ISSN: 2667-5676 **e-ISSN:** 2667-6109

BİLİŞİM HUKUKU DERGİSİ

(BHD)

Cilt: 1 **Sayı: 1** **Haziran-2019**

Vol.: 1 No.: 1 June-2019

ADALET YAYINEVİ
Ankara - 2019

BİLİŞİM HUKUKU DERGİSİ
(ASBÜBHD)

ISSN: 2667-5676 **e-ISSN:** 2667-6109
Cilt: 1 Sayı: 1 **Vol.: 1 No.: 1**
Haziran-2019 **June-2019**

Dergi İletişim Bilgileri/ ASBÜBHD Contact Information:
ASBÜ Hukuk Fakültesi Dekanlığı
Hükümet Meydanı No: 2, 06030 Ulus, Altındağ, ANKARA
Tel: +90 312 596 44 44–45 **Fax:** +90 312 311 86 00
e-mail: bilisimhukukudergisi@asbu.edu.tr https://dergipark.org.tr/bilisimhukukudergisi

YAYINA HAZIRLAYAN
Adalet Yayınevi
Strazburg Caddesi No: 10/B Sıhhiye-Ankara
Tel: (0312) 231 17 00 Fax: (0312) 231 17 10
www.adalet.com.tr

Baskı
Ay-bay Kırtasiye İnş. Gıda Paz. ve Tic. Ltd. Şti.
Sertifika No: 33365
Tel: (0 312) 472 58 55 - Ankara

Basım Tarihi:
Temmuz, 2019

YAZIM KURALLARI

Sayfa Düzeni

1. Sayfa boyutu: A4
2. Kenar boşlukları: 4 taraftan 2,5 cm

Başlangıç

1. Makale başlığı: Amerigo Md BT, 15 pt., Tüm harfler büyük, Kalın, Ortalanmış.

2. Yazar adı: Amerigo Md BT, 13 pt., Kalın, Sağa yaslı, İlk harfler büyük, yıldız ile dipnotta yazarın mesleği,

3. Öz, Abstract ve Anahtar Kelimeler: Kalın, İlk harfler büyük

Metin

1. Metin içi başlıklar: Amerigo Md BT, 12 pt.

2. Başlık başındaki işaretler için yeni liste stili tanımlanması (Word'de Giriş sekmesinde paragraf kutucuğunun içinde üst sıradaki liste işareti/numaralandırma işaretlerinden çok düzeyli liste başlığı altında yeni liste stili tanımla daha sonra sol alttan biçimden numaralandırma seçeneği seçilecek) sıralaması:

   1. Seviye: Numaralandırma stili: **I, II, III**… Kalın, Tümü büyük harfler

   2. Seviye: Numaralandırma stili: **A, B, C**… Kalın, İlk harfler büyük

   3. Seviye: Numaralandırma stili: **1, 2, 3**... Kalın, İlk harfler büyük

   4. Seviye: Numaralandırma stili: **a, b, c**… Kalın, İlk harfler büyük

   5. Seviye: Numaralandırma stili: *i, ii, iii*... Normal, İlk harfler büyük, İtalik

   3. Ana metin: Palatino Linotype, 11 pt.

   4. Metin paragrafları: İlk satır 0,75 cm içeride, her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi 5nk paragraf sonrası 0 nk aralık, satır aralığı 1.

Dipnotlar

1. Dipnot: Palatino Linotype, 9 pt.

2. Dipnot paragrafları: Asılı 0,5 cm içeride, her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi 2 nk paragraf sonrası 0 nk aralık, Aynı stildeki paragraflar arasına boşluk ekleme seçeneği seçilmemiş, satır aralığı 1. Ancak aynı dipnotta birden çok paragraf verilecekse bu durumda söz konusu iki paragraf arasında aralık 0 olmalıdır (üstteki paragrafın paragraf ayarlarından "sonra" kısmı 0 nk, alttaki paragrafın ise "önce" kısmı 0 nk yapılmalıdır).

3. Dipnottaki cümle ile dipnotta sol baştaki numara arasında 1 boşluk bırakılmalıdır.

4. Dipnotta sonu nokta ile biten bir ifade varsa tekrar nokta konulmasına gerek yoktur, bunun haricinde herhangi bir işaretten sonra mutlaka nokta konulmalıdır.

5. Metin içerisinde gösterilen dipnot numaraları şayet bir noktalama işareti varsa onun hemen ardından boşluk bırakılmaksızın belirtilecektir.

- **Yanlış:** verilecektir[1]. **Doğru:** verilecektir.[1]

Kaynakça

1. Kaynakça ayrı sayfada başlayacaktır.

2. Alfabetik sıralı, Palatino Linotype, 11 pt.

3. Kaynakça paragrafları: 0,75 cm asılı (ilk satırdan sonraki satırlar 0,75 cm içeride), her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi aralık 3 nk paragraf sonrası aralık 0 nk, Aynı stildeki paragraflar arasına boşluk ekleme seçeneği seçilmemiş, satır aralığı 1.

Yazım şekline ilişkin yukarıdaki kurallara uygun olarak hazırlanmış örnek word formu için bkz.

http://dergipark.org.tr/download/journal-file/14834

Yazım-İmla Kuralları ve Atıf Usulü

1. Derginin yazım ve imla kurallarında Türk Dil Kurumunun yayınları ve kararları esas alınmaktadır.

2. Dipnot ve kaynakçalarda "The Chicago Manual of Style" atıf sistemi benimsenmiştir. Atıf sistemine ilişkin detaylı bilgi için bkz.

https://librarybestbets.fairfield.edu/citationguides/chicagonotes-bibliography#BookwithTwoorThreeAuthors

https://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

3. Eserin yayın dilinin Türkçe olması halinde atıf yapılırken;

- "and" yerine "ve"
- "unpublished" yerine "yayımlanmamış" veya "yayınlanmamış"
- "Anonymous" yerine "Anonim"
- birden fazla ciltten oluşan eserlerde "volume/vol." yerine "Cilt."
- "see" yerine "bkz."
- "in" yerine "iç."
- "accessed" yerine "erişim tarihi"
- "trans." yerine "çev."
- "edited by" yerine "editör"
- "translated by" yerine "çeviren"
- "interview by" ifadesi yerine "röportajı yapan"
- "PhD diss." yerine "doktora tezi"
- "thesis" yerine "tez"
- "last modified" yerine "son değiştirilme"
- "filmed" yerine "çekim" ifadeleri kullanılmalıdır.
- Tarih belirtirken kullanılan ay isimleri Türkçeleştirilmiştir ancak yazım formatı korunmuştur. Örneğin; Mayıs 8, 2019 şeklinde yazılmalıdır.
- Dergi sayısını ifade eden "no." ifadesi korunmuştur. Keza "ed." ifadesi aynen korunmuştur.
- Sayfa numarasında "vd." kullanılmamalıdır. Bunun yerine ilgili numara ile arasına boşluk konulmaksızın "*ff.*" İfadesi konulmalıdır. Eğer "*ff.*"dan sonra "." gelecekse kullanılmaz ancak ";", "?" vb. gelecekse onlar "*ff.*"deki noktaya bitişik yazılır.

4. Metin içerisinde dipnotta gösterilen mevzuat veya mahkeme kararı kaynakçada gösterilmeyecektir. Yargı kararlarına yapılan atıflarda aşağıdaki kural ve kısaltmalar dikkate alınmalıdır:

- Mahkemenin/kurumun adı varsa dairesi, E. esas numarası K. karar numarası tarih[gün.ay.yıl formatında], (kararın ulaşıldığı kaynak, varsa ulaşıldığı kaynaktaki sayfa numarası veya URL veya DOI numarası).

- Yabancı kararlarda ilgili mahkemenin veya kurumun kendisinin benimsemiş olduğu karar atıf usulü kullanılabilir. Eğer tercih edilirse Türk kararları için kullanılan sistem de uygun düştüğü ölçüde uygulanabilir. Ancak, bir eserde aynı mahkemenin veya kurumun bir kararı için hangi sistematik kullanılmışsa diğer kararlarında aynı sistematiğin kullanılması gerekir.

Anayasa Mahkemesi	AYM
Bireysel Başvuru	BB
Bölge Adliye Mahkemesi	BAM
Ceza Dairesi	CD
Ceza Genel Kurulu	CGK
Daire	D
Danıştay	Dan.
Esas	E.
Hukuk Bölümü	HukukB
Hukuk Dairesi	HD
Hukuk Genel Kurulu	HGK
İçtihadı Birleştirme Kurulu	İBK
İçtihatları Birleştirme Büyük Genel Kurulu	İBK
İdari Dava Daireleri Kurulu Kararı	İDDK
Karar	K.
Uyuşmazlık Mahkemesi	UM
Vergi Dava Daireleri Kurulu Kararı	VDDK
Yargıtay	Yar.

Örnekler:

AYM, E.2017/172, K.2018/32, 28.03.2018.

Yar. 1. HD, E.2015/1456, K.2017/7086, 05.12.2017, (Kazancı İçtihat ve Bilgi Bankası).

Ankara BAM 2. HD, E.2016/113, K.2017/21, 23.01.2017, (https://legalbank.net/belge/ankara-bolge-adliye-mahkemesi-2-hd-e-2016-113-k-2017-21-t-23-01-2017-bosanmadan-kaynaklanan-tazminat/3040600).

Rekabet Kurulu, K.19-12/136-60, 13.3.2019, (https://www.rekabet.gov.tr/Karar?kararId=c4268558-edce-48b5-996d-152defb6a7e4).

5. Resmi Gazeteye yapılacak atıflar şu şekilde belirtilmelidir: RG. 02.01.2019, S. 30643.

WRITING FORM

Page Layout

1. Size: A4

2. Margins: 2,5 cm from all sizes

Beginning

1. Main text: Times New Roman 12 pt.

2. Title of the works: Times New Roman 12 pt., bold and capital letter, centered paragraph style, 1.5 line spacing, paragraph spacing after 10 nk.

3. Names(s) of author(s): Times New Roman 12 pt., bold, first letter capital, right justified. job of author(s) shall be written with an actinoid footnote. Name(s) of author(s) shall be written after one line space from the title of the work.

4. Öz, Abstract: Bold and first letter capital

5. Anahtar Kelimeler, Keywords: Bold and first letter capital, 1,25 inside

Text

1. Titles in the text: Times New Roman 12 pt.

2. Authors should arrange the text utmost with five-degree heading and the number of the titles has a style as follows:

First level: Numbering style: I, II, III... Alignment: 0 cm, Text indent: 1 cm, Title: bold and capital letter.

Second level: Numbering style: A, B, C... Alignment: 0,8 cm, Text indent: 1,8 cm, Title: bold and first letter capital.

Third level: Numbering style: 1, 2, 3... Alignment: 1,6 cm, Text indent: 2,6 cm, Title: bold and first letter capital.

Fourth level: Numbering style: a, b, c... Alignment: 2,4 cm, Text indent: 3,4 cm, Title: bold and first letter capital.

Fifth level: Numbering style: i, ii, iii... Alignment: 3,2 cm, Text indent: 4,2 cm, Title: italic and first letter capital.

3. Paragraphs: 1,25 cm first line indent, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 0 nk, 1.5 line spacing

4. Page number**:** centered and at the bottom of the page.

Footnotes

1. Style: 10 pt., Times New Roman

2. Footnotes paragraphs: 0,5 cm first line indent, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 6 nk, 1 line spacing. The box for adding space to same styled paragraphs should not be filled. If there are more than one paragraph in a footnote, pre/post-paragraph space should be 0 nk in this footnote.

3. Between the footnote number and footnote text one character space should be left.

4. All footnotes should be completed with a dot.

5. Footnotes numbers should be demonstrated after punctuations.

- **False:** ... given[1]. **True:** ... given.[1]

Bibliography

1. Bibliography should start on a separate page.

2. Style: alphabetically ordered, 12 pt., Times New Roman.

3. The title of "Bibliography" should be as centered and bold character.

4. Bibliography paragraphs: 1,25 cm hanging indentation, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 10 nk, 1 line spacing. The box for adding space to same styled paragraphs should not be filled.

For the sample word form edited aptly *writing form rules* of ASBÜ BHD, please see at http://dergipark.org.tr/download/journal-file/14834

Spelling and Footnotes Rules

1. The works should be prepared aptly the spelling and orthographic rules of Turkish Language Association. See at http://tdk.gov.tr/

2. "The Chicago Manual of Style" is accepted for footnotes and bibliography. For further information please see at

https://librarybestbets.fairfield.edu/citationguides/chicagonotes-bibliography#BookwithTwoorThreeAuthors

https://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

DEKANIN MESAJI

ASBÜ Hukuk Fakültesi birinci sınıf öğrencileri, ilk Türkiye Büyük Millet Meclisi'nin kurularak demokrasinin temellerinin atıldığı, Türkiye Cumhuriyeti'nin üzerine inşa edildiği kamu binalarında 2019-2020 eğitim öğretim yılında öğrenime başlamaktadır. ASBÜ Hukuk Fakültesi olarak akademik kadromuz, eğitim ve idari binalarımız ile yeni öğretim yılına hazırlanmaktayız. Bunun yanında bilim dünyasına katkı sunmak, Bilişim Hukuku alanındaki çalışmaları ve bu alandaki yenilikleri teşvik ederek gündeme taşımak amacıyla Fakültemiz bünyesinde Bilişim Hukuku Dergisi (ASBÜ BHD) ve Hukuk Fakültesi Dergisi (ASBÜ HFD) Haziran 2019'da yayın hayatına başlamaktadır.

Kamu Hukuku ve Özel Hukuk ayrımının yeterince işlevsel olmadığı ortaya çıkmasının da bir sonucu olarak, gelişen dünyadaki her bilim dalında olduğu gibi hukuk alanında da daha spesifik alanların öne çıkarılması elzem olmuştur. Bu anlamda Bilişim Hukuku görece yeni bir hukuk alanıdır. Hukukun birçok alanını ilgilendiren bu hukuk dalı da bir devlet üniversitesinde ilk kez ASBÜ Hukuk Fakültesi bünyesinde "Bilişim ve Teknoloji Hukuku Ana Bilim Dalı" ile daha da ileriye taşınacaktır.

Gerçek yaşamda olduğu gibi "sanal âlem" denilen dünyada da kurallara uygun davranmak gerekmektedir. Bu alanda sonsuz ve sınırsız bir özgürlük tanımlaması yapılamaz. Kişilik haklarının korunması, bu açıdan üzerinde dikkatle durulması gereken bir konudur. Kişilik haklarının öznesi olarak insan, dijital dünyanın savunmasız çocuğu pozisyonunda kalmamalıdır. Bilişim Hukuku, başta Sosyal Medya Hukuku olmak üzere İnternet Hukuku, Telekomünikasyon Hukuku, Elektronik Ticaret Hukuku, Bilişim Ceza Hukuku, Siber Güvenlik Hukuku, Kişisel Veriler Hukuku, Erişim Engelleme Hukuku, E-Devlet, E-İmza, gibi alanlardan oluşmaktadır.

ASBÜ Hukuk Fakültesi bünyesinde yayımlanan her iki derginin ilk sayılarının ortaya çıkmasında yazıları ile katkı ve destek sunan öğretim elemanlarına, derginin idari ve bilimsel alt yapısının hazırlanmasında emeklerini esirgemeyen editör ve editörler kuruluna, makalelerin değerlendirilmesinde emek veren danışma ve hakem kurulumuza, derginin dizgiye hazırlanması ve yayımlanmasını üstlenen Adalet Yayınevi çalışanlarına teşekkür ederim.

Prof. Dr. Bülent KENT
Ankara Sosyal Bilimler Üniversitesi
Hukuk Fakültesi Dekanı

İÇİNDEKİLER / TABLE OF CONTENTS

MAKALE BÖLÜMÜ

MAKALE
BÖLÜMÜ

TELEKOMMUNİKATİONSÜBERWACHUNGSMAßNAHME IN DER TÜRKISCHEN STRAFPROZESSORDNUNG - ANHAND ART. 8 EMRK

Türk Ceza Muhakemesi Hukukunda İletişimin Denetlenmesi Tedbiri- AİHS 8. Maddesi Işığında

Çiler Damla BAYRAKTAR*

Zusammenfassung

Der EGMR hat in vielen Rechtsprechungen zu geheimen Überwachungsmaßnahmen zur Vermeidung von Machtmissbrauch neben die Bestimmungen zur „Art der Straftaten, die eine Überwachungsanordnung rechtfertigen können", zu den „Personengruppen, bei denen die Maßnahme Anwendung findet" und zur „Begrenzung der Dauer der Maßnahme" auch Bestimmungen über „die Umstände, unter denen die Aufzeichnungen gelöscht und die Bänder vernichtet werden müssen oder dürfen", in den gesetzlichen Regelungen als Mindestgarantien entwickelt.

Die Vorschriften der Telekommunikationsüberwachungsmaßnahme in der Türkischen Strafprozessordnung sind trotz der Gesetzesänderungen vom 21.02.2014, 02.12.2014 und 24.11.2016, in Hinblick auf die Anforderungen des EGMR immer noch mangelhaft.

* Doktor Öğretim Üyesi, Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, cilerdamla. bayraktar@asbu. edu.tr, ORCID: 0000-0002-7611-5088.

Makale Gönderim Tarihi: 12.02.2019

Makale Kabul Tarihi: 23.04.2019.

Schlüsselwörter: Telekommunikationsüberwachungsmaßnahme in der türkischen Strafprozessordnung, §135 der türkischen Strafprozessordnung, Mindestgarantien in den gesetzlichen Regelungen, die Bestimmungen zur ‚Art der Straftaten', die Bestimmungen zu den „Personengruppen, die Bestimmungen zur „Begrenzung der Dauer der Maß¬nahme", Bestimmungen über „die Umstände unter denen die Aufzeichnungen gelöscht und die Bänder vernichtet werden müssen oder dürfen".

Öz

Avrupa İnsan Hakları Mahkemesi gizli denetleme tedbirlerine ilişkin vermiş olduğu pek çok kararında denetleme yapılmasını hukuka uygun kılacak nitelikteki suç tiplerine ilişkin belirlemelerin, denetleme tedbirinin uygulanabileceği kişi gruplarına ilişkin belirlemelerin ve tedbirin süresinin sınırlanmasına ilişkin belirlemelerin yanı sıra tutulan kayıtların silinmesi ve bantların yok edilmesi gereken durumlara ilişkin belirlemelerin yetkinin kötüye kullanılmasının önüne geçilmesi adına minimum garantiler olarak tedbirin uygulanmasına yetki veren yasal temelde öngörülmesi gerektiğini ifade etmiştir.

Türk Ceza Muhakemesi Kanununda düzenli iletişimin denetlenmesi tedbiri (CMK 135) 21.02.2014 tarihli, 02.12.2014 tarihli ve 24.11.2016 tarihli yasa değişikliklerine rağmen Avrupa İnsan Hakları Mahkemesinin bu talepleri açısından hala bazı yönleri itibariyle eksiktir.

Anahtar Kelimeler: İletişimin Denetlenmesi Tedbiri, CMK m. 135, Avrupa İnsan Hakları Mahkemesi, Avrupa İnsan Hakları Mahkemesinin İletişimin Denetlenmesi Tedbirinin Yasal Temelinde Aradığı Minimum Garantiler, Tedbirin Uygulanabileceği Suç Kategorisinin Belirlenmesi, Tedbirinin Uygulanabileceği Kişi Gruplarının Belirlenmesi, Tedbirin Süre Sınırının Belirlenmesi, Tutulan Kayıtların Silinmesi ve Bantların Yok Edilmesi Gereken Durumların Belirlenmesi.

I. EINLEITUNG

Telekommunikationsüberwachungsmaßnahme[1] ist eine der wichtigsten Maßnahmen in Rechtsordnungen, weil das Medium der Telekommunikation häufig zur Begehung bzw. Vorbereitung von Straftaten benutzt wird und der Eingriff mit seinem heimlichen Charakter zu einem entsprechenden Erfolg führt.[2]

Telefongespräche im häuslichen und im geschäftlichen Umfeld ist Bestandteil der Privatsphäre. Diese grundsätzlich als Bestandteil der Privatsphäre behandelten Telefongespräche sind seit der Entscheidung im Fall *Klass* folgendermaßen eher Bestandteil des Rechts auf Achtung des Briefverkehrs.[3]

Im Fall *Klass*, in dem es um das Abhören und Aufzeichnen von Telefongesprächen ging, hat der EGMR die Reichweite des Rechts auf Achtung des Briefverkehrs auf jede andere Kommunikationsform ausgedehnt,[4] indem er feststellt, dass jede Kommunikationsform, die innerstaatlich vergleichbar wie die Post geregelt und geschützt ist und unabhängig von der Schriftlichkeit, auch im Sinne von Art. 8 als „correspondence" qualifiziert werden kann.[5]

---

1 Für die detaillierten Ausführungen über die Telekommunikationsüberwachungsmassnahme in der türkischen Strafprozessordnung vgl. Çiler Bayraktar, *Eingriffe in die Privatsphäre durch technische Überwachung Ein deutsch-türkischer Vergleich anhand Art. 8 EMRK* (Hamburg: Dr. Kovac, 2017), 411*ff.*

2 *Bär*, MMR 2000, 472 (473*ff.*).

3 Vgl. hierzu EGMR, Urteil vom 06.09.1978 – Klass u.a. gegen Deutschland, http://www.eugrz.info/pdf/EGMR31.pdf; Jochen Abr. Frowein, „Art. 8 EMRK," in *Europäische Menschenrechtskonvention EMRK- Kommentar*, hrsg. Jochen Abr. Frowein und Wolfgang Peukert (Baden: Engel N.P., 2009), 290, Rn. 6.

4 EGMR, Urteil vom 06.09.1978 – Klass u.a. gegen Deutschland, http://www.eugrz.info/pdf/EGMR31.pdf; später ebenso EGMR, Urteil vom 02.08.1984 – Malone gegen Vereinigtes Königsreich, http://www.eugrz.info/ PDF/EGMR2/ urteil39.pdf.

5 Frowein, „Art. 8 EMRK," 314, Rn. 48; für detaillierte Informationen zu diesem Fall vgl. Stephan Breitenmoser, *Der Schutz der Privatsphäre gemäß Art. 8 EMRK das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs* (Frankfurt am Main: Helbing u. Lichtenhahn, 1986), 185*ff.*

Heute werden Telefongespräche einschließlich der Internet-Telefonie unter den Begriff „Briefverkehr" gefasst[6] und fallen zusammen mit den Kommunikationsvorgängen per E-Mail oder Pager[7] auch unter den Schutz des Rechts auf Achtung des Briefverkehrs des Art. 8 EMRK,[8] wodurch neben dem Inhalt individueller Kommunikation, von dem die am Kommunikationsvorgang Beteiligten selbst bestimmen können müssen, wer Kenntnis erlangen soll, der Kommunikationsvorgang, also die näheren Umstände des Fernmeldeverhältnisses, beispielsweise die Tatsache, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist, geschützt werden.[9]

Allerdings steht das Recht auf Achtung des Briefverkehrs nach Abs. 2 Art. 8 dem Bürger nicht schrankenlos zur Verfügung. Das heißt, die Telekommunikationsüberwachungsmaßnahmen sind in bestimmten Fällen zulässig.

Insofern wird bei dieser Arbeit zuerst die Grundlagen der Rechtfertigung des Eingriffs in das Recht auf Achtung des Briefverkehrs, bzw. die Zulässigkeit einer Telekommunikationsüberwachungsma ßnahme nach Abs. 2 Art. 8 EMRK dargelegt. Dementsprechend werden zweitens die Vorschriften der Telekommunikationsüber

---

6 Frowein, „Art. 8 EMRK," Frowein, „Art. 8 EMRK," 314, Rn. 48; EGMR, Urteil vom 06.09.1978 – Klass u.a. gegen Deutschland, http://www.eugrz.info/pdf/EGMR31.pdf.

7 EGMR, Urteil vom 22.10.2002 – Taylor-Sabori gegen Vereinigtes Königreich, Rn. 18, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60696#{"itemid":["001-60696"]}.

8 Thilo Marauhn und Judith Thorn, „Kapitel 16: Privat- und Familienleben," in *EMRK/GG Konkordanzkommentar*, hrsg. Oliver Dörr, Rainer Grote und Thilo Marauhn (Tübingen: Mohr Siebeck, 2013), Rn. 62; EGMR, Urteil vom 09.07.2009 – Kvasnica gegen Slovakia, Rn. 76, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-92879#{"itemid":["001-92879"]}.

9 EGMR, Urteil vom 01.03.2007 – Heglas gegen die Tschechische Republik, Rn. 61, http://hudoc.echr.coe.int/eng#{"itemid":["001-79650"]}; Juliane Pätzold, „Recht auf Achtung des Privat- und Familienleben," in *EMRK Konvention zum Schutz der Menschenrechte und Grundfreiheiten*, hrsg. Ulrich Karpenstein und Franz C. Mayer (München: C. H. Beck, 2015), Art. 8 EMRK, Rn. 36.

wachungsmaßnahme in Türkischer StPO (CMK) auf die Maßgaben der EMRK basierend geprüft.

II. DIE GRUNDLAGEN DER RECHTFERTIGUNG DES EINGRIFFS IN DAS RECHT AUF ACHTUNG DES BRIEFVERKEHRS NACH ABS. 2 ART. 8 EMRK

Eingriffe in die Rechte aus Art. 8 Abs. 1 EMRK, bzw. in das Recht auf Achtung des Briefverkehrs, ist nach Art. 8 Abs. 2 EMRK gerechtfertigt, wenn der Eingriff gesetzlich vorgesehen und zur Verfolgung eines der in Art. 8 Abs. 2 EMRK genannten Ziele in einer demokratischen Gesellschaft notwendig ist.[10]

Im Rahmen des Gesetzesvorbehaltsmerkmals des Art. 8/2 setzt der Gerichtshof bei der Rechtfertigung des Eingriffs eine vorhersehbare und zugängliche gesetzliche Grundlage voraus.

Eine Rechtsgrundlage des Eingriffs ist ausreichend zugänglich, wenn es dem Bürger möglich ist, die einschlägigen Rechtsnormen zu ermitteln und ihren Inhalt – beziehungsweise welches die Rechtsnormen sind, die in einem bestimmten Fall anwendbar sind – zu erfahren.[11]

Im Hinblick auf die Maßgabe der Vorhersehbarkeit muss die gesetzliche Grundlage eines Grundrechtseingriffs so bestimmt sein, dass der Bürger die Umstände und die Bedingungen behördlichen Handelns voraussehen, sein Verhalten dem Gesetz entsprechend einrichten und die Folgen seines Handelns voraussehen kann.[12]

---

[10] Marauhn und Thorn, „Kapitel 16," Rn. 79; Robert Uerpmann-Wittzack, „Höchstpersönliche Rechte und Diskriminierungsverbot," in *Europäische Grundrechte und Grundfreiheiten*, hrsg. Dirk Ehlers (Berlin: De Gruyder, 2014), 90, Rn. 25.

[11] EGMR, Urteil vom 26.04.1979 – Sunday Times gegen Vereinigtes Königreich, Rn. 49, EGMR-E, Band 1, 366*ff.*; Thilo Marauhn und Katrin Merhof, „Kapitel 7: Grundrechtseingriff und –schranken," in *EMRK/GG Konkordanzkommentar*, hrsg. Oliver Dörr, Rainer Grote und Thilo Marauhn (Tübingen: Mohr Siebeck, 2013), Rn. 29.

[12] Christoph Grabenwarter und Katharina Pabel, *Europäische Menschenrechtskonvention*, vol. 3 (München: C.H. Beck, 2016), §18. Struktur der Grundrechtsprüfung, Rn. 11; Mark Ennulat, *Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und –einrichtungen* (Bern: Peter Lang,2008), 59.

Vorhersehbarkeit bedeutet aber nicht, dass das Gesetz alle Einzelheiten regeln muss: Besonders im Hinblick auf geheime Überwachungsmaßnahmen räumt der Gerichtshof den Vertragsstaaten einen Ermessenspielraum ein, und als Vorhersehbarkeitsanforderungen verlangt es, dass das Gesetz einen Minimalschutz gegen Willkür bietet.[13]

Besonders für staatliche Telefonüberwachungsmaßnahmen hat der EGMR wegen der schwerwiegenden Beeinträchtigung des Privatlebens und der Korrespondenz im Hinblick auf die Klarheit und Präzision der gesetzlichen Grundlage bestimmt,[14] dass sie insbesondere den betroffenen Personenkreis – also wer in seiner Kommunikation kontrolliert werden kann –, die Straftatbestände, die eine Abhörmaßnahme nach sich ziehen können, zeitliche Grenzen von Abhörmaßnahmen, das Verfahren für die Erstellung der Abhörprotokolle – also welche Stellen über diese Kontrolle entschieden und in welcher Art und Weise –, die Aufbewahrung und Bereithaltung der Aufzeichnungen für eine Überprüfung durch Gerichte und die Verteidigung sowie die Umstände, unter denen die Aufnahmen gelöscht oder Bänder zerstört werden dürfen, genau bezeichnen muss.[15]

Nach Art. 8 Abs. 2 EMRK muss zudem eine Beschränkungsregelung in einer demokratischen Gesellschaft notwendig sein. Aber es zeigt sich eine Unbestimmtheit in Bezug auf den offenen Rechtsbegriff der Notwendigkeit in einer demokratischen Gesellschaft, obwohl das Begriffspaar „demokratische Gesellschaft" mit den ihr

---

[13] Anne Peters, *Einführung in die Europäische Menschenrechtskonvention* (München: C. H. Beck, 2003), 23; Robert Esser, „EMRK/IPBPR," in Löwe-Rosenberg stopp, vol. 11 (Berlin: De Gruyder, 2012), Art. 8 EMRK, Rn. 82; EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 151ff., https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 28.06.2007 – Ekimdzhiev gegen Bulgarien, Rn. 74, https://hudoc.echr.coe.int/eng#{"itemid":["001-81323"]}.

[14] Vgl. Esser, „EMRK/IPBPR," Art. 8 EMRK, Rn. 81: Die allgemeine gesetzliche Ermittlungsbefugnis der Polizei stellt keine Grundlage dar.

[15] Marauhn und Thorn, „Kapitel 16," Rn. 84; Anne Peters und Tilmann Altwicker, *Europäische Menschenrechtskonvention* (München: C. H. Beck, 2012), 197, Rn. 13.

innewohnenden Prinzipien dazu dient, die Grenze zu ziehen zwischen noch tolerablen nationalen Abweichungen und Verstößen gegen die Konvention, d. h. zwischen legitimen Grundrechtseinschränkungen und Verletzungen des demokratischen Kerns und Wesensgehalts.[16]

In diesem Sinne ist die Notwendigkeit des Eingriffs für den konkreten Zweck aus der Sicht der Werte einer demokratischen Gesellschaftsordnung zu beurteilen. Sie ist also an einem Staatsverständnis zu messen, das vom Leitbild einer Demokratie geprägt ist, in der das Verhältnis zwischen Staat und Bürger von typischen Wertvorstellungen wie Toleranz, Pluralismus und Anerkennung der Grundrechte und insbesondere von dem Grundsatz der Verhältnismäßigkeit beherrscht wird.[17]

Danach soll der Eingriff aus der Sicht eines demokratischen Staatsbildes einem dringenden gesellschaftlichen Bedürfnis entsprechen, um das berechtigte Ziel zu erreichen.[18] Es genügt nicht, wenn sie aus der Sicht einer demokratischen Gesellschaft nur nützlich oder zweckmäßig erscheint[19], denn die Konvention verlangt eine Notwendigkeit, also mehr als Nützlichkeit oder Zweckmäßigkeit.[20]

---

16 Luzius Wildhaber und Stephen Breitenmoser, „Art. 8 EMRK," in *Internationaler Kommentar zur Europäischen Menschenrechtskonvention*, hrsg. Katharina Pabel und Stefanie Schmahl (Köln: Carl Heymanns Verlag, 2010), 251, Rn. 729; vgl. auch *Von Bogdandy* und andere, ZaöRV 2012, 45 (70).

17 Walter Gollwitzer, *Menschenrechte im Strafverfahren MRK und IPBPR Kommentar* (Berlin: De Gruyder, 2005), Art. 8, 459, Rn. 20; Marauhn und Merhof, „Kapitel7," Rn. 53.

18 Jens Meyer-Ladewig, *EMRK Europäische Menschenrechtskonvention Hand Kommentar* (Basel: Helbing Lichtenhahn, 2011), EMRK Art. 8, Rn. 109ff.; Florian Fischer, *Rheinischer Kommentar zur Europäischen Menschenrechtskonvention Privat- und Familienleben* (Berlin: Logos, 2015), Art. 8 EMRK, Rn. 11.

19 EGMR, Urteil vom 13.08.1981 – Young, James, Webster gegen Vereinigtes Königsreich, Rn. 63, http://www.eugrz.info/pdf/EGMR49.pdf; Frowein, „Art. 8 EMRK," 284, Rn. 14.

20 Gollwitzer, *Menschenrechte*, Art. 8, 459, Rn. 20; Esser, „EMRK/IPBPR," Art. 8 EMRK, Rn. 41 und Rn. 54.

Dieses hat der EGMR bei seinen Rechtsprechungen mehrfach betont[21] und dadurch gefördert, dass der Eingriff in Bezug auf die durch das Gesetz bestimmten zulässigen Zwecke verhältnismäßig sein soll,[22] weil durch diese Klausel der Ermessensspielraum der öffentlichen Gewalt auf ein vernünftiges Maß beschränkt wird.

