korunması kapsamında verdiği kararlarla dikkat çekmektedir.

Yargıtay kararları ise Türkiye'nin dijital deliller konusunda bulunduğu pozisyonu en iyi şekilde gösteren kararlardır. Bu konuda özellikle Balyoz güvenlik harekât planı davası belki de tüm diğer mahkeme kararlarından daha önemli ve çarpıcı sonuçlar içermektedir. Bu nedenle davanın dijital delillere yönelik tüm detaylarının ortaya konması, konunun anlaşılması ve aydınlatılmasında son derece yararlı ve yol gösterici olmuştur. Yine Yargıtay'ın dijital delillere ilişkin diğer kararları ise kronolojik olarak incelenerek, Yargıtay'ın zamana göre yaptığı değerlendirmelerde oluşan farklılıkların görülmesi açısından önemli olmuştur.

Çalışmanın en son kısmı ise bir tamamlayıcı kısımdır. Nitekim hukuk düzenlemeleri ve mahkeme kararları sonucunda dijital delillere ilişkin ortaya çıkan doğru hukuki tablonun, Türkiye'de ne gibi değişiklikler aracılığıyla oluşturulabileceği ortaya konulmuştur. Bu nedenle bu kısım sadece konunun doğrudan bir parçası olmamakta, ileriye dönük önerileri de içeren bir değerlendirme bütünü de içermektedir.

Yapılan her çalışmanın mutlaka geliştirilebilecek yönleri bulunmaktadır. Nitekim bilimle uğraşmak da bunu gerektirir. Özellikle hukuk gibi derin bir alanda ise yazılacak şeyler hiç bitmeyebilir. Ancak bir noktada edinilen bilgilerin toparlanması gerekir. Örneğin bu konuda elbette daha çok yabancı hukuk sistemi incelenerek, bu sistemlerin tümünün karşılaştırması ulusal düzenlemeler içerisinde katılarak bir bütünleştirme yapılabilirdi. Ancak mevcut durumda sistemler ve kavramlar arasında bulunan derin farklılıklar gereği her sistemin kendi içerisinde değerlendirmesinin yapılması daha doğru görünmektedir.

Sonuç olarak daha önce de belirtildiği gibi, tezin başlığının bile tartışmalı olduğu bir durumda, tezin ana amacının bu tartışmalara bir cevap getirebilmesidir. Nitekim ceza muhakemesinde dijital deliller açısından temel değerlendirmeleri içeren bu çalışmanın, tezin dayanak noktaları olan dijital delillerin ceza muhakemesindeki yerinin tespit edilmesi ve bu konuda yaşanan sorunların çözülmesine ilişkin problemlere ilişkin tartışmaları ve çözümleri içerdiği söylenebilir. Bu nedenle çalışmanın amacına ulaştığı söylenebilir.

KAYNAKÇA

Kitaplar:

Alangoya, H. Yavuz/Yıldırım, M. Kâmil/Deren-Yıldırım, Nevhis, Medenî Usul Hukuku Esasları, 6. Bası, İstanbul: Alkım Yayınevi, 2006.

Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk, Ankara: Ankara Barosu Yayınları, 2009.

Arslandaş-Toktaş, Selma/Binark, Mutlu/Dikmen, Ergin Şafak/Fidaner, Işık Barış/Küzeci, Elif/Özaygen, Alkım, Türkiye’de Dijital Gözetim, İstanbul: Alternatif Bilişim Derneği Yayınevi, 2012.

Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, A. Caner, 3. Baskı, Ceza Hukuku Genel Hükümler I, Ankara: Seçkin Yayınevi, 2002.

Avşar, Zakir/Öngören, Gürsel, Bilişim Hukuku, İstanbul: Pasifik Ofset, 2010.

Casey, Eoghan, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3. Edition, Londra: Academic Press, 2011.

Centel, Nur/Zafer, Hamide, Ceza Muhakemesi Hukuku, İstanbul: Beta Yayınevi, 6. Bası, 2008.