Bei der Beurteilung bzw. bei der Wahl der Maßnahme, ob diese Maßnahme „notwendig in einer demokratischen Gesellschaft" ist – also ob ein „dringendes soziales Bedürfnis" besteht[23], haben die Konventionstaaten nach ständiger Rechtsprechung einen gewissen Ermessensspielraum.[24]

Allerdings wurde dieser weite Ermessensspielraum durch den EGMR begrenzt, wenn durch die Maßnahme in die innerste Privatsphäre eingegriffen wird:[25] Der EGMR prüfte bei der Rechtfertigungsabwägung neben dem abstrakt einschlägigen Beschränkungsziel die konkret vorliegenden schwerwiegenden Gründe.[26]

Beim Datenschutz und im Kontext der informationellen Selbstbestimmung ist es bedeutungsvoll für den Gerichtshof, um welche Art von Daten es sich jeweils handelt und welche Bedeutung diese für den Persönlichkeitskern haben.[27]

---

21 EGMR, Urteil vom 07.12.1976 – Handyside gegen Vereinigtes Königsreich, Rn. 48, EGMR-E, Band 1, 217*ff*.; EGMR, Urteil vom 22.10.1981 – Dudgeon gegen Vereinigtes Königsreich, Rn. 50ff., http://www.eugrz.info/PDF/ EGMR2/urteil1.pdf.

22 Urteil vom 25.03.1983 – Silver gegen Vereinigtes Königsreich, Rn. 97, EGMR-E, Band 2, 227*ff*.

23 Uerpmann-Wittzack, „Höchstpersönliche Rechte," 90, Rn. 25.

24 EGMR, Urteil vom 07.12.1976 – Handyside gegen Vereinigtes Königsreich, Rn. 48, EGMR-E, Band 1, 217*ff*.; Meyer-Ladewig, *Menschenrechtskonvention*, EMRK Art. 8, Rn. 118; Angelika Nußberger, „Das Verhältnismäßigkeitsprinzip als Strukturprinzip richterlichen Entscheidens in Europa," *NVwZ-Beilage* 1, (2013): 42.

25 Vgl. hierzu Ennulat, *Datenschutzrechtliche*, 37; Esser, „EMRK/IPBPR," Art. 8 EMRK, Rn. 55.

26 Marauhn und Thorn, „Kapitel 16," Rn. 98; Pätzold, „Recht auf Achtung des Privat," Art. 8 EMRK, Rn. 103.

27 Marauhn und Thorn, „Kapitel 16," Rn. 98, und Rn. 24; Grabenwarter und Pabel, *Menschenrechtskonvention*, §22. Rechte der Person, Rn. 45.

Zusammen mit dem Begriff der Notwendigkeit bedingt die „demokratische Gesellschaft" die Anwendung des Verhältnismäßig keitsprinzips.[28] Danach *„erscheint eine Eingriffsmaßnahme als verhältnismäßig, wenn sie – zur Erreichung eines der acht in Art. 8 Abs. 2 aufgeführten Ziele – ‚notwendig in einer demokratischen Gesellschaft' ist"*.[29] Erscheint eine Eingriffsmaßnahme in der Geeignetheits- und Erforderlichkeitsabwägung im engeren Sinn als nicht verhältnismäßig, dann dürfte sie auch unter dem Aspekt der Demokratie keine Rechtfertigung erfahren.[30] Allerdings wendet der EGMR[31] das Prüfungsraster, das sich durch eine Erforderlichkeits-, Geeignetheits- und Angemessenheitsabwägung auszeichnet, in einer geringsten Ausdifferenzierung an,[32] und konzentriert sich auf die letzte Stufe der Angemessenheit, eine faire Abwägung durch eine Zweck-Mittel-Relation.[33]

Der EGMR strukturiert die Angemessenheitsprüfung, die den Kern der Verhältnismäßigkeitskontrolle bzw. die Rechtfertigung eines Eingriffs bildet, zwar nicht detailliert, jedoch wägt er die jeweils einschlägigen öffentlichen und privaten Güter und Interessen umfassend gegeneinander ab.[34] Dabei verlangt er „fair Balance" – vor allem bei Eingriffen in das Recht auf Privat- und Familienleben –

---

[28] Für die Bestimmung als „Schrankenschranke" siehe Fischer, *Rheinischer Kommentar*, Art. 8 EMRK, Rn. 10.

[29] Wildhaber und Breitenmoser, „Art. 8 EMRK," 249, Rn. 722; Grabenwarter und Pabel, *Menschenrechtskonvention*, §18. Struktur der Grundrechtsprüfung, Rn. 14.

[30] Wildhaber und Breitenmoser, „Art. 8 EMRK," 249, Rn. 722.

[31] Für eine detaillierte Überprüfung der Kontrolle der Verhältnismäßigkeit durch den Europäischen Gerichtshof vgl. *Kischel*, EuR 2000, 380 (380ff.).

[32] Vgl. Nußberger, „Das Verhältnismäßigkeitsprinzip,"42.

[33] Peters und Altwicker, *Menschenrechtskonvention*, 191, Rn. 7; *Koutnatzis*, VRÜ 2011, 32 (37); Julia Iliopoulos-Strangas, „Die allgemeinen Rechtsgrundsätze in der Praxis der Straßburger Organe am Beispiel des Verhältnismäßigkeitsprinzips," *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, nu. 63 (1999): 449ff.; Jürgen Kühling, „Grundrechte," in *Europäisches Verfassungsrecht*, hrsg. Armin von Bogdandy und Jürgen Bast (Heidelberg: Springer, 2009), 693*ff.*; EGMR, Urteil vom 25.02.1997 – Z gegen Finnland, Rn. 94ff., http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58033#{"itemid":["001-58033"]}

[34] Marauhn und Merhof, „Kapitel7," Rn. 51*ff.*

und prüft, ob der Eingriff „in einem angemessenen Verhältnis" zu dem damit verfolgten legitimen Ziel steht,[35] und ob die von den innerstaatlichen Behörden zur Rechtfertigung angeführten Gründe „relevant und ausreichend" sind.[36]

Zusammenfassend heißt das: Das Merkmal „in einer demokratischen Gesellschaft notwendig zu sein", das Art. 8 Abs. 2 EMRK voraussetzt, hat eine bedeutende Rolle bei der Verhältnismäßigkeitsabwägung einer Eingriffsmaßnahme. Abgesehen davon hat der EGMR durch seine Rechtsprechung einen anderen Maßstab aus dem Prinzip der demokratischen Gesellschaft entwickelt, der auch bei der Abwägung der Zulässigkeit eines Eingriffs bedeutend ist: die Wesensgehaltslehre (the very essence of the Right).

In der Literatur wird vertreten, dass diese Wesensgehaltslehre als Schrankenschranke dient, weil dadurch die Beschränkungen der Rechtsgüter in einem vernünftigen Maße beschränkt werden,[37] und im Hinblick auf deren Bedeutung wird so dargelegt, dass die Einschränkungen von Konventionsgarantien den Substanz- und Wesensgehalt solcher Rechte nicht aushöhlen dürfen.[38]

Weil durch diese Telekommunikationsüberwachungsma ßnahmen in das Recht auf Achtung des Privatlebens und das Recht auf Achtung des Briefverkehrs des Art. 8 EMRK eingegriffen werden, sollen die

---

35 Peters, *Einführung*, 24, 155; Esser, „EMRK/IPBPR," Art. 8 EMRK, Rn. 54.

36 EGMR, Urteil vom 22.10.1981 – *Dudgeon* gegen Vereinigtes Königsreich, Rn. 53ff., http://www.eugrz.info/PDF/EGMR2/urteil1.pdf; EGMR, Urteil vom 07.12.1976 – Handyside gegen Vereinigtes Königsreich, Rn. 53ff., EGMR-E, Band 1, S. 217ff.; EGMR, Urteil vom 26.10.1995 – Vogt gegen Deutschland, Rn. 53*ff*., http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58012#{"itemid":["001-58012"]}; Frowein, „Art. 8 EMRK," 286, Rn. 15*ff*.

37 Eckart Klein, „§ 150: Der Schutz der Grund- und Menschenrechte durch den Europäischen Gerichtshof für Menschenrechte," in *Handbuch der Grundrechte in Deutschland und Europa Europäische Grundrechte*, vol. 6/1, hrsg. Detlef Merten und Hans-Jürgen Papier (Heidelberg: C. F. Müller, 2010), 606, Rn. 26; Mustafa Yıldız,"Avrupa İnsan Hakları Mahkemesi'nin İşlevsel Konumu," *Anayasa Yargısı Dergisi* 14, (1997): 318.

38 Vgl. hierzu Wildhaber und Breitenmoser, „Art. 8 EMRK," 11, Rn. 4; Esser, „EMRK/IPBPR," Art. 8 EMRK, Rn. 56.

zu dieser Maßnahme die Ermächtigungsgrundlage darstellenden Gesetze insofern die Anforderungen des EGMR an die Vorhersehbarkeit und Zugänglichkeit sowie an die „Notwendigkeit in einer demokratischer Gesellschaft" erfüllen. Wie oben bereits dargelegt, muss hier grundsätzlich die Anwesenheit der Sicherheitsordnungen und der Grundsatz der Verhältnismäßigkeit beachtet werden bzw. ein angemessener Ausgleich zwischen der Schwere der grundrechtlichen Beeinträchtigung, der Bedeutung des mit der Maßnahme verfolgten öffentlichen Anliegens und den Interessen der Betroffenen hergestellt werden.[39]

Im Folgenden werden die Ermächtigungsgrundlagen der Türkischen Rechtsordnung im Lichte der EGMR-Urteile überprüft.

III. TELEKOMMUNİKATİONSÜBERWACHUNGSMAßNAHME NACH DER TÜRKİSCHEN RECHTSORDNUNG

Die aus Sicht der Praxis wichtige Eingriffsbefugnis, „den Inhalt eines Kommunikationsvorgangs aufzuzeichnen",[40] ist in § 135ff. CMK geregelt.[41] Jedoch ordnen diese Vorschriften dabei auch die Bewertung der Signalisierung und die Feststellung der Telekommunikation.

Im Folgenden wird zuerst im allgemein die Telekommunikationsüberwachungsmaßnahme nach § 135ff. CMK dargelegt. Danach werden diese Vorschriften im Hinblick auf die Vorhersehbarkeit

---

[39] Marauhn und Merhof, „Kapitel7," Rn. 43, 51; Peters, *Einführung*, 24.

[40] Für Informationen zu diesen Maßnahmen in Amerika, Österreich, Frankreich, England, Schweiz und Italien, vgl. Zeki Vatan, *Ceza Muhakemesi Hukukunda Koruma Tedbiri Olarak Iletişimin Denetlenmesi* (İstanbul: Beta Yayınevi, 2009), 46*ff.*

[41] Vgl. Cumhur Şahin, *Ceza Muhakemesi Hukuku 1* (Ankara: Seçkin Yayıncılık, 2015), 349*ff.*; Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku*, Cilt. 1 (Ankara: Adalet Yayınevi, 2016), 743; Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku* (İstanbul: Beta Yayınevi, 2015), 445*ff.*; Kunter, Nurullah, Feridun Yenisey ve Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku* (İstanbul: Beta Yayınevi, 2010), 789*ff.*

und Zugänglichkeit sowie im Hinblick auf die Notwendigkeit in einer demokratischen Gesellschaft nach den Anforderungen des EGMR geprüft, bzw. ob die Vorschriften einen Minimalschutz gegen Mißbrauch und Willkür bieten.

A. Gesetzliche Grundlage

Im Dezember 2013 begann in der Türkei der Korruptionsskandal, in dessen Folge zahlreiche Personen aus dem engsten Umfeld der Türkischen Regierungspartei Adalet ve Kalkınma Partisi (AKP) festgenommen wurden. Unter ihnen waren auch die Söhne des Innen-, des Umwelt- und des Wirtschaftsministers sowie der Geschäftsführer der staatseigenen Halkbank, Süleyman Aslan.[42]

Ministerpräsident Erdoğan und die Regierung sprachen von einer Schmutzkampagne gegen sich und behaupteten, dass der in den Vereinigten Staaten lebende islamische Prediger Fethullah Gülen und seine sogenannte Gülen-Bewegung in die Exekutive und Judikative eingesickert wären und illegale Telekommunikationsüberwachungen durchgeführt hätten.[43] Als Reaktion enthob die Regierung zahlreiche hohe Polizeibeamte, darunter den Polizeichef von Istanbul, ihres Amtes und versetzte über 400 weitere.[44]

Daraufhin ermittelte die Staatsanwaltschaft aus Istanbul und stellte im Rahmen ihrer Ermittlungen fest, dass in der Tat mehrere nicht registrierte Telekommunikationsüberwachungen durch die Polizei stattgefunden hatten. Ein Staatsanwalt habe unter dem Deckmantel der Ermittlungen gegen eine fiktive Terrororganisation

---

42 Vgl. hierzu Cem Tursun, Serpil Kırkeser ve Arzu Kaya, „Üç bakan oğluna tutuklama talebi," Hürriyet, Veröffentlichung: Dezember 20, 2013, http://www.hurriyet.com.tr/uc-bakan-ogluna-tutuklama-talebi-25409906.

43 Vgl. hierzu Tarihin en büyük dinleme skandalı, in: Haber7com, Veröffentlichung: 24.02.2014, http://www.haber7.com/guncel/haber/1131046-tarihin-en-buyuk-dinleme-skandali

44 Vgl. hierzu Çetin Aydın, Fevzi Kızılkoyun ve Banu ŞEN, "Sadece İki İlde 1700 Polisin Yeri Değişti," Hürriyet.com, Veröffentlichung: Januar 07, 2014, http://www.hurriyet.com.tr/gundem/25515006.asp.

namens „Selam Terror Organisation" die Telekommunikation von ungefähr 7000 Personen, darunter Ministerpräsident Erdoğan und seiner Angehörigen, vieler Politiker, Journalisten, Autoren und Unternehmer drei Jahre lang überwacht. Hierbei wurde gegen „X", also gegen unbekannt ermittelt.[45]

Zwar wurde daraufhin § 135 CMK durch das Gesetz Nr. 6526 am 21.02.2014 sowie durch das Gesetz Nr. 6572 am 02.12.2014 geändert[46] und wurden dadurch die Voraussetzungen für die Anordnung einer Telekommunikationsüberwachungsmaßnahme strenger gemacht, aber einige dieser Voraussetzungen wurden durch das Gesezt Nr. 6763[47] am 24.11.2016 wieder rückgängig gemacht.

Hier wird die aktuelle Version berücksichtigt.

Am Anfang wird dargelegt, was das Gesetz vorsieht, damit die Defizite nachher bei der Prüfung der Notwendigkeit in einer demokratischen Gesellschaft besser nachvollziehbar sind.

Dem Wortlaut des § 135 Abs. 1 CMK zufolge ist ausdrücklich hervorgehoben, dass die Maßnahme nur gegen Beschuldigte oder Angeklagte zulässig ist.[48]

---

45 Vgl. hierzu Tarihin en büyük dinleme skandalı, in: haber7com, Veröffentlichung: 24.02.2014, http://www.haber7.com/guncel/haber/1131046-tarihin-en-buyuk-dinleme-skandali.

46 Vgl. hierzu § 12 des Gesetzes Nr. 6526, http://www.resmigazete.gov.tr/eskiler/2014/03/20140306M1-1.htm und § 42 des Gesetzes Nr. 6572, https://www.tbmm.gov.tr/kanunlar/k6572.html.

47 Vgl. hierzu § 26 des Gesetzes Nr. 6763, http://www.resmigazete.gov.tr/eskiler/2016/12/20161202-1.htm.

48 Für detaillierte Informationen hierzu vgl. Seydi Kaymaz, *Ceza Muhakemesinde Telekomunikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (Ankara: Seçkin Yayıncılık, 2015), 175; vgl. hierzu auch Şen. „die Maßnahme im türkischen Recht, die Kommunikation zu beaufsichtigen" in *das Strafrecht im Deutsch–Türkischen Rechtsvergleich*, hrsg. Eric Hilgendorf und Yener Ünver (İstanbul: Yeditepe Üniversitesi Hukuk Fakültesi, 2010), 911; Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku* (İstanbul: Beta Yayınevi, 2013), 405*ff.*; Veli Özer Özbek et al., *Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayıncılık, 2015), 459; vgl. hierzu auch Yar. 4. CD, E. 2006/4669, K. 2006/17007, 29.11.2006, (http://legalbank.net/belge/y-4-cd-e-2006-4669-k-2006-17007-t-29-11-2006-tehdit-ve-hakaret-su-199-u/286870/).

Zu den Voraussetzungen über die Lage, wann Telekommunikation abgehört, aufgezeichnet und die Signale der Telekommunikation bewertet werden dürfen, hat der § 135 Abs. 1 CMK dargelegt, dass diese Maßnahmen nur angeordnet werden, soweit ein auf konkreten Beweisen beruhender starker Grund für einen Tatverdacht (strong grounds for suspicion) dafür vorlag, dass eine der unter § 135 Abs. 8 CMK aufgezählten Katalog-Straftaten begangen wurde[49] und wenn die Lieferung eines Nachweises auf andere Weise nicht möglich wäre.

In der Alten Fassung[50] wurde nur der „starke Grund für einen Tatverdacht" vorausgesetzt und die Bedeutung dieses Begriffs viele Male diskutiert: Ob man diesen Begriff „starker Grund für einen Tatverdacht" so verstehen soll, dass der Verdächtige mit großer Wahrscheinlichkeit verurteilt wird, haben *Öztürk et al.* geprüft und hervorgehoben, dass, wenn dem so wäre, diese Maßnahme gegen das Verhältnismäßigkeitsprinzip verstoßen würde. Denn wenn es genug Beweise für die wahrscheinliche Verurteilung des Verdächtigen gäbe, wäre die Anordnung einer solchen Maßnahme ohnehin nicht erforderlich.[51]

Auf der anderen Seite heben *Centel/Zafer* hervor, dass „starker Grund für einen Tatverdacht" bedeute, dass der Beschuldigte mit großer Wahrscheinlichkeit verurteilt werde.[52]

Außerdem schlägt *Kunter* vor, dass hier Tatverdacht und Vorzeichen zu unterscheiden sind. Insofern stellt er fest, dass für die Anordnung dieser Telekommunikationsüberwachungsmaßnahme ein „einfa-

---

[49] Nevzat Toroslu ve Metin Feyzioğlu, *Ceza Muhakemesi Hukuku* (Ankara: Şavaş Yayınevi, 2013), 254*ff*.; wobei nach Abs. 6 § 135 CMK die Telekommunikationsverkehrsdaten für alle Delikte abgeruft werden können, vgl. hierzu: Şahin, *Ceza Muhakemesi*, 354*ff*.; Bahri Öztürk et al., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayıncılık, 2015), 535*ff*.

[50] Vor der Gesetzesänderung durch das Gesetz Nr. 6526 am 21.02.2014.

[51] Vgl. hierzu Öztürk et al., *Ceza Muhakemesi*, 539, in dieser Richtung siehe auch Kunter, Yenisey ve Nuhoğlu, *Muhakeme*, 801*ff*.

[52] Vgl. hierzu Centel ve Zafer, *2015*, 435; vgl. auch Ünver ve Hakeri, *Ceza Muhakemesi*, 710.

cher" Tatverdacht schon ausreicht, wobei dort die Vorzeichen in Bezug darauf, dass dort eine Straftat begangen wird, kräftig sein sollen.[53]

Diese Debatten sind immer noch aktuell, da es diesen Begriff in der neuen Version des § 135 CMK immer noch gibt.

Nach Abs. 4 §135 CMK sind in der Entscheidungsformel der Anordnung der Name des Betroffenen, gegen den sich die Maßnahme richtete, die Art und die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, die Art und der Umfang sowie die Dauer der Maßnahme anzugeben.

Die Durchführungen der Maßnahmen können höchstens zwei Monate lang dauern und die Dauer der Maßnahmen können nur für einen Monat verlängert werden, es sei denn, es betrifft eine organisierte Straftat. Insoweit kann die Dauer der Maßnahmen zusätzlich jedes Mal höchstens einen Monat lang, und insgesamt drei Monate lang verlängert werden. (Abs. 4 § 135 CMK).

Nach Abs. 2 § 135 ist bei der Durchführung der Maßnahmen – das Abhören und Aufzeichnen der Telekommunikation sowie die Bewertung der Signale einer Telekommunikation – ein Beleg oder ein Gutachten über den Eigentümer oder den Benutzer der durch die Maßnahmen betroffenen Telekommunikationsgeräte oder des Netzwerks einzureichen.

Angesichts der Tatsache, dass der Staatsanwalt in seinen Ermittlungen gegen die fiktive[54] Terrororganisation „Selam-Tevhid" viele Personen bei der Anordnungsformel der Maßnahme lediglich als „X" bezeichnete,[55] fügte der Gesetzgeber diesen Absatz hinzu. Da-

---

53 Vgl. Kunter, Yenisey ve Nuhoğlu, *Muhakeme*, 801*ff.*; vgl. hier auch Feridun Yenisey ve Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayıncılık, 2015), 439*ff.*; Özbek et al., *Ceza Muhakemesi*, 458.

54 Das Verfahren zur Terrororganisation „Selam-Tevhid" wurde am 21.07.2014 eingestellt, vgl. hierzu „Selam-tevhid davasında 251 kişiye takipsizlik," Haber7, Veröffentlichung: Juli 22, 2014, http://www.haber7.com/hukuk/haber/1183375-selam-tevhid-davasinda-251-kisiye-takipsizlik.

55 Vgl. hierzu „MİT Müsteşarı Fidan'ı "Emin" kod adıyla dinlediler," Türkiye, Veröffentlichung: Juli 23, 2014. http://www.turkiyegazetesi.com.tr/ gundem/173435.aspx.

durch soll vermieden werden, dass die Telekommunikation von Personen überwacht wird, welche nicht einer Straftat verdächtig sind sowie dass die Telekommunikationsüberwachung durch fingierte oder erfundene Namen erfolgt.[56]

Diese Maßnahmen dürfen nach Abs. 1 des § 135 CMK durch einen Richter, oder bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet werden. In dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hat, soll er „sofort" seine Entscheidung für die Genehmigung bei dem Richter einreichen. Der Richter soll innerhalb von 24 Stunden darüber entscheiden. Wenn diese eingeräumte Frist von 24 Stunden ohne eine Entscheidung des Richters abläuft, oder wenn der Richter gegenteilig entscheidet, wird die von der StA bei Gefahr im Verzug angeordnete Maßnahme aufgehoben.

B. Sonderstellung für die Maßnahme „Feststellung der Telekommunikation"

Demgegenüber wurde die „Feststellung der Telekommunikation" als eine Maßnahme im Abs. 1 des § 135 CMK nicht aufgezählt. Daraus ergibt sich, dass für den Abruf der Telekommunikationsverkehrsdaten die Voraussetzung, dass ein „auf konkreten Beweisen beruhender starker Grund für einen Tatverdacht vorliegen müsse", nicht erforderlich ist.[57]

Außerdem wird nach Abs. 6 des § 135 CMK die Maßnahme „Feststellung der Telekommunikation" eines Beschuldigten oder Angeklagten im Ermittlungsverfahren von einem Richter und bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet, wobei dies im Hauptverfahren durch ein Gericht angeordnet wird. In der Entscheidungsformel der Anordnung sind die Art der vorgeworfenen Straftat, der Name des Betroffenen, gegen den sich die Maßnahme richtet, die Art und die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes

---

[56] Vgl. Ünver ve Hakeri, *Ceza Muhakemesi*, 721.

[57] Vgl. Yenisey ve Nuhoğlu, *Ceza Muhakemesi*, 445. Für die gegenseitige Ansicht vgl. Özbek et al., *Ceza Muhakemesi*, 475.

sowie die Dauer der Maßnahme anzugeben. Jedoch wurden in der Vorschrift keine Höchstdauer oder ein Zeitlimit angewiesen.[58] In dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hat, soll er seine Entscheidung innerhalb von 24 Stunden für die Genehmigung bei dem Richter einreichen. Der Richter soll innerhalb von 24 Stunden darüber entscheiden. Wenn diese eingeräumte Frist von 24 Stunden ohne eine Entscheidung des Richters abläuft, oder wenn der Richter gegenteilig entscheidet, wird die von der StA bei Gefahr im Verzug angeordnete Maßnahme aufgehoben.

Nach § 135 Abs. 3 kann die Telekommunikation zwischen den Zeugnisverweigerungsberechtigten und den Beschuldigten oder Angeklagten nicht aufgezeichnet werden. Wenn dies nach der Aufzeichnung bemerkt wird, werden die Aufzeichnungen sofort vernichtet.

Noch eine Beschränkung hat der CMK im Rahmen der Verteidigergespräche gestellt. Danach ist für die Telekommunikationsgeräte, die sich in der Wohnung, dem Büro oder der Niederlassung des Verteidigers befinden, der § 135 CMK nicht durchführbar (§ 136 Abs. 1 CMK).

Verfahrensregelungen über die Durchführung dieser Maßnahmen hat der Gesetzgeber in § 137 CMK folgendermaßen festgestellt:

1- Die Durchführung der Maßnahmen „Abhören, Aufzeichnung oder Feststellung der Telekommunikation" muss von der StA oder von ihm befugten Angestellten schriftlich von dem Telekommunikationsdienstanbieter verlangt werden (§ 137 Abs. 1).

2- Über das Datum und die Uhrzeit des Beginns und des Endes der Durchführung der Maßnahmen sowie die Identität der die Maßnahme durchführenden Person wird ein Protokoll erstellt (§ 137 Abs. 1).

3- Die Aufzeichnungen, die im Rahmen der angeordneten Maßnahmen erlangt wurden, verarbeiten die von der StA beauftragten Personen und wandeln diese Aufzeichnungen in einen schriftlichen Text um (§ 137 Abs. 2).

---

[58] Özbek et al., *Ceza Muhakemesi*, 475.

4- Die Durchführung der Maßnahme wird von der StA sofort aufgehoben, wenn der StA die Ermittlung während der Durchführung der Maßnahme einstellt. Dies gilt auch in dem Fall, wo der StA die Maßnahme bei Gefahr im Verzug selbst angeordnet hat, jedoch die Genehmigung des Richters nicht einholen konnte. Hier werden die Aufzeichnungen zu der Feststellung oder das Abhören der Telekommunikation unter Kontrolle der Staatsanwaltschaft in 10 Tagen vernichtet und der Fall der Vernichtung protokolliert (§ 137 Abs. 3). In diesem Fall wird der Betroffene von der Einstellung des Ermittlungsverfahrens an – aber auf jeden Fall nach der Vernichtung der Aufzeichnungen über die Feststellung oder das Abhören der Telekommunikation – innerhalb von 15 Tagen schriftlich über den Umfang, den Grund, die Dauer und das Ergebnis der Maßnahme von der Staatsanwaltschaft benachrichtigt (§ 137 Abs. 4).

§ 138 TCK[59] sieht weiterhin eine zwei- bis vierjährige Freiheitsstrafe für Ermittlungspersonen vor, welche die im Rahmen einer Telekommunikationsüberwachung erlangten personenbezogenen Daten nicht löschen.

5- Wird bei der Durchführung der Maßnahme ein Nachweis über die Begehung einer anderen als der verfolgten Straftat erlangt, wird dieser an den Staatsanwalt weitergeleitet, wenn diese neu in Kenntnis gebrachte Straftat eine von den in §135 CMK aufgezählten Straftaten ist (§138 Abs. 2).

C. Die Prüfung der §§ 135ff. CMK nach den Anforderungen des EGMR

1. Im Rahmen der Zugänglichkeit und Vorhersehbarkeit der gesetzlichen Grundlage

Das CMK ist ein schon veröffentlichtes parlamentarisches Gesetz in der Türkei.[60] Insofern erfüllt es die Anforderungen des EGMR an die Zugänglichkeit einer gesetzlichen Grundlage.

---

[59] Türkisches StGB.

[60] Das Gesetz ist http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf.

Jedoch ist umstritten, ob diese Vorschrift die Anforderung der Vorhersehbarkeit erfüllt.

Die Tatsache, dass das Abhören von Telekommunikation, die Aufzeichnung und die Beurteilung der Signale einer Telekommunikation nur bei Vorliegen eines qualifizierten Tatverdachts darüber, dass eine Straftat begangen wurde, angeordnet werden dürfen, ist bedeutungsvoll im Rahmen der Anforderungen der Rechtsprechung des EGMR an eine Beschränkung der Macht der öffentlichen Gewalt.[61] Jedoch ist diese Bestimmung der Tatverdachtsqualifizierung des *auf konkreten Beweisen beruhenden starken Grunds für einen Tatverdacht* nicht klar genug. Wie schon erwähnt, gibt es viele Debatten darüber, was das bedeutet. Insofern ist festzustellen, dass durch diese Bestimmung gegen die Anforderungen des EGMR an die „Vorhersehbarkeit der gesetzliche Grundlage"[62] verstoßen wird.

Allerdings ist im Sinne der Maßnahme „Feststellung der Telekommunikation" die Voraussetzung, dass ein auf „konkreten Beweisen beruhender starker Grund für einen Tatverdacht" vorliegen müsse nicht erforderlich. Im Hinblick auf diese Maßnahme kann nämlich festgestellt werden, dass die Ermächtigungsgrundlage sowohl zugänglich als auch vorhersehbar ist.

---

61 EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 43 und 51, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{"itemid":["001-91245"]}; dafür, dass diese Bestimmung in der inneren Rechtsordnung dem Verhältnismäßigkeitsgrundsatz Rechnung trägt, vgl. Şahin, *Ceza Muhakemesi*, 354.

62 EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 151, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 28.06.2007 – Ekimdzhiev gegen Bulgarien, Rn. 74, http://hudoc.echr.coe.int/eng?i=001-81323#{"itemid":["001-81323"]}; EGMR, Urteil vom 27.09.2005 – Petri Sallinen u.a. gegen Finnland, Rn. 76*ff*., http://hudoc.echr.coe.int/ sites/eng/ pages/search.aspx?i=001-70283#{"itemid":["001-70283"]}.

2. Im Rahmen der „Mindestanforderungen des EGMR gegen Mißbrauch und Willkür "und des Merkmals „Notwendigkeit in einer demokratischen Gesellschaft"

a. Ein Katalog mit Straftaten, die eine Überwachungsanordnung rechtfertigen

Nach dem EGMR ist ein Katalog mit Straftaten, die eine Überwachungsanordnung rechtfertigen, erforderlich.[63]

Nach dieser Vorschrift (CMK § 135) dürfen die Maßnahmen des Abhörens von Telekommunikation, der Aufzeichnung sowie der Beurteilung der Signale der Telekommunikation nur für die unter § 135 CMK aufgezählten Straftaten angeordnet werden (§ 135 Abs. 1 CMK).

Zwar macht der Gesetzgeber über die Schwere der Straftaten keine Angaben, es kann aber ganz klar gesagt werden, dass die Schwere des Eingriffs mit der Schwere der aufgezählten Straftaten im Einklang steht. Schließlich werden dabei nicht nur Straftaten gegen die Staatsordnung, die Verfassungsordnung und das Staatsgeheimnis aufgezählt, sondern auch Totschlag, Folter, Sex-Überfall, Sex-Überfall auf Minderjährige, Raub, Rauschgifthandel, Geldfälschung, Korruption, Waffenschmuggelei, Erschleichung sowie Straftaten, die im Kultur- und Naturwesensschutzgesetz angeordnet werden, und Straftaten, die im Schmuggeleibekämpfungsgesetz aufgezählt und mit Freiheitsstrafe bedroht sind.

Bei der Vorschrift wurde zwar nach der Änderung durch das Gesetz Nr. 6526 vom 21.02.2014 eine in der alten Fassung vorhandene Straftat, nämlich „eine Vereinigung oder Bande zu bilden, um Straftaten zu begehen", entfernt, mit der Begründung, dass das Tatbestandsmerkmal ansonsten als Auffangtatbestand fungieren würde

---

63 EGMR, Urteil vom 24.04.1990 – Huvig gegen Frankreich, Rn. 34, https://hudoc.echr.coe.int/eng#{"fulltext":["\"CASE OF HUVIG v. FRANCE\""],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57627"]}; EGMR, Urteil vom 29.06.2006 – Weber und Saravia gegen Deutschland, Rn. 125*ff*., http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001- 76586# {„itemid":[„001-76586"]}.

und somit für alle Straftaten, welche nicht ausdrücklich unter § 135 CMK aufgezählt werden, die Anordnung einer Telekommunikationsmaßnahme erleichtern würde.[64] Diese Änderung wurde aber mit der Änderung durch das Gesetz Nr. 6763 vom 24.11.2016 wieder rückgängig gemacht und die Straftat „eine Vereinigung oder Bande zu bilden, um Straftaten zu begehen" wieder in den Strafkatalog aufgenommen.

Zudem wurden durch § 42 des Gesetzes Nr. 6572 vom 02.12.2014 weitere zwei Änderungen an dem Strafkatalog vorgenommen: Die Delikte „bewaffnete Bandenkriminalität" (§ 314 TCK) und „Beihilfe zur bewaffneten Bandenkriminalität (durch Beschaffung der Waffen)" (§ 315 TCK) wurden aus dem Straftatenkatalog entfernt, stattdessen wurde das Delikt „Die Einigkeit des Staates und seiner Gesamtheit zerstören" (§ 302 TCK) in diesen Katalog aufgenommen (§ 135 Abs. 8 Nummer 15 CMK). Zweitens wurde als § 135 Abs. 8 Nummer 16 CMK ein neues Delikt dem Straftatenkatalog hinzugefügt: „Straftaten gegen das Grundgesetz und die durch dieses geschaffene Ordnung" (§§ 309, 311, 312, 313, 314, 315, 316 TCK).

Außerdem wurden durch das Gesetzes Nr. 6526 vom 21.02.2014 das Delikt qualifizierter Diebstahl (§ 142 StGB) und Plünderung (§148, 149 StGB) in den Strafkatalog aufgenommen (CMK §135 Abs. 8 (a) Nr.6).

Zuletzt wurden durch das Gesetz Nr. 6763 vom 24.11.16 weitere drei Änderungen an dem Strafkatalog vorgenommen, danach wurden in den § 135 Abs. 8 (a) Nr. 6. das Delikt qualifizierter Betrug (§ 158 StGB) in den Absatz 8 (a) Nr. 1 das Delikt Organ oder Gewebe Handel (§ 91 StGB) und in den Absatz 8 (a) Nr. 12 das Delikt Wucher (§ 241 StGB) aufgenommen.

Dass in der Vorschrift die Katalogfälle aufgelistet sind und dadurch die Straftaten in vernünftigem Maß beschränkt wurden, trägt auch den Anforderungen der EGMR-Rechtsprechungen Rechnung. Jedoch ist die Bestimmung des Gesetzes, dass diese Maßnahme für die Straftaten, die im Schmuggeleibekämpfungsgesetz aufgezählt und

---

64 vgl. hierzu Şahin, *Ceza Muhakemesi*, 269.

mit Freiheitsstrafe bedroht sind, angeordnet werden darf [135 CMK Abs. 8 (d)], im Hinblick auf die Vorhersehbarkeit der Vorschrift kritisch zu behandeln, da dabei die Paragrafen von Straftaten nicht ausdrücklich bestimmt sind, obwohl bei den anderen Straftaten ausdrücklich auf die Paragrafennummern hingewiesen wurde.

Zudem wird auch kritisch behandelt, dass Erpressung und Bedrohung, die besonders häufig durch das Medium Telefon begangen werden, dabei nicht aufgezählt wurden.[65]

Auf der anderen Seite setzt der Gesetzgeber für die Anordnung der Maßnahme „Feststellung der Kommunikation" keine Katalogstraftaten voraus (§ 135 Abs. 6). Dass diese Maßnahme ohne eine Beschränkung im Hinblick auf das Gewicht der Straftaten angeordnet werden darf, räumt ein unbegrenztes Ermessen ein, und erfüllt nicht die Anforderungen des EGMR.[66]

Außerdem ist die Bestimmung des Gesetzgebers in Abs. 2 des § 138 verwirrend. Danach sind die bei der *Überwachung der Telekommunikation* zufälligerweise erlangten Nachweise über die Begehung einer Straftat, die eine andere als die verfolgte ist, aufzubewahren und der StA mitzuteilen, soweit diese neu in Erfahrung gebrachte Straftat eine von den in § 135 CMK aufgezählten Straftaten ist.

Auf den ersten Blick kann man sagen, dass diese Bestimmung ebenso den Anforderungen des EGMR Rechnung trägt, da die Maßnahmen nur auf diese aufgezählten Katalogfälle beschränkt sind. Jedoch ist es angesichts dessen, dass die Überschrift von § 135 CMK „Überwachung der Telekommunikation" und der Untertitel „Feststellung, Abhören und Aufzeichnung der Telekommunikation" lauten, ganz klar, dass dem Begriff „Überwachung der Telekommuni-

---

[65] Özbek et al., *Ceza Muhakemesi*, 430; Veli Özer Özbek, *CMK Izmir Şerhi Yeni Ceza Muhakemesinin Anlamı* (Ankara: Seçkin Yayıncılık, 2005), 566.

[66] EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 43, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}; EGMR, Urteil vom 24.04.1990 – Huvig gegen Frankreich, Rn. 34, https://hudoc.echr.coe.int/eng#{"fulltext":["\"CASE OF HUVIG v. FRANCE\""],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57627"]}.

kation" auch der Begriff „Feststellung der Telekommunikation" zugehört. Wenn man im Lichte dieser Feststellung den Abs. 2 des § 138 CMK interpretiert, hat man die Folgerung, dass die während der Durchführung der Maßnahme „Feststellung der Telekommunikation" zufälligerweise erlangten Nachweise über die Begehung einer Straftat, die eine andere als die verfolgte ist, aufzubewahren und der StA mitzuteilen sind, soweit diese neu in Erfahrung gebrachte Straftat eine von den in § 135 CMK aufgezählten Straftaten ist, obwohl der Gesetzgeber für die Anordnung der Maßnahme „Feststellung der Kommunikation" in Abs. 6 des § 135 keine Katalogstraftaten voraussetzt. Diese verwirrenden Bestimmungen des Gesetzgebers sind auch im Hinblick auf die Vorhersehbarkeit der gesetzlichen Grundlage zu berücksichtigen.

b. Die Bestimmung der Personengruppen

Nach dem EGMR ist es auch erforderlich, dass die gesetzliche Grundlage die Personengruppen, deren Telefongespräche abgehört werden können, bestimmt, damit die gesetzliche Grundlage die Mindestanforderungen erfüllt.[67]

Nach dem Wortlaut des § 135 Abs. 1 CMK ist ausdrücklich hervorgehoben, dass die Maßnahmen „Abhören und Aufzeichnen der Telekommunikation sowie die Bewertung der Signale der Telekommunikation" nur gegen Beschuldigte oder Angeklagte zulässig sind.

Zudem hat das Gesetz dadurch, dass in der Entscheidungsformel der Anordnung der Name des Betroffenen, gegen den sich die Maßnahme richtet, die Art und die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, die Art und der Umfang sowie die Dauer der Maßnahme anzugeben

---

[67] EGMR, Urteil vom 04.05.2000 – Rotaru gegen Rumänien, Rn. 56*ff.*, https://hudoc.echr.coe.int/eng#{"itemid":["001-58586"]}; EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 160, https://hudoc.echr.coe.int/eng#{"itemid":["001-98473"]}; EGMR, Urteil vom 24.04.1990 – Huvig gegen Frankreich, Rn. 34, https://hudoc.echr.coe.int/eng#{"fulltext":["\"CASE OF HUVIG v. FRANCE\""],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57627"]}.

sind, sichergestellt, dass die Maßnahmen nur gegen den Beschuldigten oder Angeklagten durchgeführt werden.

Dass nach Abs. 2 des § 135 bei der Durchführung der Maßnahmen – Abhören und Aufzeichnung der Telekommunikation sowie die Bewertung der Signale einer Telekommunikation – ein Beleg oder ein Gutachten über den Eigentümer oder den Benutzer der durch die Maßnahme betroffenen Telekommunikationsgeräte oder des Netzwerks einzureichen ist, trägt der Anforderung des EGMR Rechnung.

Auf der anderen Seite sind die Bestimmungen zu der Maßnahme „Feststellung der Telekommunikation" insofern nicht so anders: Für diese Maßnahme sieht die Vorschrift im Abs. 6 des § 135 CMK auch vor, dass die Betroffenen von dieser Maßnahme nur die jeweils Beschuldigten oder Angeklagten sind.[68] Zudem sieht der Gesetzgeber auch vor, dass in der Entscheidungsformel der Anordnung die Art der vorgeworfenen Straftat, der Name des Betroffenen, gegen den sich die Maßnahme richtet, die Art und die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes anzugeben sind. Dass der Gesetzgeber für diese Maßnahme, abweichend von den anderen Telekommunikationsmaßnahmen, nicht verlangt, dass ein Beleg oder ein Gutachten über den Eigentümer oder den Benutzer der durch die Maßnahme betroffenen Telekommunikationsgeräte oder des Netzwerks einzureichen ist, bedeutet nicht, dass diese Bestimmungen die Anforderungen des EGMR nicht erfüllen. Schließlich hat der EGMR im Fall Kennedy ausdrücklich hervorgehoben, dass bei der Entscheidungsformel der Anordnung der Name des Betroffenen enthalten sein soll und im Anhang der Anordnungsentscheidung Name, Adresse, Telefonnummern und andere erforderliche Daten bestimmt sein sollen.[69] Jedoch hat der EGMR dabei keinen Beleg über den Eigentümer oder den Benutzer der durch die Maßnahme betroffenen Telekommunikationsgeräte vorausgesetzt.

---

[68] Vgl. Ünver ve Hakeri, *Ceza Muhakemesi*, 718.

[69] EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 160, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}.

c. Die Dauer der Abhörmaßnahme

Nach dem EGMR gehören die Vorschriften über die Dauer der Maßnahme dem Schutz gegen Missbrauch zu.[70]

Nach dem CMK können die Durchführungen der Maßnahmen – Abhören und Aufzeichnen der Telekommunikation sowie die Bewertung der Signale der Telekommunikation – höchstens zwei Monate lang dauern und die Dauer der Maßnahmen kann um höchstens einen Monat verlängert werden. Insofern ist die Durchführung der Maßnahmen durch eine Höchstdauer zeitlich begrenzt. Außerdem kann nach § 135 CMK die Dauer der Maßnahmen zusätzlich jedes Mal um höchstens einen Monat, insgesamt jedoch nur um drei Monate verlängert werden, sofern es eine organisierte Straftat betrifft. (§ 135 Abs. 4 CMK). Diese Bestimmungen tragen den Anforderungen an die Begrenzung der Dauer der Abhörmaßnahme Rechnung. Angesichts der Tatsache jedoch, dass bei der Vorschrift weder für die Maßnahmen des Abhörens und des Aufzeichnens der Telekommunikation noch für die Bewertung der Signale der Telekommunikation eine Voraussetzung für die Verlängerung der Durchführungsdauer bzw. die Lage, unter welcher die Durchführung der Maßnahme verlängert werden darf, festgestellt ist, ist es bedenklich, ob die Bestimmung der Vorschrift einen genügenden Sicherungsmechanismus darstellt, der eine regelmäßige Überprüfung der Aufrechterhaltung der Maßnahme erlaubt, weil dadurch der öffentlichen Gewalt für die Verlängerung der Durchführungsdauer ein unbegrenztes Ermessen eingeräumt wird. Schließlich hat der EGMR im Fall Kennedy, wo die gesetzliche Grundlage der beanstandeten Maßnahme eine Höchstdauer für die Maßnahme vorsieht,

---

[70] EGMR, Urteil vom 04.12.2008 – S und Marper gegen Vereinigtes Königsreich, Rn. 99, https://hudoc.echr.coe.int/eng#{„fulltext":[„s and marper"],"documentcollectionid2":[„GRANDCHAMBER","CHAMBER"],"itemid":[„001-90051"]}; EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 153, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 21.06.2011 – Shimovolos gegen Russland, Rn. 68, https://hudoc.echr.coe.int/eng#{"itemid":["001-105217"]}.

berücksichtigt, dass der Minister stets noch mal überprüfen sollte, ob die Voraussetzungen für die Anordnung der Maßnahme fortbestehen, bevor er die Dauer der Maßnahme verlängert.[71]

Die mangelnde Voraussetzung für die Verlängerung der Durchführung der Maßnahme im CMK führt zu einem Verstoß gegen die Anforderungen des EGMR.

Auf der anderen Seite hat der Gesetzgeber für die Maßnahme „Feststellung der Telekommunikation" bei der Vorschrift keine Höchstdauer oder ein Zeitlimit angewiesen (§ 135 Abs. 6 CMK). Zudem gibt es bei der Vorschrift keine Sicherungsmechanismen, die eine regelmäßige Überprüfung der Aufrechterhaltung der Maßnahme erlauben. Insofern stellt dieser Mangel einen Verstoß gegen die Anforderungen des EGMR dar, weil der Gesetzgeber ein unbegrenztes Ermessen einräumt. Schließlich ist es nach dem EGMR nicht unbedingt erforderlich, dass in der gesetzlichen Grundlage eine konkrete absolute Höchstdauer der Maßnahmen festgeschrieben ist, soweit Sicherungsmechanismen vorliegen, die eine regelmäßige Überprüfung der Aufrechterhaltung der Maßnahme erlauben.[72] Jedoch sieht der Gesetzgeber hier keinen Sicherungsmechanismus vor.

d. Anordnung durch eine unabhängige Stelle und die Kontrolle

Der EGMR hat in seiner Rechtsprechung hervorgehoben, dass die die Maßnahme zulassende Stelle unabhängig sein muss. Darüberhinaus berücksichtigt er, ob über dieser Stelle ein Kontrollmechanismus vorhanden ist, wie eine juristische Kontrolle oder ein unabhängiges kontrollpflichtiges Organ.[73]

---

71 EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 161, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}.

72 EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 161, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 45, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}.

73 Vgl. EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 40, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":

Nach Abs. 1 des § 135 CMK dürfen diese Maßnahmen – Abhören, Aufzeichnen der Telekommunikation und Bewertung der Signalisierung – durch eine richterliche Entscheidung, oder bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet werden. Jedoch setzt die Vorschrift in dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hat, voraus, dass er „sofort" seine Entscheidung für die Genehmigung bei dem Richter einreichen muss. Ohne eine Billigung des Richters werden die Maßnahmen nicht bejaht und die von StA bei Gefahr im Verzug angeordnete Maßnahme muss aufgehoben werden.

Der Begriff „Sofort" weist auf die kürzeste Zeitspanne hin. Bei der Prüfung, ob durch diesen Begriff gegen die Anforderung der Vorhersehbarkeit des EGMR verstoßen wird, ist hervorzuheben, dass schon der EGMR festgestellt hat, dass es für die „Vorhersehbarkeit" einer gesetzlichen Grundlage nicht erforderlich ist, dass nach dem Wortlaut des Gesetzestextes jede Bestimmung mit absoluter Bestimmtheit vorhersehbar ist. Es ist schon ausreichend, wenn genügende Bestimmtheit gegeben wird,[74] soweit ein Schutz gegen willkürliche Eingriffe und Missbrauch gegeben wird.[75]

Allerdings ist hier kritisch zu behandeln, dass die vorgestellte Version dieser Vorschrift den Anforderungen des EGMR mehr Rechnung trug, wonach diese Maßnahmen – nämlich das Abhören und Aufzeichnen der Telekommunikation sowie die Bewertung der Signale einer Telekommunikation - durch eine durch Übereinstimmung ergehende Entscheidung der Strafkammer, die von drei Richtern eingerichtet wird, oder bei Gefahr im Verzug durch die Staats-

[„001-91245"]}; EGMR, Urteil vom 15.01.2015 – Dragojević gegen Kroatien, Rn. 94, http://hudoc.echr.coe.int/eng?i=001-150298#{"itemid":["001-150298"]}; EGMR, Urteil vom 28.04.2005 – Buck gegen Deutschland, Rn. 46, https://hudoc.echr.coe.int/eng#{"itemid":["001-68920"]}.

74 EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 159, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 26.04.1979 – Sunday Times gegen Vereinigtes Königsreich, Rn. 49, EGMR-E, Band 1, 366*ff*.

75 Marauhn und Merhof, „Kapitel7," Rn. 32; Pätzold, „Recht auf Achtung des Privat," Art. 8 EMRK, Rn. 95; vgl. EGMR, Urteil vom 26.03.1987 – Leander gegen Schweden, http://www.eugrz.info/PDF/EGMR3/EGMR03-35.

anwaltschaft angeordnet werden durften. In dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hatte, sollte er „sofort" seine Entscheidung für die Genehmigung bei der Strafkammer einreichen. Die Strafkammer sollte innerhalb von 24 Stunden darüber entscheiden. Die Maßnahmen wurden bejaht, nur wenn diese Entscheidung der StA durch eine Übereinstimmung der Strafkammer gebilligt wurde (Abs. 1 des § 135 CMK, zwischen der Gesetzesänderungen vom 21/02/2014 und 24.11.2016).

Auf der anderen Seite hat der Gesetzgeber die Maßnahme „Feststellung der Telekommunikation" in Abs. 6 des § 135 gesondert angeordnet, wonach im Ermittlungsverfahren ein Richter und bei Gefahr im Verzug die Staatsanwaltschaft und im Hauptverfahren ein Gericht für die Anordnung dieser Maßnahme befugt sind. In dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hat, soll er seine Entscheidung innerhalb von 24 Stunden für die Genehmigung bei dem Richter einreichen. Der Richter soll innerhalb von 24 Stunden darüber entscheiden. Wenn diese eingeräumte Frist von 24 Stunden ohne eine Entscheidung des Richters abläuft, oder wenn der Richter gegenteilig entscheidet, wird die von der StA bei Gefahr im Verzug angeordnete Maßnahme aufgehoben.

Insofern trägt diese Bestimmungen den Anforderungen des EGMR ebenfalls Rechnung.

Jedoch ist von der Vorschrift kein Kontrollmechanismus vorgesehen.

e. Qualifizierter Verdacht

Der EGMR hat im Fall Iordachi beanstandet, dass bei der Ermächtigungsgrundlage keine Bestimmung über den Grad der Tatverdachts und über die Erforderlichkeit einer ernsten Begründung vorgesehen wurde.[76]

[76] EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 51, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}.

Im Fall S und Marper hat der EGMR im konkreten Fall die gesetzliche Grundlage insofern beanstandet, als dass dabei für die Speicherung und Erhaltung der Daten keine Bestimmung über die Relation der Betroffenen mit der Tatbegehung vorgesehen wurde.[77]

Im Fall Kruslin hat der EGMR die gesetzliche Grundlage insofern beanstandet, als dass dabei für die Anordnung der Maßnahme keine Angabe über den Verdacht vorgesehen ist.[78]

Nach Abs. 1 des § 135 CMK darf die Telekommunikation abgehört, aufgezeichnet und die Signale einer Telekommunikation bewertet werden, soweit ein auf konkreten Beweisen beruhender starker Grund für einen Tatverdacht dafür vorliegt, dass eine der unter § 135 Abs. 8 CMK aufgezählten Katalog-Straftaten begangen wurde.

Abgesehen davon, dass der Begriff „auf konkreten Beweise beruhender starker Grund für einen Tatverdacht" nicht verständlich ist, wird durch diese Klausel den Anforderungen des EGMR an den Verdacht Rechnung getragen. Schließlich weist dieser unbestimmte Begriff auf jeden Fall auf einen qualifizierten Verdachtsgrad hin.

In Abs. 6 des § 135 CMK ist über den Verdachtsgrad für die Maßnahme „Feststellung der Telekommunikation" nichts vorgesehen. Nach der Vorschrift kann die Telekommunikation der Angeklagten oder Beschuldigten im Ermittlungsverfahren durch eine richterliche Entscheidung und bei Gefahr im Verzug durch die Staatsanwaltschaft und im Hauptverfahren durch eine gerichtliche Entscheidung angeordnet werden (§ 135 Abs. 6 CMK).

Dass dabei die Begriffe „Angeklagte" und „Beschuldigte" erwähnt werden, weist darauf hin, dass ein „einfacher Verdacht/Anfangsverdacht" für die Anordnung dieser Maßnahme ausreichend ist. Schließlich ist der Verdächtige nach § 2 CMK im Ermittlungsverfahren (im Strafverfahren von Beginn der Ermittlungen

---

77 EGMR, Urteil vom 04.12.2008 – S und Marper gegen Vereinigtes Königsreich, Rn. 119, https://hudoc.echr.coe.int/eng#{„fulltext":[„s and marper"]," documentcollectionid2" :[„GRANDCHAMBER","CHAMBER"],"itemid":[„001-90051"]}.

78 EGMR, Urteil vom 24.04.1990 – Kruslin gegen Frankreich, Rn. 35*ff.*, https://hudoc.echr.coe.int/eng#{„itemid":[„001-57626"]}.

an bis zu der Zulassung der Anklage von dem Gericht) als „Beschuldigter" und in der Gerichtsverhandlung (von der Zulassung der Anklage von dem Gericht bis zum rechtskräftigen Urteil), als „Angeklagter" benannt, und obwohl nach § 170/2 CMK ein hinreichender Tatverdacht für eine Klageerhebung durch die StA vorausgesetzt wird, ist für den Beginn der Ermittlungen, wo also der Verdächtige als „Beschuldigter" benannt wird, ein einfacher Verdacht (Anfangsverdacht) ausreichend.[79] Diese Bestimmung verstößt gegen die Anforderungen des EGMR,[80] weil dadurch die Maßnahme nicht auf ein vernünftiges Maß beschränkt und der öffentlichen Gewalt ein unangemessener Ermessenspielraum eingeräumt wird.

f. Subsidiaritätsklausel

Der EGMR hat in seinen Rechtsprechungen hervorgehoben, dass verdeckte Überwachungsmaßnahmen als letzte Mittel angesehen werden sollen.[81]

Nach Abs. 1 des § 135 CMK darf die Telekommunikation abgehört, aufgezeichnet und die Signale einer Telekommunikation bewertet werden, wenn die Lieferung eines Nachweises auf andere Weise nicht möglich wäre. Diese Bestimmung trägt den Anforderungen des EGMR Rechnung.

In Abs. 6 des § 135 CMK ist für die Maßnahme „Feststellung der Telekommunikation" jedoch keine Subsidiaritätsklausel vorgesehen. Das heißt, dass diese Maßnahmen angeordnet werden dürfen, auch wenn die Lieferung eines Nachweises auf andere Weise möglich

---

79 Vgl. hierzu auch Öztürk et al., *Ceza Muhakemesi*, 329.

80 EGMR, Urteil vom 16.02.2000 – Amann gegen Schweiz, Rn. 76*ff*, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497#{"itemid":["001-58497"]}; EGMR, Urteil vom 04.05.2000 – Rotaru gegen Rumänien, Rn. 57, https://hudoc.echr.coe.int/eng#{"itemid":["001 58586"]}.

81 EGMR, Urteil vom 04.05.2000 – Rotaru gegen Rumänien, Rn. 59, https://hudoc.echr.coe.int/eng#{"itemid":["001 58586"]}; EMGR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 51, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}.

wäre. Dadurch wird die Anordnung der Maßnahmen nicht in vernünftigem Maße beschränkt und gegen die Anforderungen des EGMR verstoßen.

g. Die Darlegung des Verfahrens bei Auswertung, Verwendung und Speicherung der erlangten Daten

Der EGMR setzt ausdrückliche Bestimmungen über die Verfahren bei Auswertung, Verwendung und Speicherung voraus, damit die gesetzliche Grundlage die Mindestanforderungen an Rechtsschutz und Schutz gegen Willkür erfüllt.[82]

Nach der Vorschrift (§ 135 CMK) sind die aufgeführte Prozedur und die durchgeführten Maßnahmen – nämlich das Abhören, Aufzeichnen oder Feststellen der Kommunikation und die Bewertung der Signale der Telekommunikation – während der Durchführung der Maßnahme verdeckt (§ 135 Abs. 7 CMK). Das ist das einzige Gemeingut zwischen allen Maßnahmen im Rahmen der Verfahrensvorschriften.

Die anderen Verfahrensregelungen liegen in § 137 CMK. Die Formulierung der Vorschrift ist so verwirrend, dass die Bestimmungen zu den Verfahrensregelungen sich zwischen den Maßnahmen zum Teil überschneiden und zum Teil nicht.

Insofern soll jede Maßnahme im Hinblick auf die Verfahrensregelungen gesondert geprüft werden.

Das Abhören der Telekommunikation: Für die Durchführung der Maßnahme „Abhören der Telekomunikation" ist ein schriftliches

---

82 EMGR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 48, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}; EGMR, Urteil vom 16.02.2000 – Amann gegen Schweiz, Rn. 76ff., http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497#{"itemid":["001-58497"]}; EGMR, Urteil vom 04.12.2008 – S und Marper gegen Vereinigtes Königsreich, Rn. 99, https://hudoc.echr.coe.int/eng#{„fulltext":[„s and marper"],"documentcollectionid2":[„GRANDCHAMBER","CHAMBER"],"itemid":[„001-90051"]}.

Dokument von der StA oder von durch diese befugten Angestellten erforderlich (§ 137 Abs. 1 CMK). Außerdem wird im Rahmen der Durchführung ein Protokoll über das Datum und die Uhrzeit des Beginns und des Endes der Durchführung der Maßnahmen sowie die Identität der die Maßnahme durchführenden Personen erstellt (§ 137 Abs. 1).

Aufzeichnen der Telekommunikation: Die Bestimmungen über die Voraussetzungen „schriftliches Dokument" von der StA oder von durch diese befugten Angestellten und eine Protokollführung bezüglich der Daten, die das Datum und die Uhrzeit des Beginns und des Endes der Durchführung der Maßnahmen sowie die Identität der die Maßnahme durchführenden Personen enthalten, sind auch für diese Maßnahmen gültig (§ 137 Abs. 1).

Außerdem: Nach Abs. 2 des § 137 CMK werden die in den im Rahmen des § 135 angeordneten Maßnahmen erlangten *Aufzeichnungen* durch von der StA beauftragte Personen verarbeitet und in einen Text umgewandelt (§ 137 Abs. 2). Naturgemäß fällt die Maßnahme „Aufzeichnung der Telekommunikation" unter diese Vorschrift.

Jedoch wurden bei dem Gesetz keine Vorschriften über das Speicherungsverfahren der in einen Text umgewandelten Daten oder die Verwendung z. B. für andere Zwecke vorgesehen. Insofern erfüllen diese Bestimmungen die Anforderungen des EGMR nicht.

Feststellung der Telekommunikation: Die Bestimmungen über die Voraussetzung „schriftliches Dokument" von der StA oder von ihm befugten Angestellten und eine Protokollführung bezüglich der Daten, die das Datum und die Uhrzeit des Beginns und des Endes der Durchführung der Maßnahmen sowie die Identität der die Maßnahme durchführenden Person enthält, sind auch für diese Maßnahmen gültig (§ 137 Abs. 1).

Außerdem ist zu überprüfen, ob die Bestimmung von § 137 Abs. 2 CMK, wonach die durch *die im Rahmen des § 135 angeordneten Maßnahmen* erlangten *Aufzeichnungen* durch von der StA beauftragte Personen verarbeitet und in einen Text umwandelt werden, auch für diese Maßnahme gültig ist.

Die Maßnahme „Feststellung der Telekomunikation" wird nach § 135 CMK angeordnet und ist insofern mit dieser Bestimmung einschlägig.

Zweitens ist zu prüfen, ob durch die Bestimmung „Aufzeichnung" auch die durch die Maßnahme „Feststellung der Telekommunikation" erlangten Aufzeichnungen gemeint wird.

Erdem erwähnt nur die Inhaltsaufzeichnungen von einer Telekommunikation, als er diese Bestimmung prüft.[83]

Nach dem Wortlaut des Gesetzestextes ist nach der „Verarbeitung der Aufzeichnungen" die „Umwandlung in einen Text" vorgesehen. Meiner Meinung nach, soweit die durch die Maßnahme „Feststellung der Telekomunikation" erlangten Aufzeichnungen am Anfang aus kodierten Zeichen bestehen, erfordern sie eine Verarbeitung und Umwandlung. Insofern ist festzustellen, dass § 137 Abs. 2 CMK eine Verfahrensregelung über die Auswertung der erlangten Daten im Hinblick auf diese Maßnahme darstellt. Außerdem wurde in dem Gesetz nicht bestimmt, wie man die Aufzeichnungen der Maßnahme „Feststellen der Telekomunikation" verwenden und speichern soll. Dies stellt einen weiten Ermessenspielraum dar und verstößt gegen die Anforderungen des EGMR.

Bewertung der Signale der Telekommunikation: Die Bestimmungen über die Voraussetzung „schriftliches Dokument von der StA oder von durch diese befugten Angestellten und eine Protokollführung bezüglich der Daten, die das Datum und die Uhrzeit des Beginns und des Endes der Durchführung der Maßnahmen sowie die Identität der die Maßnahme durchführenden Person feststellt" sind für diese Maßnahmen nicht gültig (§ 137 Abs. 1).

Außerdem ist zu überprüfen, ob die Bestimmung von § 137 Abs. 2 CMK, wonach die durch die im Rahmen des § 135 angeordneten Maßnahmen erlangten *Aufzeichnungen* von durch die StA beauftragte Personen verarbeitet und in einen Text umwandelt werden, auch für diese Maßnahme gültig ist.

---

83 Öztürk et al., *Ceza Muhakemesi*, 487*ff*.

Die Maßnahme „*Bewertung der Signale der Telekommunikation*" wird nach § 135 CMK angeordnet und ist insofern mit dieser Bestimmung einschlägig.

Zweitens ist zu prüfen, ob durch die Bestimmung „Aufzeichnung" auch die durch die Maßnahme „*Bewertung der Signale der Telekommunikation*" erlangten Aufzeichnungen gemeint sind.

Dem Wortlaut des Gesetzestextes nach ist nach der „Verarbeitung der Aufzeichnungen" die „Umwandlung in einen Text" vorgesehen. Insofern ist festzustellen, dass § 137 Abs. 2 CMK eine Verfahrensregelung über die Auswertung der erlangten Daten im Hinblick auf diese Maßnahme darstellt, soweit die durch die Maßnahme „*Bewertung der Signale der Telekommunikation*" erlangten Aufzeichnungen am Anfang aus kodierten Zeichen bestehen, die eine Verarbeitung und Umwandlung erfordern. Jedoch ist durch das Gesetz nicht bestimmt, wie man die Aufzeichnungen der Maßnahme „*Bewertung der Signale der Telekommunikation*" verwenden und speichern soll. Insofern stellt das Gesetz für diese Maßnahme keinen genügenden Missbrauchsschutz dar und eröffnet einen weiten Ermessenspielraum. Darin verstößt es gegen die Anforderungen des EGMR.

Folgerung: Wie ganz klar gesehen wurde, sind die Darlegungen der Verfahren bei Auswertung, Verwendung und Speicherung der erlangten Daten für die Maßnahme „Überwachung der Telekommunikation" im CMK ganz ungenügend. Insofern gewährleistet dieses Gesetz keinen genügenden Missbrauchsschutz und erfüllt die Anforderungen des EGMR nicht.

h. Löschungspflicht

Laut EGMR sollen in der gesetzlichen Grundlage die Umstände, unter denen die Aufzeichnungen gelöscht und die Bänder vernichtet werden müssen oder dürfen, ausdrücklich bestimmt sein.[84]

---

[84] EGMR, Urteil vom 04.12.2008 – S und Marper gegen Vereinigtes Königsreich, Rn. 99, https://hudoc.echr.coe.int/eng#{„fulltext":[„s and marper"],"documentcollectionid2" :[„GRANDCHAMBER","CHAMBER"],"itemid":[„001-90051"]};

Nach Abs. 6 des § 135 CMK wird die Maßnahme „Feststellung der Telekommunikation" im Ermittlungsverfahren von einem Richter und bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet. In dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hat, soll er seine Entscheidung innerhalb von 24 Stunden für die Genehmigung bei dem Richter einreichen. Der Richter soll innerhalb von 24 Stunden darüber entscheiden. Wenn „die Zeit" abläuft oder wenn der Richter gegenteilig entscheidet, muss die Aufzeichnungen über die Feststellung der Telekommunikation *„sofort"* vernichtet werden.

Diese Bestimmung, dass die Aufzeichnungen über die Feststellung der Telekommunikation in dem Fall, wo der Staatsanwalt die Genehmigung des Richters nicht einholen konnte, vernichtet werden muss, wird zudem in §137 Abs. 3 folgendermaßen hervorgehoben.

Nach § 137 Abs. 3 CMK muss die Durchführung der Maßnahme, die nach § 135 angeordnet wird, von der StA sofort aufgehoben werden, wenn die StA die Ermittlung während der Durchführung der Maßnahme einstellt oder die StA die Genehmigung des Richters für ihre bei Gefahr im Verzug selbst angeordnete Maßnahme nicht einholen konnte. Insofern werden die *Aufzeichnungen* über die *Feststellung oder über das Abhören der Telekommunikation* unter der Kontrolle der Staatsanwaltschaft innerhalb von zehn Tagen vernichtet und der Fall der Vernichtung protokolliert.

Aus dem Gesetzestext ergibt sich, dass der Aufhebungszwang der StA für alle Maßnahmen, die in § 135 CMK erwähnt werden, gültig ist, nämlich für die Maßnahmen des Abhörens, Aufzeichnens und Feststellens der Kommunikation und der Beurteilung der Signale der Telekommunikation.

EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 162ff., https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}; EGMR, Urteil vom 24.04.1990 – Huvig gegen Frankreich, Rn. 34, https://hudoc.echr.coe.int/eng#{"fulltext":["\"CASE OF HUVIG v. FRANCE\""],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57627"]}.

Zudem ist hier zu bestimmen, dass das Gesetz die Löschungspflicht an die Aufhebung der Durchführung der Maßnahme knüpft. Jedoch ist die Lage, unter welcher die Durchführung der Maßnahme aufgehoben werden muss, mangelhaft bestimmt. Das heißt: Auch die löschungspflichtigen Fälle sind mangelhaft bestimmt, weil sie auf die Fälle, bei denen die Durchführung der Maßnahme aufgehoben werden muss, beschränkt sind.

Nach der Gesetzesbestimmung ist die StA bei der Durchführung der Maßnahme aufhebungspflichtig, wenn sie die Ermittlung während der Durchführung der Maßnahme einstellt oder die Genehmigung des Richters für ihre bei Gefahr im Verzug selbst angeordnete Maßnahme nicht einholen konnte.

Diese Bestimmung ist erstens schon mangelhaft, weil dabei zweifelhaft ist, ob „das Ende der Dauer" als ein aufhebungspflichtiger Fall im Rahmen dieser Vorschriften vorgesehen wird:

Schließlich heißt es nach dem Gesetzestext der Vorschrift § 135 Abs. 1: „Diese Maßnahmen dürfen durch eine Entscheidung des Richters oder bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet werden. Jedoch setzt die Vorschrift bei diesem Fall, in dem die Staatsanwaltschaft diese Entscheidung getroffen hat, voraus, dass diese „sofort" seine Entscheidung für die Genehmigung bei dem Richter einreichen. Der Richter soll innerhalb von 24 Stunden darüber entscheiden. Wenn *„die Zeit"* abläuft, oder wenn der Richter gegenseitig entscheidet, werden die von der StA bei Gefahr im Verzug angeordneten Maßnahmen aufgehoben."