Centel, Nur/Zafer, Hamide/Çakmut, Özlem, Türk Ceza Hukukuna Giriş, 4. Bası, İstanbul: Beta Yayınevi, 2006.

Değirmenci, Olgun, Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara: Seçkin Yayıncılık, 2014.

Dönmezer, Sulhi/Erman, Sahir, Nazarî ve Tatbikî Ceza Hukuku: Genel Kısım, Cilt: I, 5. Bası, İstanbul: Sulhi Garan Matbaası Vârisleri Koll. Şti. , 1973.

Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, 5. Baskı, Ankara: Seçkin Yayıncılık, 2014.

Erem, Faruk, Diyalektik Açısından Ceza Yargılaması Hukuku, 6. Baskı, Ankara: Işın Yayıncılık, 1986.

Ergün, İsmail, Siber Suçların Cezalandırılması ve Türkiye’de Durum, Ankara: Adalet Yayınevi, 2008.

Evik, Vesile Sonay, Çıkar Amaçlı Örgütlenme Suçu, İstanbul: Beta Yayınevi, 2004.

Feyzioğlu, Metin, Ceza Muhakemesinde Vicdani Kanaat, Ankara: Yetkin Yayınları, 2002.

Göksu, Mustafa, Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayınevi, 2011.

Hames, Joanne Banker/Ekern, Yvonne, Constitutional Law: Principles and Practice, The West Legal Studies Series, New York: Thomson/Delmar Learning, 2004.

Henkoğlu, Türkay, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, 2. Baskı, İstanbul: Pusula Yayıncılık, 2014.

Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 4. Baskı, Ankara: Seçkin Yayıncılık, 2012.

Kaymaz, Seydi, İletişimin Denetlenmesi: Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan, 4. Baskı, Ankara: Seçkin Yayınevi, 2015

Keser Berber, Leyla, Adli Bilişim, Ankara: Yetkin Yayınları, 2004.

Ketizmen, Muammer, Türk Ceza Hukuku'nda Bilişim Suçları, Ankara: Adalet Yayınevi, 2008.

Kocasakal, Ümit, Avrupa Birliği Ceza Hukukunun Esasları, İstanbul: Veday Yayıncılık, 2004.

Kunter, Nurullah, Ceza Muhakemesi Hukuku, İstanbul: Sermet Matbaası, 5. Bası, 1974.

Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe, Açıklamalı Ceza Muhakemesi Kanunu, Cilt I, İstanbul: Beta Yayınevi, 2013.

Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Baskı, İstanbul: Beta Yayınevi, 2010.

Kuru, Baki, Hukuk Muhakemeleri Usulü, Cilt II, 6. Baskı, İstanbul: Demir – Demir Yayıncılık, 2001.

Leach, Philip, Taking a Case to the European Court of Human Rights, 3. Edition, Oxford University Press, 2011.

Öztürk, Bahri/Erdem, Mustafa Ruhan/Özbek, Veli Özer, Uygulamalı Ceza Muhakemesi Hukuku, 7. Baskı, Ankara: Seçkin Yayıncılık, 2002.

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

Pazarcı, Hüseyin, Uluslararası Hukuk, 12. Baskı, Ankara: Turhan Kitabevi, 2013.

Sanders, Donald H. , Computers Today, 2. Edition, Singapur: McGraw – Hill Book Company, 1986.

Sınar, Hasan, İnternet ve Ceza Hukuku, İstanbul: Beta Yayınevi, 2001.

Sommer, Peter, Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers, Third Edition, Information Assurance Advisory Council, 2012.

Taner, Tahir, Ceza Muhakemeleri Usulü, 2. Bası, İstanbul: Duygu Matbaası, 1950.

Tanrıkulu, Cengiz, Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma, Ankara: Adalet Yayınevi, 2014.

Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sancakdar, Oğuz/Önok, Rifat Murat, İnsan Hakları El Kitabı, 4. Baskı, Ankara: Seçkin Yayıncılık, 2011.

Toroslu, Nevzat/Feyzioğlu, Metin, Ceza Muhakemesi Hukuku, 7. Baskı, Ankara: Savaş Yayınları, Eylül 2009.