Nach *Erdem* weist hier die Bestimmung von „Zeit" darauf hin, dass die Maßnahme nach dem Ende der Durchführungsdauer der Maßnahme aufgehoben werden muss.[85]

Diese Auffassung wird hier nicht vertreten. Meiner Meinung nach weist der Begriff „Zeit" auf den Fall hin, dass die Maßnahme bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet wurde und eine Genehmigungsentscheidung des Richters erwartet

85 Öztürk et al., *Ceza Muhakemesi*, 553.

wird. Also bedeutet die Bestimmung des Gesetzes, „wenn *‚die Zeit'* abläuft", den Ablauf der eingeräumten 24 Stunden, ohne dass eine Entscheidung des Richters ergangen ist.

Daraus ergibt sich, dass nach der Vorschrift „das Ende der Durchführungsdauer der Maßnahme" keinen aufhebungspflichtigen Fall darstellt.[86]

Zudem sind die Fälle, in denen die Durchführung der Maßnahme von der StA sofort aufgehoben werden müssen, folgendermaßen mangelhaft bestimmt: Die Maßnahme sollte auch in dem Fall aufgehoben werden, wenn sich die bei der Anordnung der Maßnahme maßgebenden Konditionen verändert haben. Z. B. sollte der Gesetzgeber auch feststellen, dass die Maßnahme aufgehoben werden sollten, wenn die Lieferung eines Nachweises nach dem Beginn der Durchführung der Maßnahme auf andere Weise möglich wäre oder wenn nach dem Beginn der Durchführung der Maßnahme festgestellt würde, dass durch diese Maßnahme nicht zum Abschluss der Ermittlungen gelangt werden kann. Auch, wenn gegen den Betroffenen eine Klage erhoben wird, oder wenn nach dem Beginn der Durchführung der Maßnahme festgestellt wird, dass die einschlägige Straftat nicht unter die Katalogfälle subsumiert werden kann, sollte die Durchführung der Maßnahme aufgehoben werden.[87] Dass bei diesen Fällen im konkreten Fall die Maßnahme trotzdem weitergefahren werden darf, verursacht eine willkürliche Durchführung der Maßnahme, was gegen die Anforderungen des EGMR verstößt.

Der Gesetzgeber sollte die aufhebungspflichtigen Fälle sorgfältig bestimmen und die löschungspflichtigen Fälle nicht an die aufhebungspflichtigen knüpfen, weil nicht bei jedem aufhebungspflichtigen Fall die Löschung erforderlich ist, wie es z. B. der Fall bei dem „Ende der Durchführungsdauer der Maßnahme" ist. Stattdessen sollte er die Löschung der Daten an die „Erforderlichkeitsklausel" knüpfen.[88]

---

86 Vgl. hier auch Özbek et al., *Ceza Muhakemesi*, 466.

87 Öztürk et al., *Ceza Muhakemesi*, 553; Faruk Turhan, *Ceza Muhakemesi Hukuku* (Ankara: Asil Yayın Dağıtım, 2006), 272.

88 Vgl. Öztürk et al., *Ceza Muhakemesi*, 490*ff*.

Insofern sollte der Gesetzgeber z. B. die Löschung der Aufzeichnungen anweisen, wenn der Betroffene freigesprochen wird.[89]

Außerdem sollte er vorsehen, dass die Daten zu löschen sind, die dem verfolgten Zweck nicht dienlich sind, schließlich hat der EGMR im Fall Kennedy ausdrücklich darauf hingewiesen.[90]

Außerdem sind bei der Vorschrift nur für *die Aufzeichnungen über die Feststellung oder über das Abhören der Telekommunikation* Löschungsplichten vorgesehen. Dabei wurde keine Angabe über die der Bewertung der Signale der Telekommunikation dienenden Aufzeichnungen vorgesehen. Insofern gewährleistet die gesetzliche Grundlage keinen genügenden Schutz gegen Missbrauch dieser Aufzeichnungen.

Dass das § 138 TCK eine zwei- bis vierjährige Freiheitsstrafe für Ermittlungspersonen vorsieht, welche die im Rahmen einer Telekommunikationsüberwachung erlangten personenbezogenen Daten nicht löschen, ist jedoch positiv zu erwähnen.

i. Benachrichtigung

Laut EGMR wird eine Benachrichtigungspflicht nicht als unerlässlich angesehen, soweit es Kontrollmechanismen gibt.[91]

Im CMK ist die Benachrichtigungspflicht nicht ausdrücklich unter einer gesonderten Rubrik sichergestellt. Zudem ist der Umfang der Benachrichtigungspflicht sehr begrenzt.

Nach § 137 Abs. 4 CMK ist eine Benachrichtigungspflicht nur für die Fälle, in denen die StA die Ermittlung während der Durchführung der Maßnahme einstellt oder die StA die Genehmigung des Richters für ihre bei Gefahr im Verzug selbst angeordnete Maßnah-

---

89 Öztürk et al., *Ceza Muhakemesi*, 490.

90 EGMR, Urteil vom 18.05.2010 – Kennedy gegen Vereinigtes Königsreich, Rn. 162, https://hudoc.echr.coe.int/eng#{"itemid":["001 98473"]}.

91 EGMR, Urteil vom 06.09.1978 – Klass u.a. gegen Deutschland, Rn. 36*ff*., http://www.eugrz.info/pdf/EGMR31.pdf.

me nicht einholen konnte, vorgesehen. Danach wird der *„Betroffene"* von der Einstellung des Ermittlungsverfahrens an– und auf jeden Fall aber nach der Vernichtung der Aufzeichnungen über die Feststellung oder das Abhören der Telekommunikation – innerhalb von 15 Tagen schriftlich über den Umfang, den Grund, die Dauer und das Ergebnis der Maßnahme von der Staatsanwaltschaft in Kenntnis gesetzt (§ 137 Abs. 3 i. V. m. § 137 Abs. 4 CMK) .

Diese Bestimmung ist mangelhaft, weil dabei für die anderen Fälle, wo die Maßnahme wegen anderer Ursachen aufgehoben werden sollte, wie z. B. deswegen, weil die Lieferung eines Nachweises nach dem Beginn der Durchführung der Maßnahme auf andere Weise möglich wäre oder weil nach dem Beginn der Durchführung der Maßnahme festgestellt wird, dass die vorgeworfene Straftat nicht den Katalogfällen unterstellt ist, keine Benachrichtigungspflicht vorgesehen wurde.

Zudem ist die Benachrichtigungspflicht nur für die Maßnahme *„Aufzeichnungen über die Feststellung oder das Abhören der Telekommunikation"* gültig, nicht für andere Maßnahmen und auf jeden Fall erst nach der Vernichtung der Aufzeichnungen.

Außerdem wird der Betroffene nach der Vernichtung benachrichtigt, wodurch seine Möglichkeit auf Rechtsschutz beeinträchtigt wird, weil er sich nach der Vernichtung im Rechtsschutzprozess nicht auf die Inhalte der Aufzeichnungen berufen kann.

Zudem wurden bei dieser Vorschrift keine Kontrollmechanismen wie z. B. ein Gremium vorgesehen. Insofern erfüllt diese Bestimmung die Anforderungen des EGMR nicht. Der Gesetzgeber sollte die aufhebungspflichtigen Fälle der Maßnahme sorgfältiger bestimmen und danach die Benachrichtigungspflicht an die Aufhebung der Maßnahme knüpfen oder einen Kontrollmechanismus vorsehen.

j. Begrenzte Befugnis der Richter

Im CMK ist keine Pflicht vorgesehen, während der Durchführung der Maßnahme den Richter, von dem die Maßnahme angeordnet wurde, über den weiteren Verlauf der Maßnahme zu informieren.

Auch sind der Richter nicht befugt, im Stadium der Durchführung die Aufzeichnungen über die Maßnahme zu prüfen. Dies entspricht nicht den Anforderungen des EGMR, schließlich hat es der EGMR im Fall Iordachi beanstandet, dass dem Richter nach den gesetzlichen Bestimmungen sehr begrenzte Befugnisse über die Beurteilung der Abfolgen der Maßnahme oder über die erneute Beurteilung zur Maßnahmenserforderlichkeit eingeräumt wurden.[92]

k. Regelung zu den Zeugnisverweigerungsberechtigten/ Verteidiger

Nach § 135 Abs. 3 CMK kann die Telekommunikation zwischen den Zeugnisverweigerungsberechtigten und Beschuldigten oder Angeklagten nicht aufgezeichnet werden. Wenn dies nach der Aufzeichnung bemerkt wird, werden die Aufzeichnungen sofort vernichtet. Dass die Vorschrift nur im Hinblick auf die Maßnahme „Telekommunikationaufzeichnung" einen Schutz vorgesehen hat, andere Maßnahmen aber wie das Abhören von Telekommunikation, die Feststellung der Telekommunikation oder die Beurteilung der Signale der Telekommunikation hier nicht erwähnt und für diese Maßnahmen auch kein Schutz im Hinblick auf Zeugnisverweigerungsberechtigte vorgesehen wurden,[93] stellt ein Defizit im Hinblick auf den Missbrauchschutz dar. Insofern erfüllt die gesetzliche Grundlage die Anforderungen des EGMR nicht. Schließlich hat der EGMR im Fall Petri Sallinen den mangelnden Schutz des Vertrauensverhältnisses zwischen Mandaten und Rechtsanwälten beanstandet.[94]

Jedoch ist dieses Defizit im Rahmen der Verteidigergespräche nicht vorhanden, weil durch § 136 Abs. 1 CMK der öffentlichen Gewalt entzogen wurde, an den Telekommunikationgeräten, die sich

---

92 EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 47, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{"itemid":["001-91245"]}.

93 Öztürk et al., *Ceza Muhakemesi*, 483.

94 EGMR, Urteil vom 27.09.2005 – Petri Sallinen u.a. gegen Finnland, Rn. 87, https://hudoc.echr.coe.int/eng#{„itemid":[„001-70283"]}.

in der Wohnung, dem Büro oder der Niederlassung des Verteidigers befinden, die in § 135 CMK aufgezählten Maßnahmen durchzuführen. Das Handy von einem Verteidiger wurde hier nicht aufgezählt, jedoch gilt dieser Schutz auch hier, weil das Handy sich auf jeden Fall in der Niederlassung des Verteidigers befindet. An dieser Stelle ist auch hervorzuheben, dass es nicht immer möglich wäre, zwischen einem Rechtsanwalt und einem Verteidiger eine zeitliche Grenze zu ziehen.

l. Regelung über die Übermittlung an andere Behörden

Der EGMR berücksichtigt bei seinen Rechtssprechungen, ob die bei der Übermittlung der Daten an andere Behörden zu beachtenden Vorsichtsmaßnahmen vorhanden sind.[95]

Im Rahmen des CMK gibt es keine Vorschrift über die Übermittlung der durch diese Maßnahmen erlangten Daten an andere Behörden.

m. Der Schutz dritter Personen

Bei dieser Vorschrift ist bestimmt, inwiefern die Verwendung der Daten von Dritten, die durch die Durchführung dieser Maßnahmen erlangt wurden, möglich ist (§ 138 CMK Abs. 2).

Nach § 137 Abs. 4 wird der „*Betroffene"* zudem von der Einstellung des Ermittlungsverfahrens an – und auf jeden Fall aber nach der Vernichtung der *Aufzeichnungen über die Feststellung oder dem Abhören der Telekommunikation* – innerhalb von 15 Tagen schriftlich über den Umfang, den Grund, die Dauer und das Ergebnis der Maßnahme von der Staatsanwaltschaft in Kenntnis gesetzt (§ 137

[95] EGMR, Urteil vom 24.04.1990 – Huvig gegen Frankreich, Rn. 34, https://hudoc.echr.coe.int/eng#{"fulltext":["\"CASE OF HUVIG v. FRANCE\""],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57627"]}; EGMR, Urteil vom 26.03.1987 – Leander gegen Schweden, Rn. 54*ff*., http://www.eugrz.info/PDF/EGMR3/EGMR03-35.

Abs. 3 i. V. m. § 137 Abs. 4 CMK) . Dass bedeutet nicht nur, dass für Beschuldigte oder Angeklagte, sondern auch für einschlägige dritte Personen eine Benachrichtigungspflicht vorgesehen ist.[96]

Jedoch ist, wie bereits erwähnt, eine Benachrichtigungspflicht nur für die Fälle, in denen die StA die Ermittlung während der Durchführung der Maßnahme einstellt oder die StA die Genehmigung des Richters für ihre bei Gefahr im Verzug selbst angeordnete Maßnahme nicht einholen konnte, vorgesehen (§ 137 Abs. 4 CMK).[97] Diese Bestimmung ist mangelhaft, weil dabei für die anderen Fälle, in denen die Maßnahme wegen anderer Ursachen aufgehoben werden sollte, wie z. B. deswegen, weil die Lieferung eines Nachweises nach dem Beginn der Durchführung der Maßnahme auf andere Weise möglich wäre oder weil nach dem Beginn der Durchführung der Maßnahme festgestellt wird, dass die vorgeworfene Straftat nicht zu den Katalogstraftaten zählt, keine Benachrichtigungspflicht vorgesehen wurde.[98]

Außerdem wurde dabei keine Regelung über den Schutz dritter Personen bzw. keine Anfechtungsmöglichkeit für Dritte vorgesehen, die von der Durchführung der Telekommunikationsüberwachung von Anderen beeinträchtigt werden. Dies entspricht jedoch nicht den Anforderungen des EGMR, schließlich hat der EGMR im Fall Lambert die gesetzliche Grundlage insofern beanstandet, als dass sie keinen Schutz bzw. keine Anfechtungsmöglichkeit für Dritte vorsieht, die von der Durchführung der Telekommunikationsüberwachung von Anderen beeinträchtigt werden.

n. Vorbeugende Regelung gegen erneute Durchführung

Im Fall Iordachi wurde vom EGMR beanstandet, dass die Ermächtigungsgrundlage für die Telekommunikationsüberwachungsmaßnahme keine vorbeugende Regelung vorgesehen hat, die

---

96 Öztürk et al., *Ceza Muhakemesi*, 491.

97 Öztürk et al., *Ceza Muhakemesi*, 491.

98 Vgl. Öztürk et al., *Ceza Muhakemesi*, 489.

das Vorhaben des Staatsanwalts zu Fall bringt, nach der Beendigung der Durchführung der Maßnahme eine erneute Maßnahme anzuordnen,[99] die also nach dem Ablauf der ersten Durchführung eine erneute Anordnung der Maßnahme versagt.

Die Vorschrift enthält hierzu keine Bestimmung. Insofern erfüllt diese Vorschrift die Anforderung des EGMR nicht.

IV. FAZIT

Der EGMR hat in vielen Rechtsprechungen zu geheimen Überwachungsmaßnahmen zur Vermeidung von Machtmissbrauch neben die Bestimmungen zur „Art der Straftaten, die eine Überwachungsanordnung rechtfertigen können", zu den „Personengruppen, bei denen die Maßnahme Anwendung findet" und zur „Begrenzung der Dauer der Maßnahme" auch Bestimmungen über „die Umstände, unter denen die Aufzeichnungen gelöscht und die Bänder vernichtet werden müssen oder dürfen", in den gesetzlichen Regelungen als Mindestgarantien entwickelt.[100] Der türkische Gesetzgeber soll sorgfältiger sein, indem er diesen Anforderungen des EGMR Rechnung trägt. Schließlich sind die Vorschriften der Telekommunikationsüberwachungsmaßnahme in CMK trotz der Gesetzesänderungen vom 21.02.2014, 02.12.2014 und 24.11.2016 in Hinblick auf die Anforderungen des EGMR an den Schutz gegen Mißbrauch und Willkür immer noch mangelhaft.

Insofern ist die Gesetzesänderung vom 24.11.2016, die die durch das Gesetz Nr. 6526 vom 21.02.2014 gestellten strengeren Voraussetzungen für die Anordnung der Telekommunikationsmaßnahmen wieder erleichtert hat, hier auch kritisch zu behandeln.

---

[99] EGMR, Urteil vom 10.02.2009 – Iordachi u.a. gegen Moldawien, Rn. 45, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245#{„itemid":[„001-91245"]}.

[100] Vgl. EGMR, Urteil vom 29.06.2006 – Weber und Saravia gegen Deutschland, Rn. 95, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-76586#{"itemid":["001-76586"]}.

Nach dem jüngsten Telekommunikationsüberwachungsskandal in der Türkei, der gezeigt hat, dass insbesondere in diesen äußerst grundrechtsgeschützten Bereichen viele Missbräuche durch Polizei, Staatsanwaltschaft oder sogar Richter vorkommen können, wurde § 135 CMK durch das Gesetz Nr. 6526 vom 21.02.2014[101] geändert und wurden dadurch die Voraussetzungen für die Anordnung einer Telekommunikationsüberwachungsmaßnahme strenger gemacht: Nach dieser Änderung wurde eine in der alten Fassung vorhandene Straftat, nämlich „eine Vereinigung oder Bande zu bilden, um Straftaten zu begehen", entfernt, mit der Begründung, dass das Tatbestandsmerkmal ansonsten als Auffangtatbestand fungieren würde und somit für alle Straftaten, welche nicht ausdrücklich unter § 135 CMK aufgezählt werden, die Anordnung einer Telekommunikationsmaßnahme erleichtern würde,[102] und zweitens wurde für die Anordnung der Telekommunikationsüberwachungsmaßnahmen – nämlich das Abhören und Aufzeichnen der Telekommunikation sowie die Bewertung der Signale einer Telekommunikation – eine durch Übereinstimmung ergehende Entscheidung der Strafkammer, die von drei Richtern eingerichtet wird, als erforderlich angesehen; sowie bei Gefahr im Verzug in dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hatte, wurden die Maßnahmen bejaht, nur wenn diese Entscheidung der StA durch eine Übereinstimmung der Strafkammer gebilligt wurde. Diese Änderungen wurden aber mit der Änderung durch das Gesetz Nr. 6763 vom 24.11.2016 wieder rückgängig gemacht und die Straftat „eine Vereinigung oder Bande zu bilden, um Straftaten zu begehen" wieder in den Strafkatalog aufgenommen und für die Anordnung der Telekommunikationsüberwachungsmaßnahmen wieder eine richterliche Entscheidung, bzw. bei Gefahr im Verzug in dem Fall, wo der Staatsanwalt diese Entscheidung getroffen hatte, eine Billigung durch eine richterliche Entscheidung, als ausreichend angesehen. Insofern ist kritisch zu behandeln, dass die strengeren Voraussetzungen für die Anordnung der Telekommunikationsmaßnahmen wieder erleichtert wurden.

---

[101] Vgl. hierzu § 12 des Gesetzes Nr. 6526, http://www.resmigazete.gov.tr/eskiler/2014/03/20140306M1-1.htm.

[102] vgl. hierzu Şahin, *Ceza Muhakemesi*, 269.

DIE BIBLIOGRAPHIE

Aydın, Çetin, Fevzi Kızılkoyun ve Banu Şen. „Sadece Iki Ilde 1700 Polisin Yeri Değişti." Hürriyet.com. Veröffentlichung: Januar 07, 2014. http://www.hurriyet.com.tr/gundem/25515006.asp.

Bär, MMR 2000, 472 (473ff.).

Bayraktar, Çiler Damla. *Eingriffe in die Privatsphäre durch technische Überwachung Ein deutsch-türkischer Vergleich anhand Art. 8 EMRK*. Hamburg: Dr. Kovac, 2017.

Breitenmoser, Stephan. *Der Schutz der Privatsphäre gemäß Art. 8 EMRK das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs*. Frankfurt am Main: Helbing u. Lichtenhahn, 1986.

Centel, Nur ve Hamide Zafer. *Ceza Muhakemesi Hukuku*, İstanbul: Beta Yayınevi, 2013.

Centel, Nur ve Hamide Zafer. *Ceza Muhakemesi Hukuku*. İstanbul: Beta Yayınevi, 2015.

Ennulat, Mark. *Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und –einrichtungen*. Bern: Peter Lang, 2008.

Esser Robert. „EMRK/IPBPR." in *Löwe-Rosenberg StPO*. Vol. 11. Berlin: De Gruyder, 2012.

Fischer, Florian. *Rheinischer Kommentar zur Europäischen Menschenrechtskonvention Privat- und Familienleben.* Berlin: Logos, 2015.

Frowein, Jochen Abr. „Art. 8 EMRK" in *Europäische Menschenrechtskonvention EMRK- Kommentar*, hrsg. Jochen Abr. Frowein und Wolfgang Peukert. Baden: Engel N.P., 2009.

Gollwitzer, Walter. *Menschenrechte im Strafverfahren MRK und IPBPR Kommentar*. Berlin: De Gruyder, 2005.

Grabenwarter, Christoph und Katharina Pabel. *Europäische Menschenrechtskonvention*. Vol. 3. München: C.H. Beck, 2016.

Haber7. „Selam-tevhid davasında 251 kişiye takipsizlik." Veröffentlichung: Juli 22, 2014. http://www.haber7.com/hukuk/haber/1183375-selam-tevhid-davasinda-251-kisiye-takipsizlik.

Iliopoulos-Strangas, Julia. „Die allgemeinen Rechtsgrundsätze in der Praxis der Straßburger Organe am Beispiel des Verhältnismäßigkeitsprinzips." *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, nu. 63 (1999): 414-451.

Kaymaz, Seydi. *Ceza Muhakemesinde Telekomunikasyon Yoluyla Yapılan İletişimin Denetlenmesi*. Ankara: Seçkin Yayıncılık, 2015.

Klein, Eckart. „§ 150: Der Schutz der Grund- und Menschenrechte durch den Europäischen Gerichtshof für Menschenrechte." in *Handbuch der Grundrechte in Deutschland und Europa Europäische Grundrechte*. vol. 6/1, hrsg. Detlef Merten und Hans-Jürgen Papier, 593-662. Heidelberg: C. F. Müller, 2010.

Kühling, Jürgen. „Grundrechte." In *Europäisches Verfassungsrecht*, hrsg. Armin von Bogdandy und Jürgen Bast, 657-704. Heidelberg: Springer, 2009.

Kunter, Nurullah, Feridun Yenisey ve Ayşe Nuhoğlu. *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*. İstanbul: Beta Yayınevi, 2010.

Marauhn, Thilo und Judith Thorn. „Kapitel 16: Privat- und Familienleben." in *EMRK/GG Konkordanzkommentar,* hrsg. Oliver Dörr, Rainer Grote und Thilo Marauhn, Rn. 1-106. Tübingen: Mohr Siebeck, 2013.

Marauhn, Thilo und Katrin Merhof. „Kapitel 7: Grundrechtseingriff und -schranken." in *EMRK/GG Konkordanzkommentar, hrsg.* Oliver Dörr, Rainer Grote und Thilo Marauhn, Rn. 1-68. Tübingen: Mohr Siebeck, 2013.

Meyer-Ladewig, Jens. *EMRK Europäische Menschenrechtskonvention Hand Kommentar*. Basel: Helbing Lichtenhahn, 2011.

Nußberger, Angelika. „Das Verhältnismäßigkeitsprinzip als Strukturprinzip richterlichen Entscheidens in Europa." *NVwZ-Beilage* 1, (2013): 36-44.

Özbek, Veli Özer, Mehmet Nihat Kanbur, Pınar Bacaksız, Koray Doğan ve İlker Tepe. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, 2015.

Özbek, Veli Özer. *CMK Izmir Şerhi Yeni Ceza Muhakemesinin Anlamı*. Ankara: Seçkin Yayıncılık, 2005.

Öztürk, Bahri, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin F. Saygılar Kırıt, Özdem Özaydın, Esra Alan Akcan ve Efser Erden Tütüncü. *Nazari ve Uygulamali Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, 2015.

Pätzold, Juliane. „Recht auf Achtung des Privat- und Familienleben." in *EMRK Konvention zum Schutz der Menschenrechte und Grundfreiheiten*, hrsg. Ulrich Karpenstein und Franz C. Mayer, 252-284. München: C. H. Beck, 2015.

Peters, Anne und Tilmann Altwicker. *Europäische Menschenrechtskonvention*, München: C. H. Beck, 2012.

Peters, Anne. *Einführung in die Europäische Menschenrechtskonvention*. München: C. H. Beck, 2003.

Şahin, Cumhur. *Ceza Muhakemesi Hukuku 1*, Ankara: Seçkin Yayıncılık, 2015.

Şen. „die Maßnahme im türkischen Recht, die Kommunikation zu beaufsichtigen" in d*as Strafrecht im Deutsch–Türkischen Rechtsvergleich*, hrsg. Eric Hilgendorf und Yener Ünver. İstanbul: Yeditepe Üniversitesi Hukuk Fakültesi, 2010.

Toroslu, Nevzat ve Metin Feyzioğlu. *Ceza Muhakemesi Hukuku*. Ankara: Şavaş Yayınevi, 2013.

Turhan, Faruk. *Ceza Muhakemesi Hukuku*. Ankara: Asil Yayın Dağıtım, 2006.

Türkiye Gazette. „MİT Müsteşarı Fidan'ı "Emin" kod adıyla dinlediler." Veröffentlichung: Juli 23, 2014. http://www.turkiyegazetesi.com.tr/gundem/173435.aspx.

Tursun, Cem, Serpil Kırkeser ve Arzu Kaya. „Üç bakan oğluna tutuklama talebi." Hürriyet. Veröffentlichung: Dezember 20, 2013. http://www.hurriyet.com.tr/uc-bakan-ogluna-tutuklama-talebi-25409906.

Uerpmann-Wittzack, Robert. „Höchstpersönliche Rechte und Diskriminierungsverbot." In *Europäische Grundrechte und Grundfreiheiten*, hrsg. Dirk Ehlers. Berlin: De Gruyder, 2014.

Ünver, Yener ve Hakan Hakeri. *Ceza Muhakemesi Hukuku*. Cilt. 1. Ankara: Adalet Yayınevi, 2016.

Vatan, Zeki. *Ceza Muhakemesi Hukukunda Koruma Tedbiri Olarak Iletişimin Denetlenmesi*. İstanbul: Beta Yayınevi, 2009.

Wildhaber, Luzius und Stephen Breitenmoser. „Art. 8 EMRK." In *Internationaler Kommentar zur Europäischen Menschenrechtskonvention*, hrsg. Katharina Pabel und Stefanie Schmahl (Köln: Carl Heymanns Verlag, 2010).

Yenisey, Feridun ve Ayşe Nuhoğlu. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, 2015.

Yıldız, Mustafa. "Avrupa İnsan Hakları Mahkemesi'nin İşlevsel Konumu." *Anayasa Yargısı Dergisi* 14, (1997): 255-332.

BİLİŞİM SUÇLARINDA IP TESPİTİ İLE EKRAN GÖRÜNTÜLERİ ÇIKTILARININ İSPAT DEĞERİ

Evidence Value of Ip Address Detection and Screenshot Print Outs in Cybercrimes

Doğan Gedik*

Öz

Bilişim teknolojilerindeki baş döndürücü gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmiştir. İnternet ve bilişim teknolojilerindeki gelişmelerin yarattığı sorunlar, yalnızca yeni suç tiplerinin ortaya çıkması veya klasik suçların yeni işlenme şekilleriyle sınırlı kalmamış; buna bağlı olarak soruşturma ve delillendirme ile mevzuata dair yeni sorunların da ortaya çıkmasına neden olmuştur. Bu çalışmada; bilişim suçlarında uygulaması oldukça çok olan IP adresi (numarası) tespiti ile ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değeri üzerinde durulacaktır.

Anahtar Kelimeler: Dijital Delil, IP Numarası, Ekran Görüntüsü Çıktısı, İspat.

* Dr., İstanbul Bölge Adliye Mahkemesi Hâkimi, dogangedik@hotmail.com, ORCID: 0000-0001-6131-9726.

Makale Gönderim Tarihi: 27.03.2019.

Makale Kabul Tarihi: 18.05.2019.

Abstract

Developments in information Technologies bring new problems to both substantive and procedural law. These problems are not only limited to new crime types or the new ways to commit classical crimes but also affect evidence and cause issues related to body of laws. In this work, the importance of IP address detection and screenshot print outs, which are widely encountered in cybercrimes, as evidence in criminal procedure will be examined.

Keywords: Digital Evidence, IP Number, Screenshot, Evidence.

I. GİRİŞ

Son yılların en hızlı büyüyen bilişim sektörü olan internet; sınırları tanımlanamayan, kuralları konamayan, demokratik bir platform olarak kabul edilmekte;[1] bireylere, gerçek kimliğini gizleme veya başka bir ad kullanma imkânı da sağlayarak kendisini ve düşüncesini serbestçe ifade etme hürriyeti tanımaktadır.[2] Bu gelişme, dünyayı küçük bir köy haline getirirken, bilgisayar ortamında sesli ve görüntülü her türlü sohbet, özel hayatın paylaşılması, internet üzerinden alışveriş gibi birçok yeni gelişmelere öncülük etmiş, sonuçları olumlu veya olumsuz yeni alışkanlıklar kazandırmıştır.[3] Nitekim gelişen iletişim teknolojileri ile insanların hayatında önemli bir yer edinen sosyal medya,[4] hemen her yaştan, cinsiyetten ve kültürden insanların çevrelerini genişleteceği, iletişim kurabileceği, bilgi ve

---

1 Buna ilişkin örnek olarak, bkz. Ceren Yegen, "Demokratik Ve Yeni Bir Kamusal Alan Olarak Sosyal Medya," *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (Aralık 2013): 119*ff*.

2 Servet Yetim, "Bilişim Suçları ve Etkin Mücadele Yöntemleri," *Terazi Hukuk Dergisi* 9, no. 95 (Temmuz 2014): 80*ff*.; Ufuk Taşçı ve Ali Can, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2015): 229.

3 Taşçı ve Can**,** "Siber Suçlarla Mücadele," 230.

4 Bkz. Fehmi Şener Gülseren, "İnternet Ortamında İşlenen Hakaret Suçları," *LAÜ Sosyal Bilimler Dergisi* 4, no. 1 (Nisan 2013): 16; Yegen, "Yeni Bir Kamusal Alan," 120*ff*.; Ceren Çubukçu ve Berrin Atiker, "Sosyal Medya ve Bilişim Suçları," Academia, erişim tarihi Mayıs 5, 2019, https://www.academia.edu/31785425/ Sosyal_Medya_ve_Bilişim_Suçları. 2000'li yılların ortalarında Web 2.0 teknolojisinin kullanılmaya başlanması ile birlikte sosyal medya kavramı herkesin hayatına girmiştir. Sosyal medya, bireylerin internette birbirleriyle yaptığı paylaşımlar, diyaloglar ve sosyal ağ uygulamalarından oluşan bir dijital platformu ifade etmektedir. Örneğin kullanıcıların, kendi içeriklerini ürettiği ve paylaştığı Facebook, Youtube, Flickr gibi web ağları; yazarların, okurlarına bilgi, görüş ve düşüncelerini aktardıkları bloglar; anlık paylaşımların yapıldığı Twitter gibi mikro bloglar ve bunların yanında, e-posta ve sohbet siteleri, iletişim ve mesajlaşma programları, forumlar, diğer bir deyişle, kişilerin internet yoluyla yaptıkları tüm bilgi ve içerik paylaşımları sosyal medyayı oluşturmaktadır.

deneyimlerini paylaşıp üzerinde tartışmalar yapabileceği bir platform haline gelmiştir.[5]

İnternet ve bilişim teknolojilerindeki gelişmelerle birlikte bireyin kişisel, ekonomik, siyasi ve sosyal birçok faaliyeti sanal ortama taşınmış, günlük hayata dair ne varsa sanal ortamda yaşanır olmuştur. Bu şekilde internet ve dolayısıyla sosyal ağların, kullanıcılarının bireysel ve sosyal yaşamlarına kolaylık ve katkı sağlayarak hayatın merkezine yerleşmesi, adeta vazgeçilmez hale gelmesi suçluluk olgusuna da davetiye çıkarmıştır. Nitekim bu durum hem bazı yeni suç tiplerinin ortaya çıkmasına neden olmuş, hem de hakaret, tehdit, şantaj ve dolandırıcılık gibi klasik suçların bilişim sistemleri aracı kılınmak suretiyle işlenmesine zemin hazırlamıştır. Ancak bilişim dünyasındaki gelişme yalnızca yeni suç tiplerinin ortaya çıkması veya klasik suçların yeni işlenme şekilleriyle sınırlı kalmamış; buna bağlı olarak soruşturma ve delillendirme ile mevzuata dair yeni sorunların da ortaya çıkmasına neden olmuştur. Zira suç mahalli genişleyerek fiziksel alandan dijital ortama kaydığı gibi klasik delillerden farklı özellikler taşıyan, bilgisayar ve benzeri cihazlar ile bilişim sistemlerinden elde edilen bir delil türü (dijital/sayısal delil) ile delillendirme sürecini (adli bilişim) ortaya çıkarmıştır. Böylece bilişim teknolojilerindeki gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmiştir.

Bu çalışmada, ağırlıklı olarak sosyal ağlar üzerinden işlenen suçlar olmak üzere bilişim suçlarının soruşturulmasında adeta bir anahtar vazifesi gören IP adresi (numarası) tespiti ile gerek şikayetçi/ihbarcı kişi veya kurumların şikayete ekledikleri gerekse soruşturma makamlarının dosyaya dahil ettiği ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değeri üzerinde durulacaktır.

---

[5] Gülçin Cebecioğlu ve İpek Beyza Altıparmak**,** "Dijital Şiddet: Sosyal Paylaşım Ağları Üzerine Bir Araştırma," *Sakarya University Journal of Education* 7, no. 2 (2017): 424; Yegen, "Yeni Bir Kamusal Alan," 120; Gürkan Özocak**,** "Sosyal Medyada İşlenen Suç Tipleri Ve Suçluların Tespiti," Özocak Hukuk & Danışmanlık, erişim tarihi Mart 11, 2019, http://www.ozocak.com/Dosyalar/a104b3.pdf.