Türk Hukuk Lûgatı, 3. Baskı, Ankara: Başbakanlık Basımevi, 1991.

Ünver, Yener/Hakeri Hakan, Ceza Muhakemesi Hukuku, 2. Cilt, 6. Baskı, Ankara: Adalet Yayınevi, 2012.

van Dijk, Pieter/van Hoof, Fried/van Rijn, Arjen/Zwaak, Leo, Theory and Practice of the European Convention on Human Rights, Fourth Edition, Antwerp: Intersentia, 2006.

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

Yayla, Yıldızhan, İdare Hukuku, 2. Basım, İstanbul: Beta Yayınevi, 2010.

Yazıcıoğlu, Yılmaz, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul: Alfa Yayınevi, 1997.

Yenidünya, Caner/Değirmenci, Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul: Legal Yayıncılık, 2003.

Yurtcan, Erdener, Ceza Muhakemeleri Usulü Kanunu Şerhi ve İlgili Mevzuat, 2. Cilt, İstanbul: Kazancı Hukuk Yayınları, 1988.

Makaleler:

Akıncı, Hatice/Alıç, A. Emre /Er, Cüneyd, “Türk Ceza Kanunu ve Bilişim Suçları”, İnternet ve Hukuk, Yeşim Atamer (der.), İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

Akyürek, Güçlü, “Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu”, Türkiye Barolar Birliği Dergisi, Sayı: 101, Temmuz 2012, ss. 61-82.

Dokurer, Semih, “Adli Bilişim”, Ses Görüntü ve Data İncelemeleri, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008.

Fabbrini, Federico, “Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.”, Tilburg Law School Research Paper No. 15/2014.

Feyzioğlu, Metin, “Belirtilerin Şüphenin Yenilmesindeki İşlevi ve Benzer İsnadlara Ait Delil Araçlarının Somut Olayın Çözümünde Birlikte Değerlendirilmesi”, Ankara Barosu Dergisi, 2000-1, ss. 20-44.

Galves, Fred/Galves, Christine, “Ensuring Admissibility of Electronic Forensic and Enhancing Its Probative Value At Trial”, Criminal Justice Magazine, Vol: 19, Number 1, Spring 2004, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html.

Karakuş, Oğuz/Ünal, Bülent, “Olay Yeri İnceleme”, Oğuz Karakuş (ed.), Kriminalistik, 2. Baskı, Ankara: Adalet Yayınevi, 2013, ss. 3-85.

Kerr, Orin S. , “Digital Evidence and the New Criminal Procedure”, Columbia Law Review, Ocak 2005, s. 279 vd.

Kerr, Orin S. , “Searches and Seizures in a Digital World”, Harvard Law Review, Vol. 119, 2005, ss. 531-585.

Kerr, Orin S. , “The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?”, Connecticut Law Review, Vol. 33, 2001, ss. 503-535.

Keskin, İbrahim, “İnternet Servis Sağlayıcılarının (İSS) Hukuki ve Cezai Sorumluluğu”, İstanbul Barosu Dergisi, Cilt: 84, Sayı: 2010/5, ss. 2921-2980.

Keskin, Serap, “Avrupa Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, ss. 155-180.

Koops, B. J. , “Cybercrime Legislation in the Netherlands”, Electronic Journal of Comparative Law, Vol.14, No.3, December 2010, s. 17 <http://www.ejcl.org/143/art143-10.pdf>.

Law, Frank/Chow, K. P./Mai, Y. H. , “Understanding Computer Forensics Requirements in China via the “Panda Burning Incense” Virus Case”, Understanding Computer Forensics Requirements... , 2014, ss. 51-58.

Makarim, Edmon, "Electronic Evidence and Electronic Signatures in Indonesia: The Probative Value of Digital Evidence", *Digital Evidence and Electronic Signature Law Review*, Vol. 10, 2013, ss. 136-143.

Marcus, Paul/Waye, Vicky, "Australia and the United States: Two Common Criminal Justice Systems Uncommonly at Odds", *College of William & Mary Law School Faculty Publications*, 2004, ss. 27-116, <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1245&context=facpubs>.

Mason, Stephen, "Introduction", Stephen Mason (ed.), *International Electronic Evidence*, Londra: British Institute of International and Comparative Law, 2008.

O'Leary, Kaitlin R., "What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine", *Suffolk University Law Review*, Vol. XLVI, 2013, http://suffolklawreview.org/wp-content/uploads/2013/02/OLeary_Note_PDF_Web.pdf.

Önok, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Prof. Dr. Nur Centel'e Armağan, İstanbul: Beta Yayınevi, 2013, ss. 1229-1270.

Perrin, Bertrand/Rémy, Marc/Roubaty, Romain, "Electronic Evidence in Swiss Criminal Procedure", *Digital Evidence and Electronic Signature Law Review*, Vol. 8, 2011, ss. 70-75.

Rohrmann, Carlos Alberto/Neto, Jason S. de Albergaria, "Digital Evidence and Electronic Lawsuits: How far do we go?", Sylvia Mercado Kierkegaard (ed.), *Cyberlaw, Security & Privacy*, 2. Baskı, Ankara: Ankara Barosu Yayınları, 2007.

Roxin, Claus, "İspat Hukukunun Esasları", Çev. Yener Ünver, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl: 4, Sayı: 8, Güz 2005/2, ss. 265-289.

Rozmus, Marcin/Topa, Ilona/Walczak, Marika, "Harmonisation of Criminal Law in the EU Legislation-The Current Status and The Impact of the Treaty of Lisbon", ss. 3-8, <http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf>.

Say, Kubilay, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", *Ses Görüntü ve Data İncelemeleri*, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008, s. 251-260.

Say, Kubilay, "Data İncelemeleri", Oğuz Karkuş (ed.), *Kriminalistik*, 2. Baskı, Ankara: Adalet Yayınevi, 2013, ss. 517-558.

Scholberg, Stein, "The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva", Aralık 2008.

Selinšek, Liljana, "Electronic Evidence in the Slovene Criminal Procedure Act", *Digital Evidence and Electronic Signature Law Review*, Vol. 7, 2010, ss. 77-86.

Solove, Daniel J./Richards, M. Neil, “Privacy’s Other Path: Recovering the Law of Confidentiality”, The Georgetown Law Journal, Vol. 96, 2007, ss. 124-182, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2078&context=faculty_publications.

Şahin, Cumhuriyet, “Telekomünikasyon Yoluyla İletişimin Denetlenmesi”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XI, Sayı: 1-2, 2007, ss. 1095-1112.

Şimşek, Mehmet Ali, “Delalet Kavramı Çerçevesinde Lafız ve Anlam İlişkileri”, Nüsha Şarkiyat Araştırmaları Dergisi, Yıl:1, Sayı:2, Yaz 2001, ss. 80-111.

Ünver, Yener, “Ceza Muhakemesinde İspat, CMK ve Uygulamamız”, Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, Aralık 2006, ss. 103-207.

Vandendriessche, Johan, “Belgian Cybercrime Provisions”, Digital Evidence and Electronic Signature Law Review, Vol. 9, 2012, ss. 173-177.

Yaşar, Yaşar/Dursun, İsmail, “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 19, S.3, 2013, ss. 3-34.

Yayla, Mehmet, “Ceza Yargılamasında İspat İçin Yenilmesi Gereken Şüphe”; Türkiye ve Amerika Birleşik Devletleri Sistemlerinin İncelenmesi, Ankara Barosu Dergisi, 2013/3, ss. 289-313.

Yetim, Servet, “Dijital Kanıt Araştırma Yöntemleri”, İstanbul Barosu Dergisi, Cilt: 82, Sayı: 3, 2008, ss. 1201-1221.

Yıldız, Ali Kemal, “Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu”, Ceza Hukuku Dergisi, Yıl: 1, Sayı: 2, Ankara, Aralık 2006, ss. 253-264.