II. IP TESPİTİNİN İSPAT DEĞERİ

A. Kavram ve IP Tespiti

İnternet hizmetlerini kullanmak için gerekli olan tüm yazılımlar ve bağlantı yazılımları TCP/IP protokollerine uygun olarak iletişim kurar ve işlem görürler. Bu protokoller kümesinin ulaşım katmanında TCP (Transfer Code Protocol), yönlendirme katmanında ise IP (Internet Protocol) protokolü bulunmaktadır. TCP/IP protokolü dâhilinde her bilgisayarın tanınmasını sağlayan ve birbirinden ayıran bir IP adresi vardır.[6]

IP adresi,[7] internete bağlanmak isteyen bilgisayarlara internet servis sağlayıcıları tarafından atanan benzersiz bir kimlik numarasıdır. Günümüzde bilgisayar dışında internet bağlantısı sağlayabilen akıllı telefonlar, televizyonlar, tabletler de IP adresi almaktadır.[8]

---

6 Elif Gökşen, "Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri" (yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2014), 31.

7 IP adresi: "Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres," İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m. 3/1-h.

8 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayıncılık, 2014), 694*ff*.; Murat Volkan Dülger ve Gözde Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku (Uygulama Rehberi)* (Ankara: Türk Ceza Adalet Sisteminin Etkinleştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, 2014), 109*ff*. İnternete bağlandığınızda sizin bilgisayarınızın da bir IP adresi vardır. ISS'nize telefon numarasını çevirip bağlandığınızda, aslında o ISS'de yer alan bir sunucu bilgisayara bağlanıyorsunuz demektir. Bu sunucu bilgisayar, bağlantı sırasında kullandığınız kullanıcı ismi ve şifrenize göre elindeki boş adreslerden birini (örneğin 212.172.xxx.xxx gibi) İnternet Protokolü (IP) numarasını bilgisayarınıza atar. Bu yüzden her bağlantıda IP adresinizin son numarası değişir. Ancak IP numaranız değişse bile sunucudaki LOG kayıtlarında hangi tarihte ve saatte hangi IP adresinin hangi telefon numarasına tahsis edildiği saklanır. Artık internette dolaşırken sizin kimliğiniz aldığınız IP numaranızdır. Siz de Web sitelerine, e-posta kutularına bağlanırken size atanmış olan bu IP adresini kullanırsınız. Bazı IP adresleri ise sabittir (static IP), yani IP adresleri hiç değişmez. Bir Web sitesinin adresi her yazıldığında bulunabilmesi için IP adresi genellikle sabittir.

Böylece internete bağlanan her cihaz bir IP numarası almakta ve diğer cihazlarda bu cihaza IP adresi ile ulaşmaktadırlar. IP numarası, servis sağlayıcı tarafından boşta olan bir numaranın verilmesi suretiyle her bağlantıda değişebileceği[9] gibi, erişim sağlayıcılar tarafından, ADSL abonelerine verilenlerde olduğu şekliyle statik de olabilir.[10] Bu nedenle IP adresleri kendi içinde statik ve dinamik olmak üzere ikiye ayrılmaktadır.[11]

IP numarası sayesinde bağlı olan abone ve lokasyon bilgilerine ulaşmak mümkün hale gelmektedir. Bu özelliği dolayısıyla IP adresi (numarası), sanal âlemde bilişim sistemi kullanıcılarını tanımlayan en önemli ayırt edici unsur olarak karşımıza çıkmaktadır.

Yukarıdaki açıklamadan da anlaşıldığı üzere bilişim suçlarında veya bilişim sistemleri araç olarak kullanılması suretiyle işlenen suçlarda, gerek failin gerekse lokasyonun belirlenmesi için IP adres bilgisine ihtiyaç bulunduğu kuşkusuzdur. Soruşturmada yol alınması, en nihayetinde delillendirilmesi noktasında IP kayıtlarının düzenli ve doğrulanabilir/kanıtlanabilir şekilde tutulmuş olmasının da önemi büyüktür. IP adresi belirlenmeye çalışılırken, zaman bilgilerine (tarih, saat, dakika, saniye) ve yurtdışından temin edilecekse saat farkına da dikkat edilmelidir. Yanlış bildirilen bir IP numarası, soruşturmanın seyrini değiştirebildiği gibi olayla ilgisi olmayan kişi/kişilerin şüpheli veya sanık olmasını da sonuçlayabilmektedir.[12] Nitekim 5651 sayılı

---

[9] Bu değişkenlik nedeniyle IP numarasının kullanıldığı tarih ve saatin kaydedilmesi oldukça önemlidir; zira, ancak bu tarih ve saate göre o sırada hangi bilgisayarın söz konusu IP numarasına sahip olduğu belli olur.

[10] Burcu Erdoğan, "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?," *digiSophia*, erişim tarihi Ekim 1, 2018, http://www.digisophia.com/Article/Details/61.

[11] "Statik IP adresi; hiçbir zaman değişmeyen, kalıcı bir IP adresidir. Dinamik IP adresi ise bir cihaza, internete her bağlanışında yeniden tanımlanan yani geçici bir IP adresidir. Statik IP adresleri bilgisayara, bir admin tarafından manuel olarak atanır. Dinamik IP adresleri ise bilgisayar arayüzü ya da sunucu yazılımı tarafından, otomatik olarak atanır. IP adresleri, servis sağlayıcı tarafından, statik olacak şekilde de tanımlanabilir." "IP Adresim Nedir," CHIP Online, erişim tarihi Mayıs 25, 2019, https://www.chip.com.tr/ip-adresim-nedir.

[12] Erdoğan: "Özellikle Kredi kartı dolandırıcılığı olarak adlandırılan suçlarda mahkemeler sadece bankanın sunmuş olduğu IP bilgisinden yola çıkmaktadır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, taraflara ait IP adresi bilgisini *"trafik bilgisi"* içinde kabul etmiş (m. 2/1-j; ve "*erişim sağlayıcıları*" (m. 6/1-b), "*yer sağlayıcıları*" (m. 5/3) ile "*toplu kullanım sağlayıcıları*"na (m. 7/2) trafik bilgilerini tutma yükümlülüğü yüklemiştir.[13] 5651 sayılı Kanuna dayanarak çıkarılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" de "*erişim sağlayıcı"*nın, trafik bilgisini bir yıl

Ancak bu aşamada verilen rakamlardaki en ufak bir hata dolayısı ile soruşturmanın seyrinin tamamen değişeceği düşünülmüş müdür? Bankalar bu bilgileri zaman damgalı olarak vermişler midir? Birçok yargılamada, IP bilgilerinin kaynağının güvenilir olup olmadığının araştırılması gerekirken, araştırma yapılmadığı gözlemlenmektedir. Çoğu zaman verilen IP ile ilgili sağlanan bilgilerin doğru kabul edilmesi sonucu yanlış mahkumiyet kararı verilebildiği gibi, bir çok sanık da internet bağlantılarının şifresiz olduğu ya da IP bilgisinin değiştirilmiş olabileceği savunmaları ile (başkaca delil yoksa) beraat ettikleri görülmüştür. Peki, gerçek sanıkların bıraktığı izler nerededir, ne yazık ki soruşturma makamları, bu sorunun cevabını halen verebilecek nitelikte değildir. Sayı üretmek zor olmadığından soruşturmanın yönünün ya da davanın seyrinin yetkisiz kimseler tarafından tutulan ve güvenli olmayan bilgiler doğrultusunda yönlendirmek verilen hükmün güvenilirliğini de tartışma konusu haline getirir." "Bir Kişiyi Suçlamak."

13 5651 sayılı Kanunda "trafik bilgisi", taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini (m. 2/1-j; "erişim sağlayıcı", kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri (m.2/1-e); "yer sağlayıcı", hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri (m. 2/1-m); "toplu kullanım sağlayıcı", kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı (m. 2/1- i) ifade eder şekilde tanımlamıştır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik 3. maddesinde "erişim sağlayıcı trafik bilgisi"ni, "İnternet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri" (m.3/1-g); "yer sağlayıcı trafik bilgisi"ni, "İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri" (m.3/1-ş) ifade eder şekilde tanımlamıştır.

saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü, oluşan verilerin dosya bütünlük değerlerini zaman damgası[14] ile birlikte muhafaza etmek ve gizliliğini temin etmekle (m. 8/1-b); "*yer sağlayıcı*"nın da trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle (m. 7/1-c) yükümlü olduğunu belirtmiştir. 11.04.2017 tarihli ve 30035 sayılı Resmi Gazetede yayınlanan "*İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik*" de ticari olsun olmasın internet toplu kullanım sağlayıcılarına; kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri, hedef IP adresi, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgilerini, elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamakla yükümlendirmiştir (m. 4-5). Aynı yönetmelik toplu kullanım sağlayıcıları için kamera kayıt yükümlülüğü de getirmiştir. Düzenlemeye göre "Güvenlik amacıyla işyerlerinin giriş ve çıkışlarını görecek şekilde yüksek çözünürlüklü (en az 3 mega piksel) ve "IR" (gece görüşlü) kamera kayıt sistemi kurulur. Bu sistem aracılığıyla elde edilen kayıtlar doksan gün süreyle saklanır ve bu kayıtlar yetkili makamlar haricindeki kişi ve kuruluşlara verilemez" (m. 9/1-ğ).[15]

---

[14] 5070 sayılı Elektronik İmza Kanununda "zaman damgası", "*Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı, ifade eder*" olarak tanımlanmıştır. Zaman damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar. Zaman damgası sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar. Sertel Şıracı, "İnternet Kanununa Göre Log Tutma," Av. Sertel Şıracı, erişim tarihi Şubat 02, 2019, https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/internet-kanununa-gore-log-tutma.html.

[15] 5651 Sayılı Kanun ile ilgili üzere yönetmelikler, tebliğler, genelgeler, Bakanlar Kurulu Kararları gibi ikincil mevzuatı da içeren internet hukukuna ilişkin güncel mevzuat ve içtihatlara dair kaynak için, bkz. Mehmet Bedii Kaya, "İnternet Hukuku, Mevzuat & İçtihat," Mehmet Bedii Kaya, erişim tarihi Mayıs 25, 2019, https://www.mbkaya.com/hukuk/internetmevzuat.pdf.

Erdoğan'ın belirttiği üzere, bütün bu yasal hükümlerde, trafik bilgilerini hangi kurumların tutması gerektiği, nasıl tutması gerektiği ve gizliliğini sağlamaları gerektiği açıkça yazılmış, ancak yasal süreçte bunların nasıl sunulması gerektiği konusunda hiç bir usul belirtilmemiştir. Ancak verilerin zaman damgası ile saklanması gerektiği belirtildiğine göre, bu verilerin delil niteliğinde olabilmesi için değişmemiş ve bozulmamış halde olduğunu gösteren bir biçimde mahkemeye sunulması gerektiğini de çıkarabiliriz.[16]

B. IP Tespitinin İspat Değeri

Uygulamada bir başkasının bilişim sistemine girme, sosyal medya hesaplarını (örneğin Facebook) veya e-posta adreslerini ele geçirme gibi bilişim suçlarında ya da sosyal paylaşım siteleri üzerinden kişisel verileri yayma, hakaret veya şantajda bulunma örneğindeki gibi bilişim sistemleri aracı kılınarak işlenen suçlarda faile ulaşmak için en yaygın kullanılan yöntem, suça konu işlem yapılırken kullanılan IP numarasının tespit edilmesi[17] ve daha sonra IP

---

16 Erdoğan, "Bir Kişiyi Suçlamak."

17 Belirtelim muhatap yurtdışı merkezli ve Türkiye temsilciği yok ise IP numarasının tespiti ancak "Uluslararası Adli İstinabe" yoluyla mümkündür. Bununla birlikte ABD merkezli sosyal ağlar (Facebook, Twitter, YouTube), sınırlı bazı suçlar dışında istinabe yoluyla trafik bilgi taleplerini karşılamamaktadır. Örneğin Facebook, çocuk pornosu, intihar vakaları, öldürme gibi suçlar dışında bilgi paylaşımına yanaşmamaktadır. Söz gelimi hakaret suçu konulu soruşturmalarda yapılan istinabelerde olumlu sonuç alınamamaktadır. Bu sebeple uygulamada şirket merkezinin yurt dışında olduğu ve delile ulaşmanın mümkün olmadığı gerekçe gösterilerek takipsizlik kararı verildiği gibi mahkûmiyeti gerektirir delil elde edilmediği gerekçesiyle beraat kararı da verilebilmektedir. Örneğin, "Sanığın, bahse konu facebook hesabının kendisi tarafından oluşturulmadığına yönelik savunması, şikâyete konu hesabın oluşturulduğu bilgisayarın IP adres bilgilerinin tespit edilememiş olması, katılanın eşi olan tanık Zeynep, duruşmada alınan ifadesinde, iddiayı doğrular mahiyette beyanda bulunmuş ise de, tanığın görgüye dayanmayan ve maddi delille desteklenmeyen anlatımına dayalı olarak iddiaya konu eylemleri gerçekleştirenin sanık olduğu sonucuna varılamayacak olması, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğünün, "İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri" başlıklı yazısında yer verdiği, "ABD mevzuatına göre (18 U.S.C. §

numarasının tahsis edildiği internet abonesinin belirlenmesidir.[18] Ancak bu yöntem doğru olmakla birlikte, bu tür suçlara ilişkin soruşturmalarda yapılan en yaygın hatalardan biri de, IP numarası belirlendiğinde, tahsis edildiği internet abonesinin hemen "şüpheli" sıfatıyla soruşturmaya dahil edilmesi, hakkında doğrudan dava açılabilmesi ve hatta sadece IP tespitine dayanarak mahkum edilmesidir. Oysa bu, yanlış bilgi veya kolaycılıktan kaynaklanan bir tutumdur.[19] Nitekim adli bilişim esaslarına uygun yürütülen bazı soruşturmalarda, olayla ilgisi bir yana abonenin olaydan haberi dahi olmadığı görülmüştür. Bu nedenle dijital ortamda veri bazlı işlemi gerçekleştiren kişinin tespit edilmesi, diğer delil ve yöntemlerle verinin "kişiselleştirilmesi" gerekmektedir.[20]

Anlaşıldığı üzere bilişim suçlarında soruşturmanın yönlendirilmesi ve nihayetinde faile ulaşılması bakımından IP numarasının

2703 – f) internet ortamında işlenen suçlara dair trafik bilgileri, yer sağlayıcılar veya erişim sağlayıcılar tarafından 90 gün süreyle saklanmaktadır. Bu süre içinde resmi otoritelerce başvurulduğunda anılan saklama süresine 90 gün daha ilave edilmektedir." açıklamalarına, olayın üzerinden geçen zaman dilimine ve dosya kapsamına nazaran, gelinen aşamada, savunmanın aksine maddi bir delil elde edilmesi imkânının bulunmaması karşısında, sanığın mahkumiyetine yeter, her türlü derecede şüpheden uzak, kesin ve inandırıcı delil bulunmaması sebebiyle üzerine atılı hakaret ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından dolayı CMK'nın 223/2-e maddesi gereğince beraatine karar verilmesi gerekirken, dosyada mevcut delillerden hangilerine hangi sebeplerle itibar edildiği irdelenmeyip, yasal, yeterli ve geçerli bir gerekçeye dayanılmaksızın, yazılı şekilde sanık hakkında mahkumiyet kararı verilmesi" Yar. 12. CD, E.2015/4151, K.2016/259, 13.01.2016, (UYAP). Uluslararası istinabe konusunda ayrıca, bkz. Özocak, "Sosyal Medyada İşlenen."

[18] Örneğin, "hesaba Konya ilinde İ. H. Ç. adına kayıtlı bir IP adresinden girilerek gerçekleştirildiğinin tespit edilmesi karşısında İ. H. Ç.in konuya ilişkin beyanının alınması, sonucuna göre sanığın hukuki durumunun değerlendirilmesi gerektiği gözetilmeden eksik araştırma ve inceleme ile yazılı şekilde hüküm kurulması," Yar. 2. CD, E.2016/14036, K.2018/14990, 06.12.2018, (UYAP).

[19] Dülger, *İnternet İletişim*, 695.

[20] Kişiselleştirme kavramı için, bkz. Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Ankara: Seçkin Yayıncılık, 2014), 404*ff.*; Koray Doğan, *Kuşkudan Sanık Yararlanır İlkesi* (Ankara: Seçkin Yayıncılık, 2016), 295. Nitekim Yargıtay içtihatlarında sıkça geçen "IP adresini kullanan abonenin sanıkla bağlantısı araştırılıp" ifadesi kişiselleştirmeye vurgu yapmaktadır.

tespiti oldukça önemli bir eşiktir.[21] Ancak hem IP numarasının tespiti hem de bundan yola çıkarak failin tespiti, suçun sanal ortamda işlenmesinden kaynaklı kendine özgü zorlukları ihtiva etmekte ve adli makamları daha ihtiyatlı olmaya zorlamaktadır. Gerçekten de tespit edilen IP numarasını kullanan abonenin adresi internet kafe, otel veya alışveriş merkezi gibi yerler çıktığında failin tespiti zorluk arzetmektedir.[22] Yukarıda zikrettiğimiz 5651 sayılı Yasa ve ikincil

---

[21] Yunus Balı: "Öncelikle, nereye veya kime ait olduğu bilinmeyen bir IP numarası için "Whois" sorgulaması yapılır. "Whois" sorgulaması sonucunda söz konusu IP'nin kullanıcılara tahsis işlemlerini gerçekleştiren organizasyona yani servis sağlayıcıya ulaşılmış olur. Bu aşamaya kadar herkes genel bir tespit yapabilir. Yani bir IP'nin hangi ülkeden, hangi şehirden bağlandığı yukarıdaki gibi basit bir işlemle tespit edilebilir. Ancak o IP numarasının kim tarafından kullanıldığının tespiti isteniyorsa, bu bilgi yasal yollardan elde edilmesi gereken ve yargı makamları tarafından yapılacak bir tespitle verilebilen bir bilgidir." "IP Numarası Tespiti," Dijitaldeliller, erişim tarihi Aralık 1, 2018, http://www.dijitaldeliller.com/ip_tespiti.html.

[22] "Sanığın aşamalardaki savunmalarında; suç tarihinde internet cafe sahibi olduğunu, evde ve iş yerinde kablolu internet kullandığını, atılı suçu kabul etmediğini belirtmesi karşısında; sanığın iş yerinde bulunan modemin kablosuz bağlantı (wifi) özelliği olan modem olup olmadığı ve buna göre de dışarıdan üçüncü bir kişinin haricen bağlantı yapıp yapmayacağı araştırılıp, ayrıca tespit edilen IP numarasının statik mi yoksa dinamik mi olduğu kurumdan sorulup, yapılacak bu tespitler ile sanığın savunmasının örtüşüp örtüşmediği, IP numarasının kopyalanması, kablosuz veya kablolu bağlantı ile internet hattına girilerek havale işlemi yapılmasının mümkün olup olmadığı hususlarının araştırılarak, yapılan eylemin üçüncü bir kişi tarafından gerçekleştirme olasılığının bulunup bulunmadığı hususlarının aydınlatılması için somut olaya ilişkin konusunda uzman bilirkişi incelemesi yaptırılarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeden, eksik inceleme ile mahkûmiyet hükmü kurulması" Yar. 2. CD, E.2018/6474, K.2018/1368, 20.11.2018, (UYAP).

"Sanığın internet cafe çalıştırdığını, merkez bilgisayara bağlı 30 adet bilgisayar bulunup tek hat üzerinden internete bağlanıldığını, bu bilgisayarlardan böyle bir işlem yapılmış olabileceğini savunması karşısında; merkez bilgisayar ve buna bağlı başka bilgisayarın bulunup bulunmadığı, işlemin hangi bilgisayardan yapıldığı, merkez bilgisayarda suça konu işlemlere ilişkin bir kaydın bulunup bulunmadığı, GSM şirketi tarafından IP adresi yanında PORT numarası verilip verilmediği, PORT bilgisine ulaşıldığında birden fazla kişiye verilen IP'nin belirlenen saatte kim tarafından kullanıldığı tespit edilmeden ayrıca mağdurun kredi kartı bilgileri haksız olarak ele geçirilerek internet üzerinden kontör yük-

mevzuat uyarınca müşterilerine şifreli veya şifresiz şekilde kablosuz internet hizmeti sağlayan bu tür yerlerin; hem iç IP dağıtım loglarını elektronik ortamda kendi sistemlerine kaydetmek, hem de bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydedip saklamak yükümlülükleri bulunmaktadır.[23] Bu nedenle zaman geçirilmeden bu kayıtların, kamera kayıtlarıyla birlikte temin edilmesi gerekmektedir.[24] Ancak işletmecilerin her zaman kayıt tutma yükümlülüğünü mevzuata uygun şekilde yerine getirdiklerinden söz etmek mümkün görünmemekte, bu da failin belirlenmesini zorlaştırmaktadır.

Diğer taraftan tespit edilen adres konut çıktığında ise uygulamada başta abone görünen kişi olmak üzere, duruma göre konutta yaşayan diğer kişilerin de ifadesine başvurulmaktadır. Ancak böyle bir durumda kişi veya kişilerin suçlamayı kabul etmemesi veya örneğin 3. kişiler tarafından şifresi kırılmak suretiyle internete girilmiş olabileceği şeklinde savunmada bulunulması[25] halinde, soruşturmanın derinleştirilmesi, özellikle adli bilişim yöntemleriyle failin belir-

leme işlemi yapıldığı iddia olunduğundan, kontör yüklendiği belirlenen telefon hatlarının, suç tarihindeki hat sahipleri ve kullanıcıları araştırılıp, tanık sıfatıyla dinlenerek ve tüm deliller birlikte değerlendirilerek sonucuna göre sanığın hukuki durumunun tayini ve takdiri gerektiği gözetilmeden, eksik araştırma ile yazılı şekilde karar verilmesi," Yar. 8. CD, E.2014/11582, K.2013/9756, 6.5.2014, (UYAP).

[23] 5651 sayılı Kanun kapsamında yer alan erişim sağlayıcılar, yer sağlayıcılar, içerik sağlayıcılar, internet toplu kullanım sağlayıcılarının yükümlülükleri konusunda ayrıntılı bilgi için, bkz. Yasemin Durnagöl, "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar," *Türkiye Adalet Akademisi Dergisi* 2, no. 4 (2011): 382*ff*.

[24] "Oluşa ve tüm dosya kapsamına göre, katılanın mail adresine girildiği tespit edilen IP numarası adına kayıtlı olan sanığın internet kafe işlettiğini ve tüm bilgisayarların aynı IP'ye bağlı olduğunu beyan etmesi üzerine beraat kararı verilmiş ise de, IP numarasının internet kafeye ait olup olmadığı hususu ve bilgisayarlara ait LOG kaydı bulunup bulunmadığı araştırılmadan eksik inceleme ile yazılı şekilde beraat kararı verilmesi" Yar. 8. CD, E.2013/2357, K.2014/7186, 20.03.2014, (UYAP).

[25] Gerçekten de kablosuz modem belli bir abone adına kayıtlı IP adresi üzerinden hizmet vermektedir. Eğer modem şifrelenmemiş veya uygulamadaki tabiriyle şifresi kırılmışsa, sinyalinin ulaştığı her yerden internete bağlanmak mümkün hale gelmektedir. Aynı yönde, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 406.

lenmesi yoluna gidilmesi gerekmektedir.[26] Bilişim sisteminde yer alan verinin, işlendiği iddia edilen suçun delili olup olmadığı, delil niteliğinde ise doğru ve inanılır olup olmadığı hususlarında teknik bilgiye ihtiyaç duyulabilecektir. Bu şekilde çözümü uzmanlık ve teknik bilgi gerektiren durumlarda delillerin değerlendirilmesine imkan sağlamak bakımından bilirkişiden istifade edilecektir.[27]

---

[26] "Sanığın suçlamayı kabul etmeyerek, kablosuz modem kullanıldığından hattının başkaları tarafından girilip kullanılmış olabileceğine ilişkin savunması karşısında; bildirilen IP numaralarının bağlı bulunduğu internet hattında ne özellikte modem kullanıldığı, kablolu veya kablosuz olup olmadığı, şifreli olup olmadığı, modemden başka kullanıcıların internete bağlanılıp bağlanılmadığının belirlenmesi açısından ilgili internet sağlayıcısından bilgi istenmesi ve sanığa ait bilgisayar getirtilip uzman bilirkişi tarafından LOG kayıtları incelenerek sonucuna göre" Yar. 8. CD, E.2016/12634, K.2017/4967, 03.05.2017, (UYAP).

"…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." Yar. 11. CD, E.2008/16570, K.2009/101, 28.01.2009, (UYAP).

"Sanığın, bahse konu elektronik posta adresi ile sahte facebook hesabının sahibi ve kullanıcısı olmadığını, kablosuz ağ üzerinden internet hizmeti aldığı ve kablosuz modemine şifre koymadığından üçüncü kişilerin hattına giriş yapıp, kendisinden habersiz iddiaya konu eylemleri gerçekleştirmiş olabileceğini ifade etmesi, sanığın savunmasını doğrular mahiyette, sanığa ait bilgisayar ve modem üzerinde yapılan teknik inceleme sonucu hazırlanan 21.03.2012 tarihli bilirkişi raporunda, ..." Yar. 12. CD, E.2013/20187, K.2014/11414, 12.05.2014, (UYAP).

[27] Değirmenci, *Sayısal (Dijital) Delil*, 402. "23.10.2008 tarihli bilirkişi raporunda, sanık B.Yalçın'ın bilgisayarına bağlı modem hattının kablosuz olması durumunda modemin markasına göre değişmekle beraber 500 metre alan içerisinde herhangi bir şahsın bilgisayarı ile 88.229.208.155 IP numarasından suç konusu paranın havale edilmiş olabileceği belirtildiğinden; bilgisayar ve internet kullanmayı bilmediğini, bilgisayarın sadece çocuklarının dersleri için kullanıldığını savunan sanık B. Yalçın'ın bilgisayarının, modemin ve dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiye tevdi edilerek adı geçen sanığın bilgisayarına bağlı modemin türünün tespit edilmesi, modem hattının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, sanığın internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, sanığın bilgisayarına virüs gönderilerek bilgilerinin alınıp alınmadığı konularında rapor düzenlettirilmesi, gerekirken bu hususlar araştırılmadan eksik soruşturma ile hüküm kurulması" Yar. 13. CD, E.2012/3887, K.2013/15354, 21.05.2013, (UYAP).

Dijital birçok veri gibi (ister statik atanmış olsun ister dinamik olsun) IP adreslerinin de çeşitli yöntemlerle (örneğin Proxy vasıtasıyla gerçeği gizlenerek veya başka kullanıcıya ait IP numarası kopyalanarak) değiştirilebilmesi mümkün[28] olup bu tür durumlarda faile ulaşmak da o kadar güçtür. Diğer yandan IP adresi, teknik açıdan çoğu zaman doğrudan bir bilgisayarı veya bir kişiyi göstermekten ziyade, yalnızca bir internet aboneliğini gösterebilir.[29] Abonelik ise bir kişiyle sınırlandırılamayacak olup, internete bağlanma hakkı olan hesaba erişimi olan herkesi işaret etmektedir.[30] Bu nedenle yukarıda izah edilen kolaycı bir yaklaşımın yerine tespit edilen IP'nin diğer teknik verilerle, söz gelimi kişiye ait bilgisayar, cep telefonu gibi elektronik cihazların adli içerik incelemesi ile MAC adresinin tespitiyle desteklenmesi gerekir[31] ki, sanığın suçu işlediğine dair

---

[28] Dijital verilerin en önemli özelliklerinden biri de kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olmalarıdır. Bu konuda, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 132*ff*., 405**.** Nitekim Gülsel Öykü Özç**e**lik: "TCP yönlendirmesi, "proxy" sunucular, paket yönlendirmeleri, web ve e-posta isimleri, IP adresi ve e-posta adresi ele geçirme, oturum engelleme, DNS yanıltma gibi uygulamalar söz konusu delile şüpheden arındırılmış bir delil olarak yaklaşılmasını imkansız kılar." "IP Adresleri Tek Başına Delil Olabilir Mi? IP Adreslerine Yargılamada Ne Kadar Güvenilir?," TAG Hukuk Bürosu, erişim tarihi Ekim 1, 2018, taghukuk.com/wp-content/uploads/2018/04/ip_adreslerinin_delil_niteliği.pdf.

[29] "…IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi.., kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılınmamıştır" Yar. 8. CD, E.2012/21817, K.2013/25428, 24.10.2013, (UYAP).

[30] Özçelik**, "**IP Adresleri."

[31] "Maddi gerçeğin ortaya çıkarılması açısından, suç tarihinde sanığın ve katılanın kullandığı facebook hesaplarına girmeye elverişli bilgisayar, telefon, tablet vb. cihazların neler olduğunun ve halen taraflarda olup olmadığının tespitine çalışılması, tespiti halinde bu cihazlardan, aksi durumda halen kullandıkları cihazlardan "Ümmüye Şoleum" isim ve soyismiyle açılan facebook adresinin ve tespit edildiği takdirde buna bağlı mail adresinin kullanılıp kullanılmadığı, kullanıldığı tespit edildiği takdirde hangi tarihler arasında girildiği, ayrıca soruşturma aşamasında dosyaya sunulan facebook çıktısı örnekleri esas alınmak suretiyle, internet servis sağlayıcısı ve IP adresinin tespit edilip edilemeyeceği hususunda, bilişim alanında uzman bilirkişilerden rapor aldırılması ayrıca sözkonusu hesabın üzerindeki bilgilerden yola çıkarak açık kaynak araştırması yapılmak suretiyle ve sonucuna göre sanığın hukuki durumunun belirlenmesi" Yar. 4. CD, E.2014/32543, K.2018/21151, 05.12.2018, (UYAP).

şüphe ortadan kalksın ve bu yönde hüküm kurulabilsin.[32] Gerçekten de suçun kesin şekilde ispatlanabilmesi için adreste arama yapılması; bilgisayar veya bilgisayar özelliği taşıyan tablet, akıllı telefon ve hatta smart tv gibi cihazlar tespit edilip, CMK'nın 134. maddesi gereğince bu cihazlarda içerik araması yapılması gerekebilir. Bununla birlikte CMK'nın 134. maddesine göre arama yapılırken suç ile uygulanacak tedbir arasındaki dengenin de gözetilmesi[33] ve elbette ki CMK 134.maddede düzenlenen koruma tedbirinin koşullarının da gerçekleşmesi gerekmektedir.[34] Zaten, cihazlar formatlanmışsa veya özel programlar kullanılarak içerik silinmişse aranılan içeriğe ulaşma şansı da azalmaktadır.[35]

---

[32] Özçelik, "IP Adresleri."

[33] "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma 5271 Sayılı CMK'nın 134. maddesinde düzenlenmiş olup, CMK'nın 116 ve 123. maddeleri arasında yer alan arama koruma tedbirinin özel bir görünümünü oluşturmaktadır. CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan verilerin; sıhhatini ve güvenliğini sağlamak amacıyla ve bireyin özel hayatına, kişisel verilerine yönelik olumsuz tesirleri göz önünde tutularak "son çare" olarak başvurulabilecek "özel koşullara bağlı" bir koruma tedbiri olması nedeniyle, genel adli aramadan ayrıksı ve istisnai olarak, ayrıntılı düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür" Yar. 16. CD, E.2015/2056, K.2017/5023, 21.09.2017, (UYAP).

[34] "Ceza muhakemesi hukukunda, elektronik delillerin toplanması, bir başka deyişle bilgisayarlarda yapılacak delil araştırması Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenmiştir… Şu unutulmamalıdır ki, delil araştırmasının bu aşamasında CMK tarafından öngörülen usule eksiksiz bir biçimde uyulması delillerin hukuki olması ve ceza yargılamasında verilecek hükme esas teşkil edebilmesi açısından son derece önemlidir" Özocak, "Sosyal Medyada İşlenen."

"…CMK'nın 134. maddesi uyarınca bilgisayar ve bilgisayar kütükleri üzerinde arama yapılmasına dair hakim tarafından verilmiş bir karar bulunmadığı cihetle, arama sonucu 2 adet harddiskte bulanan 471 adet filmin hukuka aykırı şekilde elde edilmiş delil niteliğinde olması sebebiyle hükme esas alınamayacağı ve atılı suçlamayı kabul etmeyen sanık hakkında hukuka aykırı şeklinde elde edilmiş bu delil dışında mahkumiyetine yeterli başkaca bir delil de bulunmadığı gözetilmeden, beraati yerine yazılı şekilde mahkumiyetine karar verilmesi" Yar. 19. CD, E.2015/11396, K.2016/1087, 02.02.2016, (UYAP).

[35] Dülger ve Modoğlu, *Soruşturma ve Kovuşturma*, 162.

Yukarıdaki açıklamalar ışığında sonuca bağlayacak olursak; IP adresi (numarası), adres sahibi tarafından suçun işlendiğini doğrudan göstermez.[36] Bu nedenle IP adresi soruşturma için bir sonuç değil, ancak başlangıç noktası olarak kabul edilebilir.[37] IP numarası kullanılarak tespit edilen adreste sadece internet abonesi yaşasa dahi o kişi ikrarda bulunmadıkça veya diğer delillerle desteklenmedikçe, sadece IP numarası esas alınarak o kişi hakkında mahkumiyet hükmü verilmesi doğru değildir.[38] Dolayısıyla IP adresi, tek başına mahkûmiyeti gerektiren bir delil niteliği taşımayacak**,** ancak ikrar veya başkaca destekleyici deliller de varsa mahkumiyet kararı verilebilecektir. Yargıtay'ın yaklaşımı da bu yöndedir.[39]

---

[36] Değirmenci, *Sayısal (Dijital) Delil*, 108, 405.

[37] Dülger, *İnternet İletişim*, 695-696.

[38] Aynı yönde, bkz. Doğan, *Kuşkudan Sanık*, 295.

[39] "Sanık S. Kaya'nın tüm aşamalarda atılı suçu işlemediğini savunduğu, katılan şirketin hesabından alındığı belirtilen paranın sanık tarafından alındığına veya sanığın hesabına aktarıldığına ilişkin maddi delil ve tanık beyanı bulunmadığı ve sanık S. Kaya'nın katılan tarafa ait paranın çekilmesi için şifre bilgilerinin gönderildiği telefon hattını kullandığı iddia olunan diğer sanık S. Adgu'yu da tanımadığı ve yakınana ait internet bankacılığı hesabına girilmek suretiyle paranın başka hesaplara aktarılmasında kullanılan bilgisayarın sanık S. Kaya'nın internet cafe olarak kullandığı işyerindeki bilgisayar olmasının tek başına sanığın atılı suçu işlediğini ispata yetmeyeceği gözetildiğinde; sanığın atılı hırsızlık suçunu işlediğine dair delillerin nelerden ibaret olduğu karar yerinde denetime olanak sağlayacak şekilde açıklanmadan, " …söz konusu IP numarasının kullanıldığı bilgisayarın sanık S. Kayanın işletmekte olduğu internet cafede kullanıldığı…" şeklindeki yetersiz gerekçeyle sanık Sinan Kaya'nın atılı suçtan mahkûmiyetine karar verilmesi, yasaya aykırıdır" Yar. 12. CD, E.2012/18065, K.2012/45207, 06.11.2012, (UYAP).

"Dosya kapsamına göre; sanığın, bir süre duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu şikayetçinin müstehcen fotoğraflarını, onun bilgisi dışında, bir sosyal paylaşım sitesine koyduğu iddiasına konu olayda, şikayetçinin beyanında geçen sosyal paylaşım sitesine onun adına üyelik işlemlerinin yapıldığı bilgisayarın internet servis sağlayıcısı ve internet servis sağlayıcısı tarafından verilen IP adresinin tespit edilmesi, tespit edilen IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin belirlenmesi, IP adresini kullanan abonenin sanıkla bağlantısı araştırılıp, gerektiğinde sanığın iş yerinde ve evinde kullandığı bilgisayarlar üzerinde bilişim uzmanı üç kişilik bilirkişi marifetiyle inceleme yapılarak, söz konusu üye

profilinin, sanığın kullanımında olan bilgisayar aracılığıyla oluşturulup oluşturulmadığı hususunun belirlenmesi; şikayetçinin 31.08.2009 tarihli şikayet dilekçesi de göz önüne alınarak, iddia olunan suç tarihinde şikayetçi ve sanığın abonesi olduğu telefon hatları araştırılıp, bu tarihten önceki ve sonraki altı aylık görüşme detaylarını gösterir HTS raporları istenilerek, toplanan tüm deliller birlikte değerlendirilerek, iddia ve savunmanın doğruluk derecesi açıklığa kavuşturulduktan sonra sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayalı olarak, sanığın beraatine karar verilmesi", Yar. 12. CD, E.2013/7154, K.2013/16476, 17.06.2013, (UYAP).

"10/10/2008 tarihli ve 03/11/2008 tarihli alınan bilirkişi raporlarına göre; olay tarihinde müştekinin hesabından internet yoluyla yapılan para havalesinin bir kısmının Taksim şubesindeki hesaptan çekilmesi sırasında alınan kamera kayıtlarının incelenmesinde; 2 kişinin bankamatikten para çektiğinin tespit edildiği, bu iki kişi ile sanıkların fotoğraflarının bilirkişice incelenmesinde aynı şahıslar olmadığının belirlendiği, ancak mahkemece sanıklar lehine olan bu delillerin kararın gerekçesine dayanak kabul edilerek çelişkiye neden olunduğu, 10.10.2008 tarihli bilirkişi raporunda, sanık Şükrü Ünal'ın bilgisayarına bağlı modem hattının kablosuz olması durumunda modemin markasına göre değişmekle beraber herhangi bir şahsın bilgisayarı ile 85.97.170.132 IP numarasından suç konusu paranın havale edilmiş olabileceği belirtildiğinden; sanık Ş. Ü'ın bilgisayarının, modemin ve dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiye tevdi edilerek adı geçen sanığın bilgisayarına bağlı modemin türünün tespit edilmesi, modem hattının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, sanığın internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, sanığın bilgisayarına virüs gönderilerek bilgilerinin alınıp alınmadığı konularında rapor düzenlettirilmesi gerekirken bu hususlar araştırılmadan eksik soruşturma ile hüküm kurulması" Yar. 13. CD, E.2012/6530, K.2013/16693, 30.05.2013, (UYAP).

"4-Suça konu havale işleminin yapıldığı IP nosunun Türk Telekom ve diğer internet servis sağlayıcılarından araştırılıp işlemin yapıldığı yer ve bilgisayarın tespiti cihetine gidilmesi, işlemi yapan bilgisayar ve telefon hattı sahibinin tespiti durumunda olay ile ilgili bilgi ve görgüsüne başvurulması, 5-Sanığa ait olan ve ayrıca suça konu işlemin yapıldığı tespit edilecek olan modemlerin, bilgisayar kasalarının ve yukarıda belirtilen hususlarıda içeren dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayarlar mühendisi bir bilirkişiye tevdi edilerek bilgisayarlara bağlı modem türlerinin tespit edilmesi, modem hatlarının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, bilgisayarlara virüs gönderilerek bilgilerinin alınıp alınmadığı suça konu işlemin ne şekilde nereden yapıldığı konularında rapor düzenlettirilmesi, sonucuna göre tüm deliller çervesinde sa-

III. EKRAN GÖRÜNTELERİ ÇIKTILARININ İSPAT DEĞERİ

A. Ekran Görüntü Çıktısı Kavramı

Ekran görüntüsü, görüntü sergileme aracı olan monitör/ekran vasıtasıyla bireylere ulaşan ışık demeti yansımasıdır. Ekrandaki bu görüntünün siber ortamda sayısal olarak anlık birebir nüshasının alınması işlemine ise "ekran görüntüsü almak/yakalamak" (=printscreen, screenshot) denmektedir. Başta bilgisayar olmak üzere bir çok elektronik cihaz (örneğin akıllı telefonlar) bir ekrana sahiptir. Bu ekrana yansıyan görüntü ve siber ortamdaki veri karşılığı aslında başlı başına bir çıktıdır (=output). Bu nedenle ekran görüntüsü çıktılarını ikiye ayırarak incelemek gerekir.[40]

Bunlardan ilki, ekran görüntüsü sayısal çıktılarıdır. Işık demeti yansımasıyla oluşan ve ekrana yansıyan anlık görüntülere "ekran görüntüsü dijital/sayısal çıktısı" adı verilmektedir. Herhangi bir işleme tabi tutulmayan bir bilgisayarda masaüstü görüntüsü bile aslında arka planda çalışan programlar nedeniyle ve hâlihazırda bir görüntüyü yansıttığı için "çıktı" sayılmaktadır. Ekran görüntüsü dijital/sayısal çıktıları geçici olduklarından ve o an itibariyle ekran görüntüsünün videoya kaydedilmesi veya ekran görüntüsünün ya-

nığın hukuksal durumunun değerlendirilmesi gerekirken, bu konularda kovuşturma genişletilmeden sanığın eksik kovuşturmayla cezalandırılmasına karar verilmesi" Yar. 13. CD, E.2012/1947, K.2013/18603, 06.06.2013, (UYAP).

"Sanığın, katılanın kredi kartı bilgilerini ele geçirerek internet üzerinden alışveriş yaptığının iddia olunması karşısında; gerçeğin kuşkuya yer bırakmayacak şekilde belirlenebilmesi bakımından, olaya konu kredi kartı kullanılarak yapılan siparişlerin verildiği bilgisayar veya bilgisayarlara ait IP numaraları üzerinden, siparişin verildiği adresin ve burada oturan kişinin araştırılması, alışveriş yapılan işyerlerinden siparişlerin kim ya da kimler tarafından yapıldığının, mal veya hizmetin kime ve nereye sağlandığının sorulması, alışverişe ilişkin faturaların işyerlerinden temin edilmesi sonrasında tüm deliller birlikte değerlendirilip sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken eksik incelemeyle yazılı şekilde karar verilmesi" Yar. 11. CD, E.2012/1017, K.2013/8345, 21.05.2013, (UYAP).

[40] Halid Özkan, "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği," iç. *Ceza Muhakemesi Hukukunda Delil ve İspat*, ed. Yener Ünver (Ankara: Seçkin Yayıncılık, 2014), 270-271.

kalaması yapılamadığı sürece tekrar edilebilir nitelikte değiller. Bu nedenle de ceza muhakemesinde ispat aracı olmak için zayıftırlar. Nitekim Amerikan Federal Mahkemesi de "web sitesi ekran görüntülerine" şüphe ile yaklaşılması gerektiğini söylemektedir.[41]

Bir diğer ekran görüntüsü çıktı türü ise "ekran görüntüsü fiziki/yazıcı çıktıları"dır. Bunlar, ekrandaki görüntünün yakalanması ve fotoğrafının çekilmesi sonrasında bir yazıcı yardımıyla görüntünün kağıt vb. materyal üzerine yazdırılmasıdır. Bazen bu çıktı bir web sitesinin o andaki görüntüsü olabilmektedir. Bir web tarayıcısı açıkken doğrudan fiziki çıktı alınması halinde URL linki ve çıktı tarihi, fiziki çıktı üzerinde yazmaktadır. Fakat bu bilgilerin fiziki çıktı üzerinde yer alması yeterli değildir; ek deliller ile URL linkinin ve URL linkine bağlı adreste bulunan görüntünün doğrulanması gerekmektedir.[42]

B. Ekran Görüntü Çıktısının İspat Değeri

Uygulamada, başta hakaret, tehdit, şantaj veya özel yaşamın ihlali suçları olmak üzere çok sayıda suç son yıllarda yoğun bir şekilde Facebook, Youtube, Twitter gibi sosyal paylaşım siteleri üzerinden veya WhatsApp, Messenger gibi mesajlaşma/konuşma uygulamaları veyahut elektronik postalar aracılığıyla işlenmekte,[43] suçun mağduru da şikayet dilekçesine genellikle buna dair (örneğin Facebooktaki hesabın ekran görüntüsünü içeren) bir çıktıyı eklemekte, bu çıktı esas alınarak hesap sahibi görünen kişi şüpheli olarak soruşturmaya dahil edilmekte, hakkında dava açılabilmektedir.[44]

---

41 Özkan, "Ekran Görüntüsü," 271.

42 Özkan, "Ekran Görüntüsü," 271.

43 Sosyal medya aracılığı ile işlenen bilişim suçları, örnek dava ve kararlar için, bkz. Çubukçu ve Atiker, "Sosyal Medya ve Bilişim Suçları," 3*ff*.

44 "… soruşturma aşamasında dosyaya sunulan facebook çıktısı örnekleri esas alınmak suretiyle, internet servis sağlayıcısı ve IP adresinin tespit edilip edilemeyeceği hususunda, bilişim alanında uzman bilirkişilerden rapor aldırılması ayrıca sözkonusu hesabın üzerindeki bilgilerden yola çıkarak açık kaynak araştırması yapılmak suretiyle ve sonucuna göre sanığın hukuki durumunun belirlenmesinin gerektiği" Yar. 4. CD, E. 2014/44927, K. 2019/2543, 20.02.2019, (UYAP).

Dijital deliller, parmak izi veya DNA delili gibi çoğu kez ilk bakışta fark edilemeyen, gizli ve görünmeyen bir yapıya sahiptir. Bu nedenle dijital delillerin bazı araçlar veya yöntemlerle somut, yani insanların duyu organlarıyla algılayabilecekleri, bir hale getirilmelerine ihtiyaç olacaktır. Donanım ve yazılımdan oluşan bu vasıtalar sayesinde elektronik ortamda yer alan bilgiler bilgisayar çıktısı ya da ekran çıktısı şeklinde beş duyu organımızla algılanabilecek niteliğe kavuşmakta ve muhakeme makamı tarafından temas edilebilir hale gelmektedir.[45] Ancak belirtmemiz gerekir ki, dijital delillerde delil niteliğinde olan ekrandan veya yazıcıdan alınabilen çıktı değil, bizzat dijital ortamdaki verinin kendisidir.[46]

Dijital verilerin kendilerine özgü özellikleri ve kolay zarar görebilen, değiştirilebilen ve yok edilebilen yapıları sebebiyle doğrulanmaları son derece önemlidir. Ancak *dijital delillerin doğrulanması*[47] konusu, dijital delillere ilişkin en tartışmalı konulardan birini oluşturmaktadır. Dijital delillerin doğrulanması, delillin iddia edilen "şey" olup olmadığını ispat etmektir. Dijital delillerin doğrulanamaması halinde delillin hukuka uygunluğu şüpheye düşebilecektir. Özellikle son yıllarda dijital delillere dayanarak sürdürülmekte olan birçok ceza yargılaması bulunmasına karşın hukukumuzda, diğer bazı hukuk sistemlerine kıyasla, dijital delillerin doğruluğunu tayin etmeye ilişkin geliştirilmiş bir kurallar bütünü bulunmamaktadır.[48]

Amerikan hukukunda genel olarak dijital deliller, özel olarak da ekran çıktılarının delil niteliğini haiz olduğunu söyleyebilmek için hem "*kabul edilebilir"* hem de "*doğrulanabilir"* olması aranmaktadır. Çünkü

---

[45] Gökşen, "Dijital Verilerin Delil Değeri," 57, 62; Uğur Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller" (yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2015), 38-39; Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı," *Türkiye Adalet Akademisi Dergisi*, no. 22 (Temmuz 2015): 520; Değirmenci, *Sayısal (Dijital) Delil*, 132; Özkan, "Ekran Görüntüsü," 268.

[46] Değirmenci, *Sayısal (Dijital) Delil*, 132; Sarsıkoğlu, "(E-Delil) Kavramı," 520.

[47] Dijital delillerin teknik olarak doğrulanması kavramı ve modelleri için, bkz. Yusuf Uzunay ve Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller," Akademik Bilişim Konferansları http://ab.org.tr/ab05/ tammetin/134.pdf.

[48] Gökşen, "Dijital Verilerin Delil Değeri," 93-94.

ekran görüntüsü çıktıları orjinalinden türetilen delil (türev) niteliğinde olup, mutlak şekilde doğrulanması ve kabul edilebilirliğinin ispatlanması gerekmektedir. Daha doğrusu delilin kabul edilebilir olması için doğrulanabilir olması, doğrulanabilirlik için de; 1) ekranda o an için aslında ne vardı? 2) ekran görüntüsünü doğrulayan doğrudan bir delil veya tanık ifadesi var mı? 3) ekran görüntüsü internet ortamında ise web site sahibi/ içerik, yer, servis veya erişim sağlayıcısı tarafından o andaki görüntü doğrulanıyor mu?, şeklinde kıstaslara ve duruma göre ek kıstaslara başvurulmaktadır. Diğer taraftan ekran görüntüsü sayısal veya fiziki değerlendirilmesi uzman kişilerce yapılmaktadır. Böylelikle dava daha jüri önüne gelmeden önce dijital delilin bilimselliği ve akılcılığı kısmen de olsa değerlendirilmiş olur. Şayet dava jüri önüne taşınırsa, ekran görüntüsü hakkında çalışmış olan taraf bilirkişi ya da mahkeme tarafından atanan bilirkişi mahkemede dinlenir, çapraz sorguya tabi tutulur.[49]

Öğretide *Gökşen'e* göre, dijital verilerin delil olarak değerlendirilmesi için içlerinde bulundukları dijital sistemin bütün olarak incelenmesi ve dijital delillerin değiştirilmesinin görece kolay olması sebebiyle mutlaka uzmanlar tarafından doğrulanması gerekmektedir. Dijital delillerin adli bilişim prosedürüne aykırı olarak incelenmesi ve bu belgelerin doğrulanamaması halinde hükme esas alınmaması gerekir.

Özkan ise, dijital verilerin sadece dijital ortamdaki şekillerinin orijinal delil kabul edilmesi ve ekran görüntüsü çıktıları doğrulanması mümkün olan "suret" olarak kabul edilmesi gerektiği görüşündedir. Yazara göre, en nihayetinde başka delillerle desteklenmediği müddetçe ekran görüntüsü çıktıları "delil başlangıcı/ dolaylı delil" kabul edilmelidir. Çünkü siber ortamdaki dijital delillerin bir yazıcı ile yazılı belge haline dönüştürülmesi, bu çıktıları doğrudan delil niteliğinde "belge" haline dönüştürmeyecektir. Ekran görüntüsü çıktıları manipülasyona açıktır ve %100 güvenilir değildir. Bu nedenle ekran görüntüsü dijital/ fiziki çıktıları, başka delillerle desteklenmediği ve dijital doğrulama yapılmadığı müddetçe, tek başına

[49] Özkan, "Ekran Görüntüsü," 273*ff*.

hükme esas alınmamalıdır. Bu çıktıların delil kabul edilebilmesi için hem doğrulanabilir hem de kabul edilebilir olması gerekir.[50]

*Sarsıkoğlu'*na göre ise dijital delillerin hukuka uygun olarak elde edildiği ve içeriklerinin de gerçeği yansıttığı dolayısıyla taklit ve tahrif edilmediği kesin olarak muhakeme makamları tarafından anlaşıldıktan sonra tek başına delil olarak kullanılmaları ve hükme esas alınmalarında bir sakınca bulunmamaktadır.[51]

Uygulamamızda ise, ekran görüntüsünün sayısal çıktısından ziyade fiziki çıktılarının sıklıkla soruşturma veya dava dosyasına dahil edildiğini görmekteyiz. Sunulan bu çıktılar üzerinden soruşturmaya yön verilmekte; ikrar, tanık ve olayın gelişimi gibi tüm delillerin değerlendirilmesi sonucunda ve diğer delillerle birlikte hükme esas alınabilmektedir.

Ekran görüntülerinin delil niteliği ve ispat değeri konusunda, konuyu açık bir şekilde tartışarak sonuca varan Yargıtay içtihadına rastlamadık. Bununla birlikte, örneğin Antalya 10. Asliye Ceza Mahkemesi, yargılamasını yaptığı bir davanın gerekçeli kararında, "Katılan son duruşmadan önce dosyaya sunduğu yazılı beyanları ve ekindeki facebook sayfasından çıkmakla bastırılmış bulunan fotoğraf, yakınan ve sanığın facebook sosyal paylaşım sitelerinde yer alan çıktılarla ilgili belgeler dosyada bulunmaktadır" diyerek *çıktıları* da deliller içerisinde saymış ve tehdit ile özel yaşamın ihlali suçundan sanığın mahkumiyetine karar vermiştir.[52] Bu kararın temyizi üzerine Yargıtay 12. Ceza Dairesi de "Dosya içeriği, sanığın ikrar içeren savunmaları, katılanın tutarlı beyanları, tanık anlatımları ve mesaj tespit tutanağına göre; ev arkadaşı ve aynı okulda öğrenci olan sanık ile mağdurun, aralarındaki anlaşmazlık nedeniyle evlerini ayırdıkları, olayın akabinde, sanığın, makyajsız hali ile uyurken çekilen fotoğrafının, mağdur tarafından internetteki facebook profil hesabında yayımlanarak, fotoğrafa olumsuz yorumlar yapılması üzerine sanığın, bu olayın meydana getirdiği haksız tahrik altında, mağdurun,

---

50 Özkan, "Ekran Görüntüsü," 272, 282.

51 Sarsıkoğlu, "(E-Delil) Kavramı," 520.

52 Antalya 10. Asliye Ceza Mahkemesi, E.2013/130, K.2013/575, 24.10.2013, (UYAP).

evde erkek arkadaşı ile öpüştüğü sırada çekilen özel fotoğrafını facebook profil hesabında yayımladığı ve mağdura, iki gün ara ile cep telefonuna mesajlar çekerek "ağzını yüzünü şişirecem, celladın olucam, anan kapıları iyi kilitlesin bu sefer kezzap yiyecek, mezarını hazırlat" gibi sözlerle tehdit ettiği, atılı suçların bu şekilde sübut bulduğu" şeklindeki içtihadıyla, ikrar, tanık anlatımı gibi diğer delillerle desteklenmiş *çıktıların* da esas alındığı yerel mahkeme hükmünü onamıştır.[53]

Yine bir başka olayda, Facebook hesabı üzerinden gerçekleştirilen hakaret ve tehdit suçlarından açılan davada, adına olan hesabın sahte olduğunu beyan ederek suçlamayı kabul etmeyen sanık savunması ile "facebook.com" adli hizmet sağlayıcı kuruluşun Türkiye temsilciliğinin bulunmaması ve Facebook'ta işlem yapan bilgisayarların IP adreslerini hizmet sağlayıcı kuruluş tarafından doğrulanmıyor olması gerekçeleri verilen beraat kararının istinaf edilmesi üzerine Gaziantep BAM 9. Ceza Dairesi, "yorum yapılan facebook sosyal paylaşım sitesinin sayfa çıktılarının dosya içerisinde mevcut olduğu ve paylaşım altında sanık adına olan hesap üzerinden yazılan hakaret ve tehdit içerikli yorumun bulunduğu, yorum içeriğinin hakaret ve sair bir kötülük yapacağına dair tehdit suçlarını oluşturacak nitelikte olduğu, sanığın kendisine ait tek bir hesabın olduğu ve yorum yapılan hesabın kendisine ait olmayıp adına sahte olarak açılmış bir hesap olduğunu ileri sürdüğü, ancak sanığın kendisine ait olmadığını ileri sürdüğü hesaptaki profil fotoğrafının yeğenine ait fotoğraf olduğunu kabul ettiği, yine bu hesap üzerinden yapılan bir paylaşımda görülmekte olan aracın da kendisine ait araç olduğunu ve bu paylaşımın altına yorum ekleyen kişilerin de kendi arkadaşları olduğunu, ancak kendisinin ne yeğeninin fotoğrafını ne de aracına ait fotoğraf paylaşımı yapmadığını ileri sürdüğü, sanığın bu paylaşımlarına ilişkin fotoğrafların özelinde kendisine ait ve sadece kendisinin paylaşıma atabileceği türden fotoğraflar olduğu, bu fotoğrafları kendisi dışında birilerinin haksız yere elde ederek adına açılan hesapta profil resmi olarak ya da paylaşım olarak kullanılmış olmasının hayatın olağan akışına uygun olmadığı, kaldı ki araç fo-

[53] Yar. 12. CD, E.2014/10722, K.2014/25542, 15.12.2014, (UYAP).

toğrafına ilişkin paylaşım altında sanığın arkadaşlarının yorumlarının bulunduğu, bir başkasının sırf suç teşkil edecek yorumlarda bulunmak üzere sanığın sosyal medya hesabını ele geçirmiş olduğu iddiasının da tek başına inandırıcı olmadığı, sanığın, sosyal medya hesabının birileri tarafından ele geçirildiğine ve kendisine ait bilgilerin bu hesap üzerinden izinsiz olarak paylaşıldığına yönelik bir başvuruda bulunduğunu da ileri sürmediği, bu hali ile sanığın bu hesabın kendisine ait olmadığına yönelik savunmasının soyut nitelikte ve kendisini suçtan kurtarmaya yönelik bir savunma olduğu ve itibar edilecek nitelikte bulunmadığı" gerekçesiyle sanığın cezalandırılmasına karar vermiştir.[54]

Ceza Dairelerinden farklı olarak Yargıtay Hukuk Dairelerinin, konuyu daha açık bir şekilde tartıştıklarına ve ekran görüntüsü çıktılarının ispat değerine ilişkin ölçütler geliştirdiklerini görmekteyiz. Nitekim Yargıtay 2. Hukuk Dairesi, davacı tarafından dosyaya sunulan elektronik ortamdan elde edilen resimler ve elektronik ortamda (sosyal paylaşım sitesi kullanılarak) yapılan görüşmelere ilişkin çıktılar esas alınmak suretiyle kocanın güven sarsıcı davranışlarda bulunduğu kabul edilerek boşanma kararı verilen bir davaya ilişkin "Elektronik ortamdaki fotoğraf, film, görüntü veya ses kaydı gibi veriler ve bunlara benzer bilgi taşıyıcılar, diğer delillerle desteklendikleri takdirde "delil" olarak hükme esas alınabilir. Bu veriler tek başına vakıaların ispatına yeterli değildir. Hükme esas alınan elektronik ortamdan elde edilen görüntülerdeki şahısların kocanın yakınları olduğu anlaşılmaktadır. "Facebook" isimli sosyal paylaşım sitesi kullanılarak kocanın, dayısıyla görüşmelerine ilişkin iletişim kayıtlarının da; davacının, sosyal paylaşım sitesinde kendisini "kocanın dayısı" yerine koymak suretiyle "dayısı ile koca" yazışıyormuş görüntüsü verilerek davacı tarafından oluşturulduğu, davacının da bunu kabul ettiği anlaşılmaktadır. Bu halde, sosyal paylaşım sitesi üzerinden yapılan görüşme kayıtları da vakıaların ispatında dikkate alınamaz (HMK md. 189/2)" şeklinde ekran görüntü çıktılarının hükme esas alınma ölçütünü ortaya koymuştur.[55]

---

[54] Gaziantep BAM, E.2017/2691, K.2018/2260, 22.11.2018, (UYAP).

[55] Yar. 2. HD, E.2013/19577, K.2014/19269, 05.02.2014, (UYAP).

Benzer şekilde ilk derece mahkemesi kararında dayanak yapılan; davacı nafaka yükümlüsü tarafından (Facebook ve WhatsApp'tan alındığı iddia olunan) görüntü kayıtlarından ibaret olan delilinin hukuken geçerli ve hükme esas alınabilecek bir delil niteliğinde olup olmadığına ilişkin olarak Yargıtay 3. Hukuk Dairesi de; Anayasa, CMK ve 6100 sayılı HMK'nın ilgili hükümlerine değinerek hukuka aykırı (yaratılmış veya elde edilmiş) delillerin hiçbir şekilde ispat aracı olarak kullanılmayacağını[56] belirttikten sonra "Somut olayda, toplanan delillerin birlikte değerlendirilmesinden; nafaka alacaklısı olan davalının, tanık olarak dinlenen şarkıcıya ait şarkının klip çekimi sebebiyle ... isimli oyuncu ile birlikte yer aldığı çekim görüntülerinin, (klibin yayınlanmasından vazgeçilmesi üzerine) davacı nafaka yükümlüsü tarafından hukuka aykırı olarak elde edildiği sabittir. Diğer taraftan, hukuka aykırı olarak elde edilen klip görüntülerinin, paylaşımlarının yapıldığı sosyal medya hesaplarının kendisine ait olduğu hususu da davalı tarafından kabul edilmediği gibi, davacı taraf sosyal medya hesaplarının (Facebook/ WhatsApp) ve bu hesaplardaki paylaşımlarında davalı tarafından yapıldığı hususunu da ispatlayamamıştır. Ayrıca, sosyal medya hesaplarında yapılan paylaşımların, ancak hesabın sahibi veya aynı paylaşım ortamında (Facebook/ WhatsApp) bulunan kişilerce delil olarak kullanımının mümkün olduğu düşünülebilecektir. Diğer bir anlatımla, sahte profil oluşturup paylaşımlarda bulunmak veya kişi profillerinde hesap sahibinin bilgisi, muvafakatı ve izni olmaksızın yapılan

[56] Yargıtay Hukuk Genel Kurulu 2012 tarihli içtihadında: "Bir delilin mahkemece kabul edilebilmesi için, gerek öğretide yer alan ağırlıklı görüş, gerekse de Hukuk Genel Kurulu Kararlarında ortaya konulan ölçüt; o delilin usulsüz olarak yaratılmamış olması ve hukuka aykırı biçimde elde edilmemesidir. Vurgulanmalıdır ki, bir delilin usulsüz olarak elde edilmesi ayrı, usulsüz olarak yaratılması ayrı bir olaydır. Usulsüz olarak elde edilen bir delil somut olayın özelliğine göre değerlendirilebilirse de; usulsüz olarak yaratılan bir delilin hiçbir şekilde delil olarak kabulü olanaklı değildir" Yar. HGK, E.2011/2-703, K.2012/70, 15.02.2012, (UYAP). Bu şekilde Yargıtay Hukuk Genel Kurulu, usulsüz yaratılan delilin hiçbir şekilde kullanılmayacağını, buna karşılık usulsüz elde edilen delilin bazı durumlarda kullanılabileceğini belirtmiştir. Bize göre, Anayasa m. 38/6 karşısında, böyle bir ayrıma gidilmeksizin hiçbir şekilde hükme esas alınmaması gerekir.

paylaşımların delil olarak sunulması halinde, bunların 6100 Sayılı HMK'nun 189/2. maddesi kapsamında hukuka aykırı delil kabul edilmesi gerekir. Hal böyle olunca, mahkemece; davacı nafaka yükümlüsü tarafından sunulan delillerin bir bölümünün hukuka aykırı olarak elde edilmiş olduğu, diğer delillerin ise hukuka aykırı bir şekilde yaratılmış olduğu gözetilerek, dosya kapsamındaki diğer delillerle de ispat edilemeyen nafakanın kaldırılması davasının reddine karar verilmesi gerekirken, yanılgılı değerlendirme ile davanın kabulüne karar verilmiş olması usul ve yasaya aykırıdır", demiştir.[57]

Bu açıklamalardan sonra sayısal veya fiziki çıktıların ispat bakımından değeri için şunları söyleyebiliriz: Öncelikle bu tür çıktılara ihtiyatla yaklaşmak gerekmektedir; zira çıktının kendisi üzerinde ekleme, çıkarma şeklinde tahrifat yapmak mümkün olduğu gibi çıktının alındığı örneğin (A) adına olan hesabın da sahte olma veya var olan bir hesabın başkası tarafından ele geçirilme ihtimali bulunmaktadır. Nitekim uygulamada bir başkası adına ve hatta bir yerden fotoğrafını bulup kullanarak sosyal paylaşım sitelerinde hesap (profil) açmak[58] veya başkasının hesabını ele geçirip bu hesap üzerinden suç işlemek[59] sıklıkla görülen yöntemlerdir. Diğer taraf-

[57] Yar. 3. HD, E.2016/14742, K.2017/2577, 7.3.2017, (UYAP).

[58] Örneğin, bkz. "…facebook oturumunu açık bırakmasından faydalanan sanık S.., tanık E.. habersiz, onun arkadaş listesinde yer alan katılan S.. sayfasına girip, katılana ait 20 adet fotoğrafı, kendi elektronik posta hesabına gönderdikten sonra, aynı sitede, katılan adına ve onun bilgisi dışında oluşturduğu sahte profile, ele geçirdiği katılana ait fotoğrafları koymak suretiyle verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlediği" Yar. 12. CD, E.2013/7765, K.2014/3758, 17.2.2014, (UYAP).

[59] Örneğin bkz. "…Oluşa, katılanın aşamalardaki anlatımlarına, sanığın da çalıştığı aile şirketine ait telefona bağlı internet hesabından katılana ait elektronik posta hesabına girildiğine ilişkin Microsoft şirketinden gelen yazı yanıtları ve kolluk araştırması sonuçlarına, katılanın 22.12.2010 tarihli dilekçesi ekinde ibraz ettiği fotoğraflara ve tüm dosya kapsamına göre; katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan … " Yar. 8. CD, E.2012/33557, K.2013/25987, 01.11.2013, (UYAP).

"Sanığın, katılanın Facebook hesabını kullandığı sırada, katılanın arkadaşı olan B. H. E.'in Facebook hesabını bir şekilde ele geçirerek katılana mesaj gönderdiğini, internet banka hesabı kullanıp kullanmadığını sorduğu, kullandığını öğrenince de kendisinden iade etmek şartıyla 450,00 TL para istediği, katılanın Akbank internet bankacılığı aracılığıyla sanığın vermiş olduğu … hattına 450,00 TL para gönderdiğini" Yar. 15. CD, E.2013/14846, K.2013/12178, 01.07.2013, (UYAP).

tan yine başkası adına (örneğin Facebooka kayıt edilerek değil de) bilgisayar program ve teknikleri kullanılarak yapay bir Facebook profili görüntüsü oluşturulabilir ve bilahare bunun çıktısı da sunulabilir. Dolayısıyla bu yönlü olası savunmaları/ itirazları göz önünde bulundurmak gerekmektedir. Bu nedenle sayısal veya fiziki çıktı savcılığa veya kolluğa sunulduğunda, ilk etapta bir tutanakla çıktı ile çıktının ait olduğu söylenen görüntünün aynı olup olmadığını belirlemeye yönelik tespit işlemi yapılmasının yararlı olacağını düşünüyoruz. Yine duruma göre hemen bilirkişiye de (adli bilişim uzmanına) başvurulabilir.[60] Bu aşamada hızlı hareket edilmesi önemlidir; zira, örneğin şikayetin dayanağını oluşturan profil her an kapatılabilir veya örneğin internet üzerinden yapılan dolandırıcılığa konu ilan kaldırılabilir veya site kapatılabilir. Bu tür bir tehlikeyi bertaraf etmek ve iddiasını güçlendirmek adına mağdur olan kişi, şikayette bulunmadan önce 1512 sayılı Noterlik Kanunu'nun 198/A maddesi uyarınca elektronik tespitte[61] bulunabileceği[62] gibi adli bilişim uzmanı yardımıyla[63] da ekran görüntüsünü alabilir.