Elektronik kaynaklar:

5237 sayılı Türk Ceza Kanunu gerekçesi,
<http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc>.

5271 sayılı Ceza Muhakemesi Kanunu genel gerekçesi,
<http://www.ceza-bb.adalet.gov.tr/mevzuat/cmkmaddegerekce.doc>.

A/RES/45/121, (14.12.1990),
<http://www.un.org/documents/ga/res/45/a45r121.htm>.

A/RES/46/152, (18.12.1991),
<http://www.un.org/documents/ga/res/46/a46r152.htm>.

A/RES/55/63, (04.12.2000),
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

A/RES/56/121, (19.12.2001),
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf.

A/RES/57/239, (20.12.2002),
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

A/RES/58/199, (23.12.2003),
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

A/RES/60/177, (16.12.2005),
https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/General_Assembly/A-RES-60-177.pdf.

A/RES/64/211, (21.12.2009),
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211.

ACPO Good Practice Guide for Computer Based Evidence,
<http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf>.

Adalet Bakanlığı Kanunlar Genel Müdürlüğü, Aylık Faaliyet Raporu (01.01.2012-31.01.2012),
<http://www.kgm.adalet.gov.tr/Faaliyetler/AyFaliyet/2012%20y%C4%B1%C4%B1/ocak2012/avr.pdf>.

Adalet Bakanlığı Kanunlar Genel Müdürlüğü, Aylık Faaliyet Raporu (01.03.2012-31.03.2012),
<http://www.kgm.adalet.gov.tr/Faaliyetler/AyFaliyet/2012%20y%C4%B1%C4%B1/Mart2012/avr.pdf>.

Avrupa Birliği Bakanlığı, Avrupa Birliği: Kurumlar,
http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_2_kurumlar/ab_kurumlar.pdf.

Charter of Fundamental Rights of the European Union,
http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Code de Procédure Pénale,
www.legifrance.gouv.fr/content/download/1958/13719/.../Code_34.pdf.

CoE Electronic Evidence Guide, 2013,
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/2467_EEG_v18protected.pdf.

COM (2007) 267 final, (22.05.2007),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

COM (2012) 140 final, (28.03.2012),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF>.

Computer Misuse Act,
<http://www.legislation.gov.uk/ukpga/1990/18/contents>.

Constitution of the United States,
http://www.senate.gov/civics/constitution_item/constitution.htm.

Convention on Cybercrime ETS no. 185,
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

Court of Justice of the European Union,
http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm.

Directive 95/46/EC, (24.11.1995),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

Directive 97/66/EC, (15.12.1997),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML>.

Directive 2006/24/EC, (15.03.2006),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

Directive 2011/92/EU, (13.12.2011),
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093&from=EN>.

Directive 2013/40/EU, (12.08.2013),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>.

Directive 2014/41/EU, (03.04.2014),
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0041&from=EN>.

ECOSOC Resolution 1992/1,
http://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-1_E.pdf

ECOSOC Resolution 1992/22,
http://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-22_E.pdf

Electronic Communications Privacy Act,
<http://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf>.

Evidence Act 1995,
http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/.

Federal Rules of Criminal Procedure,
http://judiciary.house.gov/_cache/files/86a03f0f-cbfb-4624-8029-b2eec078d211/criminal2014.pdf.

Federal Rules of Evidence,
<http://www.uscourts.gov/uscourts/rules/rules-evidence.pdf>.

Forensic Examination of Digital Evidence: A Guide for Law Enforcement,
<https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>.

Framework Decision 2005/222/JHA, (24.02.2005),
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN>.

Framework Decision 2008/978/JHA, (18.12.2008),
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF>.

Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU Publication, Eylül 2012,
<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>.

Hâkimler ve Savcılar İçin Siber Suç Eğitimi: Bir Kavram, AK Siber Suç Projesi ve Lizbon Şebekesi, Strasbourg, 2009,
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09_TUR.pdf.