---

60 Ekran görüntüsü yazıcı çıktılarının bilirkişiye incelettirilmesi ancak orijinal görüntünün siber ortamdaki versiyonun bilirkişiye tevdii ile gerçekleştirilebilir. Çünkü bir ekran görüntüsü yazıcı çıktısı üzerinden sahihliğin tespiti teknik olarak mümkün değildir. Ekran görüntüsünün yazıcı çıktısı olması durumunda, siber ortamda yer alan ekran görüntüsünün ile beraber saklanan verinin verisi olarak tanımlanan üst verileri görmek artık mümkün olmayacaktır. Bilirkişi ancak ekran görüntüsü sayısal çıktısını inceleyerek bir raporlama yapabilecektir. Ekran görüntüsü sayısal çıktısına ulaşılamadığı hallerde pek tabi yazıcı çıktısı üzerindeki delil başlangıcı olabilecek verilerin tespiti, bilirkişi tarafından yapılabilecektir. Örneğin yazıcı çıktısında URL linkinin bulunması veya sistem bilgilerinin bir pencerede açık unutulması sırasında ekran görüntüsünün alınmış olması gibi, bkz. Özkan, "Ekran Görüntüsü," 281.

61 Noterlik Kanunu'nun 198/A maddesinin ikinci fıkrasının üçüncü cümlesinde, noterlerin, Noterlik Kanunu'nun 61. maddesi çerçevesinde yapacağı işlem grupları arasında yer alan tespit işlemleri ile elektronik ortamdaki durum, görüntü, işlem veya benzeri her türlü verinin tespiti işlemlerinin, yine, elektronik ortamda da noterliklerce gerçekleştirilebileceğine açıkça işaret edilmiştir. Elektronik ortamda yapılabilecek işlemlerin gerçekleştirilmesi sırasında uyulacak olan usûl ve esasları belirlemek amacıyla, *"Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik"* (RG: 11.7.2015, S. 29413) çıkartılmıştır. Noterlerin, Noterlik Kanunu'nun 61. maddesi çerçevesinde yapacakları tespit işlemleri, ilke (olarak, fizikî ortamda gerçekleştirilir. Ancak, ilgilinin talep etmesi halinde sözü

Savcılıkça, sunulan çıktının türev olduğu dikkate alınarak ilgili web sitesi veya erişim sağlayıcısından görüntünün *doğrulanmasına* çalışılmalıdır. Çünkü dijital delil olan "çıktı"nın kendisi değil, dijital ortamdaki orijinal halidir.[64] Dijital delillerin kendine has yapıları

edilen işlem grubunun da elektronik ortamda, noterliklerce gerçekleştirilmeleri mümkündür (Yön. m. 5, V; m. 2). Burada özellik arz eden husus, elektronik ortamdaki durum, görüntü veya benzeri verilerin, tespitidir. Yönetmeliğin 6. maddesinde, elektronik ortamdaki bir verinin, tespiti işleminin nasıl gerçekleştirileceğine ilişkin olarak özel bazı belirlemelerde bulunulmuştur. Her şeyden önce, burada sözü edilen, elektronik ortamdaki bir verinin tespiti işleminden, bir donanımdaki veya internet ortamındaki verinin, tespiti işlemi ile o verinin belirli bir anda ya da zaman aralığında, o anki veya zaman aralığındaki halinin değişmez olarak belirlenmesi, tekrar edilebilir bir halde tutulması ve saklanması anlaşılır. Tespit edilecek veri, bir donanımda ise tespit, malikin ya da zilyetin rızasıyla, noterlikte veya mahallinde yapılabilir. Tespit edilecek veri, internet ortamındaysa, tespit işlemi, ancak, bu durumda, Türkiye Noterler Birliği Bilişim Sistemi kullanılmak suretiyle gerçekleştirilebilir (Yön. m. 5, VI/a,b,c). Bu konuda ayrıntılı bilgi için, bkz. Süha Tanrıver, "Noterler Tarafından Elektronik Ortamda Yapılabilecek Olan İşlemler Ve Bu İşlemlerin Gerçekleştirilmesi Usûlü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 65, no. 4 (2016): 3677*ff*.

62 Türkiye Noterler Birliği Başkanı Yunus Tutar: "Artık sosyal medyada veya internet sitelerinde gördüğünüz ya da okuduğunuz bir yayını, haberi kayıt altına aldırabileceksiniz. Bu yenilikle TNB portala girerek tespit edilmesini istediğiniz yeri online belirleyebileceksiniz. Sistem arka planda her adımı kaydediyor, hangi sayfayı açtınız, nereyi tıkladınız gibi tüm bilgiler kaydediliyor. Bu veriler ve iz kayıtları özet bilgileri alınarak zaman damgası ile damgalandıktan sonra değiştirilemez bir şekilde TNB Bilgi Sistemleri'ne kaydediliyor ve size bir başvuru numarası veriliyor. Ertesi gün size verilen başvuru numarasıyla ya da TNB web sayfasındaki e-başvuru bölümünden istediğiniz noteri seçip başvuru yaparak noterden tespit tutanağınızı alıyorsunuz." "Elektronik Ortamda Tespit," Profelis, erişim tarihi Şubat 02, 2019, https://www.profelis.com.tr/tr/hakkimizda/basari-oykuleri/e-tespit/.

63 Adli bilişim uzmanı tarafından adli bilişim standartlarına uygun olarak (örneğin zaman damgası, dosyaların hash değeri, işleme ilişkin video kaydı gibi teknik bilgiler içeren) ekran görüntüsü alınmış olmasının, ileride manipülasyon olup olmadığına dair ortaya çıkabilecek tereddütleri gidermek bakımından yararlı olacağı kuşkusuzdur.

64 Değirmenci, *Sayısal (Dijital) Delil*, 132. Diğer taraftan dijital ortamdaki veriler, çıktılara yansımayan unsurları da içerebilirler. Bu konuda *Gökşen'in* Örneğin bir e-posta metni ekranda görüntülenebildiği gibi bir yazıcı vasıtasıyla da bu metnin basılmış hali edinilebilir. Ancak yazı aracılığıyla basılmış bir e-posta metni dijital belgenin kim tarafından, ne şekilde yazıldığına ilişkin sağlıklı bilgi ver-

nedeniyle ortaya çıkan doğru (sahih) olması ve doğruluğunun sağlanması[65] meselesi, inceleme konumuz bakımından daha önem arz etmektedir. Ülkemizde yayın yapan ve kayıtlı olan internet sitelerinin sahibi olan firmalardan, içerik ve yer sağlayıcı firmalardan her türlü bilgi ve belge talebinde bulunulabilir. Örneğin dolandırıcılık şikâyetine konu "sahibinden.com" isimli platform üzerinden yapılan bir ilana ilişkin fiziki çıktı sunulmuşsa, zikredilen platformla yazışma yapılarak (üye bilgileri, IP gibi bilgilerin temini yanı sıra) ilan görüntüsünün doğrulama işlemi yapılmalıdır. Ancak muhatap yurt dışı merkezli (Youtube, Facebook, Twitter, WhatsApp gibi) ise uluslararası istinabe kuralları gereğince yazışma gerekmekte olup, bu yola başvurulduğunda da çoğu zaman sonuç alınamamaktadır.[66]

Belirtelim ki, fiziki çıktıların manipülasyona açık yönlerine rağmen dosyaya sunulduğunda, hukuka aykırı olmamak kaydıyla her şeyin delil kabul edildiği vicdani delil sistemi içerisinde elbette ki delil olarak kabul edilecektir.[67] Bunun için hukuka uygun şekilde elde edilmesi gerektiği izahtan varestedir. Zira ceza muhakemesinde bir ispat aracının delil olarak kullanılabilmesi için bazı özelliklere

meyebilir. Bu takdirde söz konusu e-posta metninin bulunduğu bilgisayar içinde incelenmesi halinde bu belgeyi destekleyen farklı verilere de ulaşılabilecektir. Çıktısı alınmış bir e-postada bu metnin kimin e-posta adresinden, kime, hangi tarihte ve hangi saatte yazıldığında genellikle ulaşılabilmektedir. Ancak bu bilgilerin doğruluğu yine de sorgulanmalıdır. Zira e-postanın çıktısından bulunan bilgiler epostanın ait olduğu zannedilen kişi dışında kişilerce de yazılmış olabilir, bkz. Gökşen, "Dijital Verilerin Delil Değeri," 58.

65 Dijital delillerin sahihliği ve doğrulanabilir olması konusunda ayrıntılı bilgi için, bkz. Özkan, "Ekran Görüntüsü," 289*ff.*; Gökşen, "Dijital Verilerin Delil Değeri," 93*ff.*; Uzunay ve Koçak, "Bilişim Suçları Kapsamında," 3*ff.*

66 Sosyal medya üzerinden işlenen suçlarda uluslararası istinabe konusunda, bkz. Özocak, "Sosyal Medyada İşlenen."

67 Ceza muhakemesi maddi gerçeği ortaya çıkarmayı amaçladığından vicdani delil sistemini benimsemiş olup bununla ifade edilmek istenen, hem delil serbestisi hem de delillerin serbestçe değerlendirilmesidir. Delil serbestisi, hukuka uygun olmak kaydıyla ceza yargılamasında her şeyin delil olabileceği esasına dayanmaktadır. Bu konuda ayrıntılı bilgi için, bkz. Doğan Gedik, *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması* (Ankara: Adalet Yayınevi, 2016), 42*ff.*

sahip olması gerekir. Bir delilde bulunması gereken en önemli özelliklerden biri de onun hukuka uygun olmasıdır.[68] Anayasamızın 38/6. maddesi hükmü ile 5271 sayılı CMK'nın 206/2-a, 217/2 ve 289/1-i maddelerindeki düzenlemeler gereğince hukuka aykırı şekilde elde edilen deliller hükme esas alınamaz. Bu bilgiler ışığında, örneğin soruşturma dosyasına sunulan çıktının ilişkin olduğu Facebook hesabı başkasına ait olup da şifresi kırılarak girilmiş veya sahte oluşturulmuş bir hesap ise, söz konusu olan hukuka aykırı delil elde etme yöntemidir ve dolayısıyla fiziki çıktıların delil olarak değerlendirilmesi mümkün değildir. Sonuç olarak bize göre, hukuka aykırı elde edildiğine dair bir belirleme yoksa ve olayla ilgili ise üzerinde durulması gereken konu; fiziki çıktıların delil olarak kabul edilip edilmemesinden ziyade, her şeyin delil olarak kabul edildiği ve hâkimin de bunları değerlendirmekte serbest olduğu vicdanı delil sisteminde, bu çıktıların ispat gücünün ne olduğudur. Bu noktada biz de, çıktıları "belirti"/ "dolaylı delil"[69] niteliğinde kabul et-

---

[68] Genel olarak bir delilde bulunması gereken özellikleri için, bkz. Gedik, *Ceza Muhakemesinde İspat*, 45*ff*.; dijital delillerde bulunması gereken özellikler için, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 114*ff*., 132*ff*.; Özkan, "Ekran Görüntüsü," 267*ff*.; Gökşen, "Dijital Verilerin Delil Değeri," 58*ff*.; Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller," 37*ff*.

[69] Öğretide, delillerin çeşitli tasniflere tabi tutularak incelendiği görülmekle birlikte, yaygın olarak "beyan", "belge" ve "belirti" şeklinde bir ayrıma tutulduğunu görmekteyiz. Yine öğretide bu delillerin, *somut olaya münhasır deliller* ve *genel mahiyette temsili deliller şeklinde* tasnifi de yapılmaktadır. Bunlardan beyan ve belge şeklindeki deliller, örneğin olayı gören tanığın beyanında olduğu gibi geçmişte kalan olayı doğrudan doğruya ispat edebilme niteliğine sahip olduğundan *somut olaya münhasır deliller*; buna karşılık belirtiler, maktulün gömleğinde bir başkasına ait saç teli bulunması örneğinde olduğu üzere somut olayın da dahil olduğu geniş bir gerçekliğin ispatına yaradığı için genel mahiyette temsili delil olarak kabul edilmektedir. Bu bağlamda ispat edilecek olayın dolaylı olarak ispatına yardımcı olan vakıalara ve izlere *belirti* denmektedir. Belirti, ispat edilmeye muhtaç olaydan geriye kalan her türlü iz ve eserlerdir. Vicdani delil sisteminde, hukuka uygun ve olayı temsil etme, akla vs. uygun olma gibi diğer özellikleri taşımak kaydıyla belirti de bir ispat aracıdır ve diğer deliller gibi hâkim tarafından değerlendirmeye tabi tutulacağı kuşkusuzdur. Ancak olayı doğrudan doğruya ispat etmediklerinden, tek başına her zaman yeterli olmayabilir, başka delillerle desteklenmesi çoğunlukla gerekebilir. Belirtinin önemli bir işlevi de, somut olaya münhasır delillerin değerlendirmesinde kendini göstermesidir.

mek;[70] ikrar, tanık beyanı veya dijital doğrulama gibi destekleyici başka delil bulunmadığı sürece soyut olarak tek başına hükme esas almamak gerektiği düşüncesindeyiz.

IV. SONUÇ

Bilişim teknolojilerindeki baş döndürücü gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmekte; bu da yeni tartışmalara ve çözüm arayışlarına neden olmaktadır. Biz bu çalışmada; bilişim suçlarında uygulaması oldukça çok olan IP adresi (numarası) tespiti ile ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değerini inceleme gayretinde olduk.

Ulaştığımız sonuçları şu şekilde toparlayabiliriz: Bilişim suçlarında soruşturmanın yönlendirilmesi ve nihayetinde faile ulaşılması bakımından IP numarasının tespiti oldukça önemlidir. Ancak hem IP numarasının tespiti hem de bundan yola çıkarak failin tespiti, suçun sanal ortamda işlenmesinden kaynaklı kendine özgü zorlukları ihtiva etmekte ve adli makamları daha ihtiyatlı olmaya zorlamaktadır. Bu bağlamda öncelikle soruşturma konusu fiilin ilişkilendirildiği IP tespitinin doğru şekilde yapılması gerekmektedir. Yanlış bildirilen bir IP numarası, soruşturmanın seyrini değiştirebildiği gibi olayla ilgisi olmayan kişi/kişilerin şüpheli veya sanık olmasını da sonuçlayabilmektedir. Bu nedenle IP numarasının tespiti kadar, IP numarasının tahsis edildiği internet abonesinin belirlenmesi aşamasında da dikkatli olunmalıdır.

Hâkim, maddi sorunu çözerken doğrudan deliller gibi belirtilerden de yararlanarak bir sonuca ulaşacaktır. Belirtiler ve ispat güçleri hakkında, bkz. Gedik, *Ceza Muhakemesinde İspat*, 93*ff*.

[70] Öğretide *Kaynakçıoğlu'na* göre de dijital delilleri, belirti delilleri içerisinde sınıflandırmak gerekir. Dijital delil içeren elektronik aygıtların da bir kan ya da DNA örneği gibi gerek elde edilmesi gerekse incelenmesi sırasında uzmanlık gerekmektedir. Dijital deliller yapısal özellikleri nedeniyle kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilirler. Bu nedenle dijital delillerin uzmanlarca incelenmeden delil olarak kabulü son derece tehlikelidir. Bkz. Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller," 46.

IP numarasının tespiti, ilişkin olduğu soruşturma bakımından sonuç değil, başlangıç noktası olabileceğini unutmamak gerekir. IP adresi kullananına işaret ediyor gibi görünse de teknik açıdan çoğu zaman doğrudan bir bilgisayarı veya bir kişiyi göstermekten ziyade, yalnızca bir internet aboneliğini gösterebilir. Bu nedenle IP adresinin tespiti, adres sahibinin suçun faili olduğunu doğrudan göstermez. IP numarası kullanılarak tespit edilen adreste sadece internet abonesi yaşasa dahi o kişi ikrarda bulunmadıkça veya diğer delillerle desteklenmedikçe, sadece IP numarası esas alınarak o kişi hakkında mahkumiyet hükmü verilmesi doğru değildir. Dolayısıyla IP adresi, tek başına mahkumiyeti gerektiren bir delil niteliği taşımayacak**,** ancak ikrar veya başkaca destekleyici deliller de varsa kişiler mahkum edilebilecektir. Yargıtay'ın da yaklaşımı bu yöndedir.

Uygulamada, başta hakaret, tehdit, şantaj veya özel yaşamın ihlali suçları olmak üzere çok sayıda suç son yıllarda yoğunlukla Facebook, Youtube, Twitter gibi sosyal paylaşım siteleri üzerinden veya WhatsApp, Messenger gibi mesajlaşma/konuşma uygulamaları veyahut elektronik postalar aracılığıyla işlenmekte, suçun mağduru da şikayet dilekçesine genellikle buna dair (örneğin Facebooktaki hesabın ekran görüntüsünü içeren) bir çıktıyı eklemekte, sunulan bu çıktılar üzerinden soruşturmaya yön verilmekte; ikrar, tanık ve olayın gelişimi gibi tüm delillerin değerlendirilmesi sonucunda ve diğer delillerle birlikte hükme esas alınabilmektedir. Gerçekten de fiziki çıktıların manipülasyona açık yönlerine rağmen dosyaya sunulduğunda, hukuka aykırı olmamak kaydıyla her şeyin delil kabul edildiği vicdani delil sistemi içerisinde elbette ki delil olarak kabul edilecektir. Hukuka aykırı elde edildiğine dair bir belirleme yoksa üzerinde durulması gereken konu; fiziki çıktıların delil olarak kabul edilip edilmemesinden ziyade, her şeyin delil olarak kabul edildiği ve hâkimin de bunları değerlendirmekte serbest olduğu vicdanı delil sisteminde, bu çıktıların ispat gücünün ne olduğudur. Bu noktada biz de, çıktıları "belirti"/ "dolaylı delil" niteliğinde kabul etmek, başka delillerle desteklenmediği ve dijital doğrulama yapılmadığı müddetçe, soyut olarak tek başına hükme esas almamak gerektiği düşüncesindeyiz.

KAYNAKÇA

Balı, Yunus. "IP Numarası Tespiti." Dijitaldeliller. Erişim tarihi Aralık 1, 2018. http://www.dijitaldeliller.com/ip_tespiti.html.

Cebecioğlu, Gülçin ve İpek Beyza Altıparmak**.** "Dijital Şiddet: Sosyal Paylaşım Ağları Üzerine Bir Araştırma." *Sakarya University Journal of Education* 7, no. 2 (Ağustos 2017): 423-431.

CHIP Online. "IP Adresim Nedir." Erişim tarihi Mayıs 25, 2019. https://www.chip.com.tr/ip-adresim-nedir.

Çubukçu, Ceren ve Berrin Atiker. "Sosyal Medya ve Bilişim Suçları." Academia. Erişim tarihi Mayıs 5, 2019. https://www.academia.edu/31785425/Sosyal_Medya_ve_Bilişim_Suçları.

Değirmenci, Olgun. *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayıncılık, 2014.

Doğan**,** Koray. *Kuşkudan Sanık Yararlanır İlkesi*. Ankara: Seçkin Yayıncılık, 2016.

Durnagöl, Yasemin. "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar." *Türkiye Adalet Akademisi Dergisi* 2, no. 4 (2011): 375 – 416.

Dülger, Murat Volkan ve Gözde Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku (Uygulama Rehberi)*. Ankara: Türk Ceza Adalet Sisteminin Etkinleştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, 2014.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık, 2014.

Erdoğan, Burcu. "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?." *digiSophia*. Erişim tarihi Ekim 1, 2018. http://www.digisophia.com/Article/Details/61.

Gedik, Doğan. *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması*. Ankara: Adalet Yayınevi, 2016.

Gökşen, Elif. "Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri." Yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2014.

Gülseren, Fehmi Şener. "İnternet Ortamında İşlenen Hakaret Suçları." *LAÜ Sosyal Bilimler Dergisi* 4, no. 1 (Nisan 2013): 15-33.

Kaya, Mehmet Bedii. "İnternet Hukuku, Mevzuat & İçtihat." Mehmet Bedii Kaya. Erişim tarihi Mayıs 25, 2019. https://www.mbkaya.com/hukuk/internetmevzuat.pdf.

Kaynakçıoğlu, Uğur. "Ceza Muhakemesinde Dijital Deliller." Yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2015.

Özçelik, Gülsel Öykü. "IP Adresleri Tek Başına Delil Olabilir Mi? IP Adreslerine Yargılamada Ne Kadar Güvenilir?." TAG Hukuk Bürosu. Erişim tarihi Ekim 1, 2018. taghukuk.com/wp-content/uploads/2018/04/ip_adreslerinin_delil_niteliği.pdf.

Özkan, Halid. "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği." İç. *Ceza Muhakemesi Hukukunda Delil ve İspat*, editör Yener Ünver, 265-288. Ankara: Seçkin Yayıncılık, 2014.

Özocak, Gürkan. "Sosyal Medyada İşlenen Suç Tipleri Ve Suçluların Tespiti." Özocak Hukuk & Danışmanlık. Erişim tarihi Mart 11, 2019. http://www.ozocak.com/Dosyalar/a104b3.pdf.

Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı." *Türkiye Adalet Akademisi Dergisi*, no. 22 (Temmuz 2015): 507-534.

Süha Tanrıver, "Noterler Tarafından Elektronik Ortamda Yapılabilecek Olan İşlemler Ve Bu İşlemlerin Gerçekleştirilmesi Usûlü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 65, no. 4 (2016): 3677*ff*.

Şıracı, Sertel. "İnternet Kanununa Göre Log Tutma." Av. Sertel Şıracı. Erişim tarihi Şubat 02, 2019. https://www.sertels.av.tr/avukat/ hukuk/bilisim-hukuku/internet-kanununa-gore-log-tutma.html.

Taşçı, Ufuk ve Ali Can. "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014." *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2015): 229-248.

Uzunay, Yusuf ve Mustafa Koçak. "Bilişim Suçları Kapsamında Dijital Deliller." Akademik Bilişim Konferansları. http://ab.org.tr/ab05/tammetin/134.pdf.

Yegen, Ceren. "Demokratik Ve Yeni Bir Kamusal Alan Olarak Sosyal Medya." *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (Aralık 2013): 119-135.

Yetim, Servet. "Bilişim Suçları ve Etkin Mücadele Yöntemleri." *Terazi Hukuk Dergisi* 9, no. 95 (Temmuz 2014): 80-86.

MARKANIN ALAN ADI OLARAK KULLANILMASI: TÜRKİYE, ABD VE AVUSTRALYA ÖRNEKLERİ

Trademark as Domain Names: The Examples of USA, Australia, and Turkey

Merve Ayşegül KULULAR İBRAHİM*

Öz

İngilizce *'domain name'* olarak ifade edilen alan adları, kişi ve eşya isimlerinden farklı özellikler taşır ve farklı düzenlemelere tabidir. İnternetin gelişimi ile web sitelerinin kullanımı için gerekli olan alan adları; bir kimsenin adı ve/veya soyadından, işletme adından veya ticaret unvanından oluşabilir. Alan adları kişi adlarından farklı düzenlemelere tabidir. Ancak alan adlarının da kişi isimleri, işletme isimleri ve ticaret unvanları gibi 4721 sayılı Türk Medeni Kanunu'ndaki adın korunması düzenlemeleri kapsamında değerlendirilmesi gerektiği yönünde tartışmalar devam etmektedir. Bu çalışmada öncelikle alan adı tanımlanacak; yapısı, tahsisi ve önemi belirtilecektir. Ardından *cybersquatting* kavramının ne olduğu açıklanacak ve sonrasında gerek uyuşmazlık çözüm hizmeti sağlayıcıları gerekse Amerika, Avustralya ve Türk hukuklarındaki düzenlemeler ele alınarak başkasına ait ticari markanın internet alan adı olarak kullanılması sorununun nasıl çözümlendiği analiz edilecektir.

Anahtar Kelimeler: İnternet Alan Adı, Marka Hukuku, İnternet Hukuku, Bilişim, Ticari Marka.

---

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Ticaret Hukuku Anabilim Dalı Araştırma Görevlisi, aysegul.kulular@asbu.edu.tr, ORCID: 0000-0001-6556-0269
Makale Gönderim Tarihi: 19.03.2019
Makale Kabul Tarihi: 12.07.2019

Abstract

Domain names that gain importance with the development of the internet; may consist of the name or surname of a person, business name or trade name. Domain names and personal names are subject to different legislations. Even though, it is discussed that domain names should be assessed within the scope of protection regulations for the personal name under the Civil Code. This study will define domain name first. Secondly, it will explain the structure and significance of domain name and what cybersquatting is. Then, it will question dispute resolution service providers and American, Australian and Turkish regulations. Lastly, the issue of using someone else's trademark as an internet domain name will be analyzed.

Keywords: Domain Names, Trademark Law, Cybersquatting, Trade Name, Internet Law.

I. GİRİŞ

Türkçe'de alan adı olarak kullanılmakta olan İngilizce *'domain name'* olarak ifade edilen internetin gelişimi ile web sitelerinin kullanımı için gerekli olan alan adları; bir kimsenin adı ve/veya soyadından, işletme adından veya ticaret unvanından oluşabilir. Kişilerin isimleri üzerindeki hakları mutlak hak olarak herkese karşı ileri sürülebilen kişiye sıkı sıkıya bağlı hak niteliğinde olduğundan vazgeçilemez, devir ve temlik edilemez ve mirasa konu olamamaktadır. Alan adları kişiye sıkı sıkıya bağlı haklardan değildir. Alan adlarının satış, devir ve feragat gibi hukuki işlemlere konu olabileceği, İnternet Alan Adları Tebliği 22nci maddesinde düzenlenmiştir. Bundan başka alan adlarının da kişi isimleri, işletme isimleri ve ticaret unvanları gibi Türk Medeni Kanunu'ndaki adın korunması düzenlemeleri kapsamında değerlendirilmesi gerektiği yönünde görüşler de mevcuttur.[1]

Genellikle marka bazlı olan alan adları, her bir internet sitesine özgü olduğundan yani her bir alan adının tek ve özgün olmasından kaynaklı yüksek bir ekonomik değer söz konusudur.[2] Elektronik ticaretin de gelişimiyle birlikte menşeinden çok daha uzak yerlere pazarlanabilme imkânını haiz hale gelen ve tüketici tercihlerini oldukça etkileyen markaların[3] alan adı olarak kullanılmaları marka sahipleri haricinde başkalarınca gerçekleşmeye başlamıştır. Özellikle 90lı yıllarda '.com' başta olmak üzere '.net' ve '.org' alan adlarıyla ticari markaların *cybersquatter* kişilerce kaydedilmesinin oluşturduğu endişe alan adlarına yönelik bir politika belirlenmesini gerektirmiştir[4]. Bunun üzerine gerek The Internet Corporation for Assigned Names and Numbers kısa adıyla ICANN'ın alan adı ve ticari marka

---

1 Tamer Soysal, *İnternet Alan Adları Hukuku (Domain Name Law)* (Ankara: Adalet Yayınevi, 2014), 332 -334.

2 Ayça Zorluoğlu, "Alan Adlarında Kötü Niyet Kavramı," *Hacettepe Hukuk Fakültesi Dergisi* 2, no. 1 (2012): 68.

3 Osman Şanal, *Markanın Hükümsüzlüğü* (Ankara: Adalet Yayınevi, 2004), 5.

4 Jackueline D. Lipton, "Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy," *Wake Forest Law Review* 40, no. 4 (2005): 1424.

sahiplerinin, bireylerin bir alan adı kullanma hakkına itiraz edebileceklerine yönelik politikasını düzenlemesi[5] gerekse ticari markaların birden fazla kez kullanılmasının engellenmesine yönelik hukuki koruma sağlanması[6] gibi önemli çalışmalar hız kazanmıştır.

Bu çalışmada alan adının tanımı, yapısı, tahsisi ve önemi ile *cybersquatting* kavramının ne olduğu açıklandıktan sonra gerek uyuşmazlık çözüm hizmeti sağlayıcıları gerekse Amerika, Avustralya ve Türk hukuklarındaki düzenlemeler ele alınarak başkasına ait ticari markanın internet alan adı olarak kullanılması sorununun nasıl çözümlendiği analiz edilecektir.

II. ALAN ADI

İnternet alan adı, 5809 sayılı Elektronik Haberleşme Kanunu 3üncü maddesinde

' v) İnternet alan adı: İnternet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol numarasını tanımlayan adları,'

ifade edecek şekilde tanımlanmıştır. Bu nitelikte tanımlanmış olan alan adları ayrıca üst alan adı, ikinci seviye alan adı ve üçüncü seviye alan adı olacak şekilde birbirinden '.(nokta)' ile ayrılacak şekilde üç tür alt birimden oluşmaktadır. Alan adları Türkçe'si İnternet Tahsisli Adlar ve Sayılar Kurumu şeklinde tercüme edilen The Internet Corporation for Assigned Names and Numbers (ICANN) tarafından koordine edilmektedir.

---

5 Stacey H. King, "The "Law That It Deems Applicable": ICANN, Dispute Resolution, and the Problem of Cybersquatting," *Hastings Communications and Entertainment Law Journal* 22, no. 3 & 4 (1999 - 2000): 456.

6 Mark D Janis ve Peter K Yu, "International and Comparative Aspects of Trademark Dilution," *Transnational Law & Contemporary Problems* 17, no. 3 (2008): 603.

A. Alan Adı Tahsisi

Alan adları ülkelere, yapılan işlem türüne, kullanım amacına ve benzeri işlevlere göre kodlanmış olmakla birlikte alan adı hangi ülkeye bağlı olursa olsun ister özel ister kamu sektörü ister uluslararası bir kuruluş olsun, kar amacı gütsün gütmesin, ister ticaret amacıyla kullanılsın ister reklamcılık amacıyla ister bireyin kişisel amaçla kullanımında olsun fark etmeksizin tüm dünyadaki internet alan adlarının bağlı olduğu yalnızca bir genel merkez bulunmakta ve Amerika temelli bu merkez en genel tabiriyle tüm dünyadaki internet alan adlarını koordine etmektedir. İngiltere tarafından benzer bir kuruluş kurulmak istenmiş olmasına rağmen başvurular reddedilmiş ve işlemlerin Amerika merkezli bu örgüt tekelinde yürütülmesi sağlanmıştır.[7] Her ne kadar bu şekilde tek merkezli bir yönetim sakıncalı olduğu dolayısıyla eleştirilmekte ise de alan adı tahsisleri göz önüne alındığında tek merkezden yönetimin karmaşa yaşanmamasının sağlanması adına doğru olduğunu düşünenler de bulunmaktadır.[8] Her ne kadar alan adlarını ICANN tek merkezden koordine etse de, alan adı tescilini ticari alt kurumlar gerçekleştirmektedir. Ancak her ticari kurumun alan adı tescili yapması mümkün değildir. Zira alan adı tescil işlemi gerçekleştirecek ticari kurumların da ICANN tarafından yetkilendirilmiş olmaları gereklidir. ICANN, internetin DNS ve IP adres sistemlerini denetlemek ve koordine etmekle görevlendirilen kâr amacı gütmeyen bir kuruluştur. ICANN dolayısı ile bilgisayarlar ve kullanıcılar online olarak bilgi alışverişinde bulunabilmektedirler. Aslında 1988 yılında internetin düzenli olarak işleyişini sağlamak ve kamu yararını artırmak amacıyla kurulmuş olan ICANN öncesinde tüm bu işlemlerin doğrudan Amerikan hükümetinin kontrolünde olduğu düşünüldüğünde,[9]

---

7 Hörnle, Julia. Cyberspace Law. LLM. London: Queen Mary University of London, 2014.

8 Sevilay Uzunallı, *Markanın Korunmasının Kapsamı ve Tazminat Talebi* (Ankara: Adalet Yayınevi, 2012), 299.

9 Wei-erh Chen, "Optimizing Online Trademark Protections Given the Proliferation of Generic Top Level Domains," *The Journal of Corporation Law* 38, no. 3 (2013): 590.

bahsedilen İngiltere başvurusunun reddedilmesinin ve alan adlarının ICANN tekelinde olmasının Amerika'nın pek tabii bir refleksi olduğu söylenebilir.

Türkiye'ye ait alan adları 'tr' ifadesiyle belirtilmektedir. Bu şekilde 'tr' uzantısını haiz alan adlarının yönetimini 1993 tarihi itibarıyla ODTÜ üstlenmiştir. Bu tarih, TÜBİTAK-ODTÜ ve TR-NET'in DPT projesi çerçevesinde Türkiye'nin internete ilk kez bağlandığı tarihtir.[10] ODTÜ Alan Adı İdaresi başlangıçta, 'önce başvuran alır' ilkesine dayalı değil, belgeye dayalı tescil sistemini benimsemiştir. Bu durum her ne kadar marka ihlallerinin önlenmesini sağlamakla birlikte, diğer taraftan prosedürle uğraşmak istemeyen birçok tüzel ve gerçek kişinin yurt dışı alan adı tescilini tercih etmesine neden olmuştur. Bu şekilde döviz kaybının engellenmesi için diğer ülkelerde kullanılmakta olan 'ilk gelen alır' ilkesine dayalı tescil sistemi Türkiye'de de benimsenmiştir[11].

"İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir."

şeklindeki 2008 yılı 5809 sayılı Elektronik Haberleşme Kanunu 35inci maddesine göre ise internet alan adı tahsis edecek kurumların belirlenmesi ve internet alan adı tahsisinde ilgili esasların belirlenmesi yetkileri Ulaştırma Bakanlığı'na verilmiştir. Bunun üzerine konuyla ilgili esaslar, 2010 yılında Resmi Gazete'de yayımlanan 27752 sayılı İnternet Alan Adları Yönetmeliği ile düzenlenmiştir.

Burada üzerinde durulması gereken önemli bir diğer nokta da herhangi bir ülkeye aidiyeti bulunmayan bir alan adında kullanılmak istenilen kelime yahut kelimeleri kayıt ettirmek isteyen kişinin bu kelimeler ile herhangi bir bağlantısının olduğunu göstermesine yahut başvuruda bulunan kişinin yahut kurumun kim olduğuna dair herhangi bir belge göstermesine gerek olmaksızın; herhangi bir kelime yahut kelime grubunun onlar için başvuru yapan ilk kişi

---

[10] Sefer Oğuz, "İnternet Alan Adı (Domain Name) Haklarının Korunması" (Doktora Tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2011), 12.