HSYK, Hukuki Müzakere Toplantıları Ceza Hukuku Grubu Raporu, Denizli, 08.11.2013-10.11.2013,
<http://hmt.hsyk.gov.tr/toplantilar/2013/adli-yargi/guz/denizli/raporlar/5grup.pdf>.

HSYK, Yargıda Durum Analizi Toplantıları Sonuç Raporu, Ocak 2012,
<http://www.hsyk.gov.tr/dosyalar/Yargida-Durum-Analizi-Toplant%C4%B1lari-Sonuc-Raporu.pdf>.

JOIN(2013) 1 final, (07.02.2013) ,
http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Kişisel Verilerin Korunması Kanunu Tasarısı,
<http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf>.

Kızıroğlu, Serap Keskin, “Ceza Muhakemesi Hukukunda Bilişim Koruma Tedbirleri”, Kazancı Hukuk Eserleri Bilgi Bankası,
<http://www.kazanci.com/kho2/hebb/files/makale-serapkeskinkiziroglu-3.htm>.

Küzeci, Elif, “Anayasal Bir Hak: Kişisel Verilerin Korunması”, ss. 142-149,
<http://www.bilisimdergisi.org/s128/pdf/142-149.pdf>.

Özel, Cevat/Ahi, Gökhan, “Bilişim Suçları’nda Usul ve Sorumluluk Sistemi Üzerine Öneriler”, Kazancı Hukuk Eserleri Bilgi Bankası,
<http://www.kazanci.com/kho2/hebb/files/makale-cevatozel-mgokhanahi-1.htm>.

Police and Criminal Evidence Act,
<http://www.legislation.gov.uk/ukpga/1984/60/contents>.

Police and Justice Act,
<http://www.legislation.gov.uk/ukpga/2006/48/contents>.

RAND Europe & Lawford, Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs, Aralık 2005
ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf.

Regulation of Investigatory Powers Act,
<http://www.legislation.gov.uk/ukpga/2000/23/contents>.

Riley v. California 573 U.S. (2014),
<https://www.law.cornell.edu/supct/pdf/13-132.pdf>.

Rose, Kristina, Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, <https://www.ncjrs.gov/pdffiles1/nij/227050.pdf>.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.

Strafprozeßordnung (StPO),
http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

TDK BSTS Bilgisayar Terimleri Karşılıklar Kılavuzu,
http://www.tdk.gov.tr/index.php?option=com_bilimsanat.

TDK BSTS Bilişim Terimleri Sözlüğü,
http://www.tdk.gov.tr/index.php?option=com_bilimsanat.

TDK BSTS Kriminal Terimleri Sözlüğü,
http://www.tdk.gov.tr/index.php?option=com_bilimsanat.

Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation: A Guide for First Responders, Temmuz 2001
<https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>.

Telecommunications (Interception and Access) Act 1979
<http://www.comlaw.gov.au/Details/C2014C00786>.

The Commonwealth’s Crimes Act 1914
http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/.

The Treaty on the functioning of the European Union (TFEU), <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN>.

Türk Dil Kurumu Güncel Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts.

United Nations Manual on the Prevention and Control of Computer-Related Crime [UNMPCCRC],
<http://www.uncjin.org/Documents/irpc4344.pdf>.

United States v. Katz, 389 U. S. 347 (1967),
<http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/wiretaps-cell-phone-surveillance/facts-case-summary.aspx>.

Wegman, Jerry, “Computer Forensic: Admissibility of Evidence in Criminal Cases”, 2004,
<http://www.webpages.uidaho.edu/wegman/JerryWegmanPapers/Computer%20Forensics%20AA%202004.htm>.

Tezler:

Ünal, Osman Gazi, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara 2011.

Yıldız, Ali Kemal, “Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi”, Doktora Tezi, Tez Danışmanı: Kayıhan İçel, İstanbul, 2002.

Konferanslar:

Sieber, Ulrich, “Enformasyon Toplumu, Siber Suçlar ve Reform”, Siber Suçlar: Olgular, Önleme, Cezalandırma Konferansı, İstanbul, 12.04.2013.

AİHM kararları (HUDOC veritabanından alınmışlardır):

Ağaoğlu v. Turkey, 27310/95, 06.12.2005.
Craxi v. Italy (No.2), 25337/94, 17.07.2003.
Dragojevic v. Croatia, 68955/11, 15.01.2015.
Huvig v. France, 11105/84, 24.04.1990.
Kennedy v. UK, 26839/05, 18.05.2010.
Kopp v. Switzerland, 23224/94, 23.03.1998.
Kruslin v. France, 11801/85, 24.04.1990.
Malone v. UK, 8691/79, 02.08.1984.
Petri Sallinen and others v. Finland, 50882/99, 27.09.2005.
Prezhdarovi v. Bulgaria, 8429/05, 30.09.2014.

S. and Marper v. United Kingdom, 30562/04 and 30566/04, 04.12.2008.
 Smirnov v. Russia, 71362/01, 07.06.2007.
 Uzun v. Germany, 35623/05, 02.09.2010.
 Yuditskaya v. Russia, 5678/06, 12.02.2015.

ABAD kararları (CURIA veritabanından alınmışlardır.):

C-101/01 – Lindqvist.
 C-350/02 – Commission v Netherlands.
 C-176/03 – Commission v Council.
 C-524/06 – Huber.
 C-518/07 – Commission v Germany.
 C-553/07 – Rijkeboer.
 C-614/10 – Commission v Austria.
 C-131/12 – Google Spain and Google.
 C-288/12 – Commission v Hungary.
 C-291/12 – Schwarz.
 C-486/12 – X.
 C-212/13 – Ryneš.
 Joined Cases Digital Rights Ireland Ltd (C-293/12) v Minister for Communications,
 Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12)
 and Others.
 Opinion 2/13, Opinion pursuant to Article 218(11) TFEU.

AYM kararları:

AYM 18.06.2014 tarih ve 2013/7800 başvuru nolu kararı,
<http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/de3fd0d1-cced-4a35-8377-750ed661dd6b?wordsOnly=False>.

AYM 09.01.2015 tarih ve 2014/253 başvuru nolu kararı,
<http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/3820ebf9-5872-483d-b088-791694cadbb8?wordsOnly=False>.

Yargıtay kararları (Kazancı İçtihat Bilgi Bankası veritabanından alınmışlardır.):

Yargıtay 4. CD, E. 2004/8763, K. 2005/21445, T. 05.12.2005.
 Yargıtay 11. CD, E. 2005/6376, K. 2007/2551, T. 16.04.2007.
 Yargıtay 11.CD, E. 2008/16570, K. 2009/101, T. 28.01.2009.
 Yargıtay 9. CD, E. 2013/9110, K. 2013/12351, T. 09.10.2013.
 Yargıtay 13. CD, E. 2012/14783, K. 2013/28348, T. 10.10.2013.
 Yargıtay 8. CD, E. 2012/21817, K. 2013/25428, T. 24.10.2013.

ÖZGEÇMİŞ

Uğur Kaynakçioğlu 1988 yılında İzmir’de doğmuştur. Lise eğitimini Bornova Anadolu Lisesi’nde tamamlamıştır. Koç Üniversitesi Hukuk Fakültesi’nden 2012 yılında mezun olmuştur. Şu anda Galatasaray Üniversitesi’nde Kamu Hukuku Anabilim Dalı’nda yüksek lisans eğitimi görmektedir.

TEZ ONAY SAYFASI

Üniversite : Galatasaray Üniversitesi
Enstitü : Sosyal Bilimler Enstitüsü
Adı Soyadı : Uğur KAYNAKÇIOĞLU
Tez Başlığı : Ceza Muhakemesinde Dijital Deliller
Savunma Tarihi : 18.06.2015
Danışmanı : Doç. Dr. Vesile Sonay EVİK

JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı

İmza

Doç. Dr. Ümit KOCASAKAL



Doç. Dr. Vesile Sonay EVİK



Yrd. Doç. Dr. Murat Volkan DÜLGER



Enstitü Müdürü

Prof. Dr. M. Yaman ÖZTEK