[11] Oğuz, "İnternet Alan Adı," 30.

yahut kurum adına 'önce gelen alır' ilkesi doğrultusunda tescil edilmesi durumudur ki bu durum aşağıda tanımlanıp değerlendirilecek olan *'cybersquatting'* eyleminin temel nedeni olarak gösterilebilir. Nitekim işleyişin bu şekilde olması, uygulamada etik olmayan tarafları alan adını rehin tutarak marka hakkı sahibinden çıkar talebinde bulunmaya teşvik etmektedir.[12]

III. CYBERSQUATTING

Cybersquatting, tanınmış bir şirket adı yahut ticari markanın alan adı olarak bir başkası tarafından alınması veya ileride satılmak amacıyla kötü niyetli kişilerin benzer alan adlarını tescil etmesi şeklinde tanımlanabilir.[13] Bir başka ifadeyle *cybersquatting*, bireylerin kendilerine ait olmayan popüler isimleri hak sahiplerinden önce alan adı olarak kaydederek bu alan adlarından bireysel fayda sağlama amacı gütmeleridir.[14] Söz konusu terim, Amerikan federal hukuku içerisinde '*Anticybersquatting* Tüketiciyi Koruma Yasası[15]' altında

'Bir markanın kötü niyetle, bu markadan kar sağlamak amacıyla alan adı olarak kaydettirilmesi veya kullanılması'

şeklinde tanımlanmıştır.[16] *Cybersquatting* yalnızca bir başkasına ait markanın ileride yarar sağlamak için alan adı olarak kaydedilmesini değil, ayrıca bir marka ile kafa karıştırıcı şekilde benzer işaretlerin kaydedilmesini de kapsamaktadır.[17]

---

12 Colby B. Springer, "Master of the Domain : a History of Domain Name Litigation and the Emergence of the Anticybersquatting Consumer Protection Act and Uniform Dispute Resolution Policy." *Santa Clara Computer and High-Technology Law Journal* 17, no. 2 (2001): 322.

13 Daniel Chandler ve Rod Munday, *A Dictionary of Social Media,* (Oxford University Press, 2016).

14 Osborne Clarke, *A Practical Guide to E-commerce and Internet Law* (London: ICSA Publishing, 2002), 175.

15 İlgili yasanın orijinal adı Anticybersquatting Consumer Protection Act'tır.

16 Zorluoğlu, "Alan Adlarında Kötü Niyet Kavramı," 71.

17 Chen, "Optimizing Online Trademark Protections ", 592.

IV. ALAN ADININ ÖNEMİ

Tüketicilerin satın almak istedikleri şey hakkında bilgi sahibi olmak yahut o şeyi satın almak gibi nedenlerle ilgili şeye internet üzerinden erişmek istemeleri halinde ilgili alan adını yazmaları gerekmektedir. Ancak alan adının bilinmemesi durumunda o şeyin markasını veya ilgili firmanın adını arama motoruna yazarak yahut deneme yanılma yolu ile tüketicinin istediği web sitesine ulaşması mümkündür. Dolayısıyla *Trade Related Aspects of Intellectual Property Rights,* Türkçesi ile Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması'nın 15inci maddesinde "*Bir işletmenin ürün ya da hizmetlerini diğer işletmelerinkinden ayırabilen her türlü işaret veya işaretler birleşimi*"[18] şeklinde tanımlanan markanın *ürünü ve kaynağını ayırt edici rolü*nü internet ortamında *alan adı*nın üstlendiği çıkarımında bulunmak mümkündür.[19] Bu durum, şirketlerin alan adı olarak unvanlarını yahut markalarını kaydetmelerine sebebiyet vermiştir. Bir markanın sahibince alan adı olarak kaydedilmeden önce başkasınca kaydedilmesi halinde aslında X markasının web sitesine ulaşmak isteyen tüketici, X markasını yazdığında X markası alan adı altında Y markasına ait ürün yahut hizmete ilişkin web sayfası ile karşılaşmakta ve bu durum haksız rekabet, tüketici hakkı ihlali ve marka hakkına tecavüz gibi çeşitli sorunlara kapı aralamaktadır.

6102 sayılı Türk Ticaret Kanunu'nun 1524üncü maddesi

'Her sermaye şirketi, bir internet sitesi açmak, şirketin internet sitesi zaten mevcutsa bu sitenin belli bir bölümünü aşağıdaki hususların yayımlanmasına özgülemek zorundadır.'

---

[18] Başak Karadenizli, "Marka Tescilinde Ayırt Edicilik, Tanımlayıcılık ve Yanıltıcılık Değerlendirmelerinin Türkiye ve Yurt Dışındaki Uygulamaları ile Bunların Karşılaştırılması" (Uzmanlık Tezi, Ankara: T.C. Türk Patent Enstitüsü Markalar Dairesi Başkanlığı, 2008), 12.

[19] Mustafa Gençer, "Markanın İnternet Ortamında Alan Adı (Domain Name), Yönlendirici Kod (Metatag) veya Anahtar Sözcük (Keyword) Olarak Kullanılması Sonucu Oluşabilecek Marka İhlallerinin İncelenmesi" (Uzmanlık Tezi, Ankara: T. C. Patent Enstitüsü Markalar Dairesi Başkanlığı, 2014), 43.

hükmü uyarınca[20] denetime tabi olan sermaye şirketleri kendileri için bir internet sitesi açarak mevzuat ile belirlenen şekilde şirkete özgü ilanların bu internet sitesinde yapılmasını sağlama yükümlülüğü altına girmiştir. Ancak bu hüküm 2012 yılında

"(1) 397 nci maddenin dördüncü fıkrası uyarınca denetime tabi olan sermaye şirketleri, kuruluşlarının ticaret siciline tescili tarihinden itibaren üç ay içinde bir internet sitesi açmak ve bu sitenin belirli bir bölümünü şirketçe kanunen yapılması gereken ilanların yayımlanmasına özgülemek zorundadır" şeklinde değiştirilmiştir.[21]

Bu şekilde bağımsız dış denetime tabi şirketlere, internet sitesi oluşturma zorunluluğu getirilmiştir. Dolayısıyla birçok şirket açacağı web sitesi için gerekli alan adını ticaret unvanı yahut markasını yazarak tescil ettirme yoluna gitmiştir. Bu durum, alan adlarının marka yahut ticaret unvanı ile bağlantısını güçlendirmiştir.

Bir kimsenin alan adı tescil ettirirken kendi alanında belirli bir müşteri kitlesine ulaşmış olan başkasına ait bir markayı alan adı olarak seçmesinin nedeni;

a. bu markanın tanınmışlığından faydalanarak kendi mal ve hizmetlerini daha geniş alıcı kitlelerine duyurabilmek -ki bu durumda marka hakkı sahibinin ticari itibarının haksız olarak kullanılması ve marka sahibinin emeğinin karşılığından marka sahibi olmayan bir kimsenin faydalanması söz konusudur-[22] olabileceği gibi,

b. sonrasında para karşılığında ilgili markanın ismi geçen alan adını marka sahibine pazarlamak da olabilir. Son derece önemli hale gelmiş olan alan adlarının bu şekilde kötü niyetli kullanımları durdurmak ve gerek marka sahiplerinin gerekse tüketi-

---

20 Konu ile ilgili detaylı bilgiler Sermaye Şirketlerinin Açacakları İnternet Sitelerine Dair Yönetmelik'te düzenlenmiştir.

21 "İnternet Alan Adları Tebliği," Mevzuat Bilgi Sistemi, Erişim terihi Şubat 03, 2019. http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=9.5.18752&MevzuatIliski=0.

22 Zeynep Şarlak, "İnternet Alan Adının (Domain Name) Hukuki Niteliği ve Marka Hakkı Üzerindeki Etkisi" (Yüksek Lisans Projesi, Ankara: T. C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Ticaret Hukuku) Anabilim Dalı, 2006), 61.

cilerin haklarını korumak için alan adlarında başkasına ait markanın kullanılması durumuna yönelik önleyici düzenlemeler yapılması gerekmektedir. Öte yandan alan adı tahsisinde ICANN'ın 'ilk başvurana tahsis edilir' anlayışını haiz olması birçok uyuşmazlığı beraberinde getirmiş ve uluslararası örgütler uyuşmazlıkların çözümü için uyuşmazlık çözüm hizmet sağlayıcıları mekanizmasını hayata geçirmişlerdir.

V. UYUŞMAZLIK ÇÖZÜM HİZMETİ SAĞLAYICILARI

1 Temmuz 1997de Amerikan Ticaret Bakanlığı, alan adı tescil ve idare yetkisini özel sektöre devredeceğini açıklamış ve 1998 yılında İnternet Ad ve Adreslerinin İdaresi Hakkında Politika Bildirisi yayınlamıştır.[23] WIPO Hakemlik ve Arabuluculuk Merkezi bünyesinde alan adları ile marka arasında çıkan uyuşmazlıkların çözümlenmesi için 30 Nisan 1999 tarihinde WIPO, *cybersquatter* kişilere karşı marka hakkı sahiplerini koruyucu önlemler ve internet alan adı prosedürünün nasıl işlemesi gerektiğine ilişkin çeşitli öneriler içeren bir rapor yayınlamıştır.[24] İlgili raporda uyuşmazlıkların çözümüne yönelik oluşturulan panellerde hangi ülke hukukunun uygulanması gerektiğine yönelik durumlara da yer verilmiştir. Örneğin her iki taraf da aynı ülkede ikamet etmekte ise, alan adı o ülkede kaydedilmiş ve alan adının kötü niyetle kaydedildiği ve kullanıldığına yönelik kanıtlar da o ülkede ise panelistin, ilgili alan adı uyuşmazlığında o ülke hukukuna göre karar vermesi gerektiği belirtilmiştir.[25] ICANN, bu rapor üzerinde geçici olarak mutabık olmakla beraber kamuoyu tavsiyelerini değerlendiren yorumları da dikkate alarak hangi WIPO önergesinin hangi kısımlarını ne şekilde kabul edeceği üzerine araş-

---

[23] Nurullah Bal, "İnternet Alan Adları ve İnternet Alan Adı Uyuşmazlıklarının Tahkim Yoluyla Çözümlenmesi," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17, no. 1-2 (2013): 323.

[24] Raporun orijinal tam metnine ulaşmak için bakınız: "Final Report of the First WIPO Internet Domain Name Process," WIPO, Erişim tarihi Şubat 03, 2019, https://www.wipo.int/amc/en/processes/process1/report/index.html.

[25] King, "ICANN, Dispute Resolution," 486.

tırma yapmayı gerekli görmüştür.[26] Bu tür uyuşmazlıkların çözüm mekanizmalarında da çeşitli sorunlarla karşılaşılmaktadır. Nitekim ICANN, üç uyuşmazlık çözüm servisi sağlayıcısına toplam 668 başvuru yapıldığını, bunlardan 129 uyuşmazlığın karara bağlandığını, 9 alan adının iptal edildiğini, davalı için 64 karar verildiğini, kararların bölünmüş olduğu 2 durum olduğu yani jürinin uzlaşıya varamadığı 2 başvuru olduğunu, 234ünün de alan adlarının devredilmesi şeklinde karara bağlandığını değerlendirmiştir. Bir başka deyişle, başvuru yapılan alan adlarından %80i devredilmiş yahut iptal edilmiş ve sadece %20sinin sahiplerinin kullanımında bırakılması hükme bağlanmıştır.[27]

Türkiye'de de 2010 yılı 27752 sayılı İnternet Alan Adları Yönetmeliği 23üncü maddesinde

'Alan adları ile ilgili ihtilaflar alternatif olarak UÇHS'ler tarafından işletilen uyuşmazlık çözüm mekanizması vasıtasıyla çözülür. Uyuşmazlık çözüm mekanizmasının işletilmesine ilişkin usul ve esaslar Kurum tarafından düzenlenir.'[28]

denmek suretiyle alan adlarına yönelik uyuşmazlıkların çözümü için alternatif yol olarak Uyuşmazlık Çözüm Hizmet Sağlayıcılar tarafından yürütülen uyuşmazlık çözüm mekanizmaları gösterilmiştir. Bu uyuşmazlık çözüm mekanizmalarına başvurmak isteyen kişi için sağlaması gereken şartlar ise ilgili yönetmeliğin 25inci maddesinde

'(1) Uyuşmazlık çözüm mekanizmasına başvuru için;

a) İhtilaf konusu alan adının, sahip olunan ya da ticarette kullanılan marka, ticaret unvanı, işletme adı ya da diğer tanıtıcı işaretlerle benzer ya da aynı olması ve

b) Alan adını tahsis ettiren tarafın bu alan adı ile ilgili yasal bir hakkı ya da bağlantısının olmaması ve

---

[26] Jennifer Golinveaux, "What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?" *University of San Francisco Law Review* 33, no. 4 (1999): 670.

[27] King, "ICANN, Dispute Resolution," 482.

[28] "İnternet Alan Adları Yönetmeliği," Mevzuat Bilgi Sistemi, erişim tarihi Ocak 01, 2018, http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.14416&MevzuatIliski=0.

c) Bu alan adının alan adı sahibi tarafından kötü niyetle tahsis ettirilmesi veya kullanılması gerekmektedir.[29]

şeklinde sıralanmış ve ikinci fıkrada

(2) Bu maddenin birinci fıkrasında yer alan üç şartın birlikte sağlandığını iddia eden şikâyetçi, uyuşmazlığın çözümü için UÇHS'lerden birini tercih ederek başvurusunu yapar. Şikâyetçi başvuruda bulunduğu UÇHS'nin kendisine kesin bir karar bildirmesine kadar aynı hususta başka bir UÇHS'ye başvuruda bulunamaz.'[30]

denmek suretiyle uyuşmazlık çözüm hizmet sağlayıcısına başvurabilmek için 'alan adının marka, ticaret unvanı vb. ile benzer ya da aynı işareti içermesi', 'kullanıcı ile alan adı arasında meşru bir ilişki olmaması' ve 'kötü niyet' unsurlarının hepsinin bir arada bulunması gerektiği belirtilmiştir.

VI. MARKANIN ALAN ADI OLARAK KAYDEDİLMESİ

İnternete yönelik hukuki düzenlemeler, diğer konulardaki hukuki düzenlemeler kadar etkili olamamaktadır. Nitekim hukuk ülkelerin yetki alanı ile sınırlandırılmış bir işleve sahip olduğundan ve internet içeriğini ülke hudutları üzerinden sorunsuzca diğer ülkelere eriştirdiğinden, internetin diğer konular gibi ülkelerin hukuki düzenlemeleri ile kontrol altında tutulması oldukça güçtür.[31] Markaların internet alan adı olarak kaydedilmesi sorununun da internetin bizatihi bu niteliğinden ötürü konunun daha iyi analiz edilmesini sağlaması açısından ülkelere göre incelenmesi tercih edilmiş ancak tüm ülkeler için ayrı ayrı inceleme yapılması zaman ve yazım kısıtından ötürü mümkün olmadığından inceleme; Amerika, Avustralya ve Türkiye hukuku şeklinde sınırlandırılmıştır.

---

[29] Mevzuat Bilgi Sistemi, "İnternet Alan Adları Yönetmeliği."

[30] Mevzuat Bilgi Sistemi, "İnternet Alan Adları Yönetmeliği."

[31] Andrew Murray, *Information Technology Law* (New York: Oxford University Press, 2013), 49.

A. Amerikan Hukukunda

ABD ticari marka hukuku uyarınca ticari marka veya hizmet markasının birden fazla kullanıcısının bir arada bulunması yasal olarak mümkün kılınmış olmakla birlikte geçerli alan adı sistemi altında bir alan adının yalnızca belirli bir Web sitesini tanımlayabileceği belirtilmiştir.[32] Bununla birlikte bir kişi birden fazla alan adı almış ise bu farklı alan adlarının tek bir siteye bağlı olması yahut her bir alan adının farklı bir siteye bağlı olması yahut aynı Web sitesinde farklı sayfalara bağlı olması da mümkündür. Aynı ticari isme sahip iki farklı şirketin tamamen aynı alan adını kullanmaları internet işleyişindeki sistem kapasitesi düşünüldüğünde tam olarak imkansız olmakla birlikte bu şirketlerin ufak farklılıklar içerecek şekilde alan adları almaları mümkündür. Bir şirket kendi ticari markasını alan adı olarak almadan önce o ticari markayı alan adı olarak rezerve eden *cybersquatter*, o şirketin kendi ticari markasını *cybersquatter* kişinin aldığı şekilde gerek üst seviye alan adı gerekse ikinci seviye alan adı olarak kullanmasını doğrudan engellemiş olmaktadır. Diğer taraftan, şirketin, ticari markasını *cybersquatter* kişinin almadığı başka bir üst seviye alan adı ile kullanabilmesi mümkündür. Ayrıca bu şekilde aynı ticari isme sahip farklı iki şirketin bu ticari ismi kullanarak Web sitelerini ziyaretçilere açmaları da; kendi aralarında anlaşmaları ile tek ticari isme ait alan adına bağlı sayfaya gelen ziyaretçilere kendi şirketlerine ait linkleri sunarak ziyaretçinin istediği şirketin linkini seçerek o sayfaya bağlanması ile mümkündür. Bu durum her ne kadar şirketlerin aralarında anlaşmaları ile aynı ticari isme ait alan adının tek bir Web sayfası sunması problemini çözmelerini sağlamakta ise de bir başkasının o ticari isimle alan adı alarak ticari isim sahibi şirketlerin bu alan adını o kişiden satın almadıkça kullanamamaları yani *cybersquatting* problemine bir çözüm sunmamaktadır.[33] Bu durum ticari marka sahibi şirketlerin kendi ticari markalarını kullanarak alan adı alarak Web sayfası açmaları için *cybersquatter* kişiye istediği yüklü miktarda ücret ödeyerek kendi

---

[32] Golinveaux, "What's in a Domain Name," 643.

[33] Golinveaux, ""What's in a Domain Name," 644.

ticari isimleri olan alan adını satın almalarına yahut *cybersquatter* kişiye karşı hukuki süreç başlatmalarına yol açmaktadır.

Bu şekilde *cybersquatter* kişilerin ilklerinden ve en meşhurlarından birisi olan Dennis Toeppen, alan adlarının ekonomik değerini büyük şirketler fark etmeden önce idrak ederek meşhur markalara ait 100 ün üzerinde alan adı almış ve ticari markalarını kullandığı şirketlerden alan adlarının kendilerine aktarılması için ödeme talep etmiştir. Dolayısıyla birçok şirket Toeppen'e ilgili alan adlarının Toeppen'den alınarak hak sahiplerine devredilmesi için ticari marka ihlali sebebiyle dava açmak durumunda kalmıştır.[34] Bu davalardan önemli birisi de Panavision'un Toeppen'e karşı panavision.com alan adından dolayı açmış olduğu davadır. Bu davada Panavision;. birincisi, 'internet alan adlarına yönelik mülkiyet hakkı nasıl, neye göre tahsis edilmelidir?', ikincisi, *kurulu marka analizi*[35] ünlü ticari markalar başta olmak üzere internet alan adları uyuşmazlıkları üzerine uygulanabilir mi?', ve 'mahkemece ilgili yasanın bu davaya uygulanması doğru şekilde gerçekleşmiş midir?' olmak üzere çözümlenmesi gereken 3 konuya dikkat çekmiştir.[36] Dava, özetle, Toeppen'in; içerisinde ABD'nin Illionis eyaletindeki Pana şehrinin kuşbakışı çekilmiş fotoğrafının olduğu 'panavision.com' ve sadece 'hello' yazılı olan 'panaflex.com' alan adları ile kaydetmiş olduğu web sitelerinin Panavision Ltd. tarafından reklamcılık ve pazarlama için kullanılmak üzere web sayfası oluşturulacağı zaman farkedilmesi üzerine kendisiyle irtibata geçerek kaydetmiş olduğu alan adlarını Panavision'a bırakmasının istenmesi ve bunun üzerine Toeppen'in şirketten alan adı kullanımının durdurulmasına karşılık $ 13,000 talep etmesi üzerine Panavision'un alan adları için kullandığı markaları ihlal ettiği iddiası ile Toeppen'e karşı mahkemeye başvurması şeklinde gelişmiştir.[37] Toeppen davasında mahkeme, Amerikan tica-

---

34 Lipton, "Beyond Cybersquatting,"1388.

35 Terimin orjinali *established trademark dilution analysis* şeklindedir.

36 Ughetta Manzone, "Panavision International, L. P. v. Toeppen," *Berkeley Technology Law Journal* 13, no. 1 (1998): 249.

37 Dava hakkında detaylı bilgi için bakınız: Manzone, "Panavision International, L. P. v. Toeppen," 249 - 264.

ri marka ihlallerinin engellenmesine yönelik yasasının ana konularından olan tüketicinin markayı karıştırmasına neden olup olmama konusu üzerinde hiç durmamış ve ticari marka mülkiyetinin marka sahibine ait olması konusu üzerinde durmuştur.[38]

Amerikan hukuku doğrultusunda, uygulamada bir kimsenin marka hakkının ihlali iddiasında bulunabilmesi için yasal olarak markanın korunması hakkını haiz olduğunu ve bu hakkın ihlal edilmiş olduğunu göstermesi gereklidir. İlgili işaret; 1.genel, 2.tanımlayıcı, 3.fikir verici, 4.hayali ve ihtiyari (rastgele) şeklindeki 4 kategoriden 3üncü yahut 4üncü kategori sınıfında yer almalıdır ki marka hukuku kapsamında korunabilsin. Ancak 2nci kategoride sınıflanan bir işaret de ikinci başka bir anlam taşıdığının ispatlanması şartıyla korunabilecektir. Ayrıca *Anticybersquatting* Tüketiciyi Koruma Yasası ile ABD Patent ve Ticari Marka Ofisi'[39]ne kayıtlı olan markalar korunduğu gibi, henüz markasını kaydettirmemiş marka sahiplerinin hakları da koruma altına alınmıştır.[40] Amerikan hukukunda asıl kural genel itibariyle marka ihlali iddialarında iddia edenin, uyuşmazlık konusu işaretin marka ile karıştırılabilir şekilde benzer olduğunu yahut marka sahibi ile iddia edilen hak ihlaline neden olan kişinin markanın kullanımı üzerinde rekabet ettiklerini göstermesi şeklindedir.

B. Avustralya Hukukunda

Avustralya'da bir alan adının yalnızca tescil edilmesi, o ticari markanın kullanımı anlamına gelmemektedir. Sports Warehouse, Inc'in Fry Consulting Pty Ltd'e karşı açmış olduğu dava[41] ile *Mantra*

---

38 Sam K. Tahmassebi, "Panavision International v. Toeppen," *The Journal of Contemporary Legal Issues* 12, no. 1 (2001): 514.

39 Kurumun orijinal ismi U.S. Patent and Trademark Office'dir.

40 Neil L. Martin, "The Anticybersquatting Consumer Protection Act: Empowering Trademark Owners, but not the Last Word on Domain Name Disputes," *The Journal of Corporation Law* 25, no. 3 (2000): 591 - 598.

41 Sports Warehouse Inc v Fry Consulting Pty Ltd davası için bakınız: "Sports Warehouse, Inc v Fry Consulting Pty Ltd [2010] FCA 664 (25 June 2010)" Federal Court of Australia, erişim tarihi Şubat 7, 2019, http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2010/664.html?query=.

Group Pty Ltd'in *Tailly Pty Ltd*'e karşı açmış olduğu davada[42] Avustralya Federal Mahkemesi'nin verdiği kararlar dikkat edilmesi gereken hususları açıklayarak marka isminin marka sahibinden başkası tarafından alan adı olarak tescil ettirilmesinin hangi durumlarda haksız ticari marka kullanımı olarak değerlendirilebileceği sorusunun çözümlenmesi için yol gösterici nitelikte olmuştur. Bu açıdan ilgili davaların ayrı ayrı incelenmesi yerinde olacaktır.

1. Sports Warehouse, Inc v Fry Consulting Pty Ltd Kararı

Kaliforniya'da kurulmuş olan *Sports Warehouse*, tenis kıyafeti ve tenis ekipmanları üzerine 1994 yılından beri ticaret yapmakta olan bir şirkettir. 1995 yılından beri tüm dünyadan müşterilerine satışlarının çoğu www.tennis-warehouse.com web sitesinden olmak üzere hizmet vermekte olan şirket, 18 Ağustos 2005 tarihinde '*tennis warehouse'* kelimesini markası olarak tescil ettirmek üzere başvuruda bulunmuştur. Başvuru, markanın ayırt edicilik unsuru açısından itiraza uğramış ancak *Sports Warehouse'ın* markanın ayırt etme kapasitesini haiz olduğunu ispatı sonrasında *Sports Warehouse'ın* başvurusu kabul edilmiştir. Ancak Avustralya'nın *Fitzroy* kentinde *Sports Warehouse'un* faaliyetleri Avustralya'ya genişledikten sonra kurmuş olduğu www.tenniswarehouse.com.au web sitesinde ana perakende faaliyetlerini yürütmekte olan tenis kıyafeti ve tenis donanımı satan bir toptancı ve perakendeci olan *Fry Consulting* başvuruya itiraz etmiştir. Dava *Sports Warehouse* tarafından Ticaret Mahkemesinden Federal Mahkeme'ye temyiz edilmiştir. İtirazlar üzerine mahkemenin öncelikle 'ticari marka tescil başvurusunun yapıldığı tarihte Sports *Warehouse'un* '*tennis warehouse'* markasını online perakende servisleri içerisinde ayırt edicilik niteliğini haiz şekilde kullanmakta olup olmadığı' sorusunu cevaplaması gerekmiştir.

---

[42] *Mantra Group Pty Ltd v Tailly Pty Ltd* davası için bakınız: "Mantra Group Pty Ltd v Tailly Pty Ltd (No 2) (includes Corrigendum dated 31 August 2010) [2010] FCA 291 (26 March 2010)," Federal Court of Australia, erişim tarihi Şubat 7, 2019, http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2010/291.html?stem=0&synonyms=0&query=Mantra%20Group%20Pty%20Ltd.

Davadaki önemli bir diğer nokta da mahkemenin 'alan adının ticari marka olarak kullanılıp kullanılmadığını' ve 'bahse konu alan adının kullanımının '*tennis warehouse'* markasının kullanımı ile aynı şey olup olmadığını' tartışmış olmasıdır. Davada 'bir alan adı ticari marka olarak kullanılabilir, ancak eleştirel olarak, alan adının içerisinde geçtiği alandaki kullanım şekli, alan adının ticari marka olarak kullanılıp kullanılmadığını belirler' şeklinde yorum yapılmıştır.[43] Ayrıca kararda, Avustralya içtihat hukukunun bu konuda eksik yönlerinin olduğu belirtilmiştir.

Kararda *cybersquatting* ile ilgili önemli davalardan olan *CSR Ltd* ile *Resource Capital Australia Pty Ltd* davası[44]na da değinilmiştir. Nitekim bu davada *cybersquatter* kişinin kaydetmiş olduğu "csrsugar.com" ve "csrsugar.com.au" alan adlarını görenler CSR'nin alan adının gerçek sahibi olduğunu ve bu alan adlarını şeker işletmeleriyle bağlantılı olarak internet üzerinden yapmayı amaçladığı işleri doğrultusunda kullanabileceğini düşünebileceğinden, ilgili olayda her iki alan adını da tescil etme eyleminin yanıltıcı ve aldatıcı davranış teşkil ettiğine ve dolayısıyla 1974 tarihli Ticaret Uygulamaları Kanunu[45]'nun ihlal edildiğine karar verilmiştir. Bununla birlikte hakim Hill J, kararında, uyuşmazlık konusu alan adları için marka hakkı ihlalinin olmadığını, zira alan adlarının CSR'nin tescil ettirmiş olduğu alana ilişkin hiçbir ürün yahut hizmete yönelik bir kullanımının ve kullanımı yönünde bir eğilimin bulunmadığını, ancak davalı bu konuda CSR ile rekabet içerisinde bir ticaret yapmış olsa idi marka hakkı ihlali ihtimalinin düşünülebileceğini belirtmiştir.

---

43 Ian Drew ve Elizabeth Godfrey, "When will Domain NamesBe Considered "Use" of a Trade Mark?" *Davies Collison Cave Intellectual Property,* 10 Aralık 2010, erişim tarihi Nisan 28, 2017, http://www.davies.com.au/ip-news/when-will-domain-names-be-considered-use-of-a-trade-mark.

44 İlgili davada hakim Hill J, davalının CSR markasını alan adı olarak aldığı ancak bu alan adına bağlı web sitesinde CSR'nin bilindiği 'şeker' de dahil herhangi hiçbir ürün satmadığı olayda marka taklitçiliğinin olduğuna, ancak CSR'nin davalı tarafından herhangi bir ürün yahut hizmet ile ilişkili olarak kullanılmamasından ötürü marka hakkına tecavüz bulunmadığına karar vermiştir. Detaylı bilgi için: Mark Davison, Ann Monotti ve Leanne Wiseman, *Australian Intellectual Property Law* (Melbourne: Cambridge University Press, 2015), 170.

45 Söz konusu kanunun orijinal ismi 'Trade Practices Act'tır.

Yine *Sports Warehouse* davasında yer verilen bir diğer karar da İngiltere Yüksek Mahkemesi'nin *Ellerman Investments Ltd* v *C-Vanci* davasında alan adı kullanımının ticari marka kullanımı olarak değerlendirilebileceğine ilişkin kararıdır. Söz konusu kararda her ne kadar davalının logosu ile davacının ticari marka yahut logosu arasında hiçbir benzerlik olmasa da genellikle oyuna yönelik açıklamaları oyun kurallarını belirterek kullanıcılara online ortamda masa etrafı kart oyunları yahut başka çeşitli oyun hizmetleri sunan *Ritz Online* hizmetleri ile davalının ritzpoker.net alan adı ile sunduğu hizmetler ve web sitelerinin önemli ölçüde benzer olduğu, ancak buna karşın davalının alan adında *Ritz* ismini değil, *ritzpoker* olarak *ritz*'den farklı bir kelime kullanmış olduğu ve bu, yani *ritzpoker*in *ritz*den farklı oluşunun, ortalama bir tüketici tarafından fark edilmeyecek derecede küçük ve önemsiz bir fark olmadığı belirtilmiştir.[46]

Amerikan Temyiz Mahkemesi'nin alan adlarında ve otomobillerle alakalı web sitelerine linkler sağlanmasında kapsamına otomobillerin de girdiği tescilli Nissan markasının ihlal edildiği şeklinde karara bağlanmış olan *Nissan Motor Co v Nissan Computer Corp* 378 F 3d 1002 (9th Circuit 2004) davası, kararda değinilen bir diğer davadır.

Bahse konu kararda hakim, yalnızca alan adı tescili yapılmasının, alan adının ticari marka olarak kullanılması anlamına gelmediği şeklinde hüküm vermiştir. Alan adının ticari marka kullanımı niteliğinde olduğunun kabul edilebilmesi için yalnızca tescil işleminin yeterli olmadığını, ayrıca alan adının hangi bağlamda kullanıldığından hareketle alan adının ticarette mal veya hizmetleri ayırt etmek için bir işaret olarak kullanılıp kullanılmadığının belirlenmesi gerektiğini belirtmiştir. Bu düşünce doğrultusunda www.tennis-warehouse.com alan adının '*tennis warehouse*' markasının kullanımı şeklinde nitelenip nitelenemeyeceğini değerlendirilmiştir. Sonuç olarak www.architectsaustralia.com.au alan adının 'architects australia' markasının kullanılması ile aynı şey olduğuna hükmedilmiş olan *Architects (Aust) Pty Ltd t/a Architects Australia v Witty Consultants Pty*

[46] Gaming Law Review, "Ellerman Investments Ltd and Another v. C-Vanci and Another Chancery Division," (Mary Ann Liebert, Inc) 10, no. 5 (2006): 514-518.

Ltd davasına dayanılarak hüküm verilmiştir. Yargıç, online hizmetler bağlamında halkın 'ticari marka ismi' olarak web sitesinde erişime açık bulunan ticari marka ile ayırt edilebilen online hizmetlere dair işaretleri anladığını, ve bunun alan adı ile aynı şey olmadığını, olayda '*tennis warehouse'* markasına çeşitli eklemeler yahut değişiklikler yapılarak yeniden yapılandırılmış bir kullanım olmakla beraber bu ekleme yahut değişikliklerin markanın ayırt edici niteliğini çok da etkilemeyen değişiklik yahut eklemeler şeklinde olduğunu ifade etmiştir.[47]

2. Mantra Group Pty Ltd v Tailly Pty Ltd Kararı

Markanın alan adı olarak kullanımına yönelik Avustralya hukukuna önemli derecede etki eden bir başka karar da *Mantra Group Pty Ltd v Tailly Pty Ltd* davasıdır. Olayda *Queensland*'ın *Gold Coast* kentinin merkezinde bulunan seçkin bir tesis olan *Mantra*, gayrimenkul yönetimi ve konaklama hizmetlerine yönelik '*circle on cavill'* kelimelerini içeren tescilli 3 markaya sahiptir. Tailly ise *circle* on *cavill* kompleksinde yaklaşık 39 daireye yönelik olarak çalışan bir saha dışı acentedir. Internet üzerinden araştırma yahut rezervasyon yapan tüketicilerin büyük bir yüzdesi göz önüne alındığında her iki tarafın da internet tabanlı reklam ve pazarlama üzerine büyük ölçüde zaman ve masraf ayırdığı görülmektedir. Tailly, pazarlama stratejisinin bir parçası olarak, ana internet sitesiyle bağlantılı olarak 10 alan adında ve web sitesinde "*circle on cavill*" ve türevlerini kullanmıştır. Tailly ayrıca "*circle on cavill*" kelimesi veya türevlerini web sitelerinin kaynak kodu içerisinde *metatag* olarak kullanmıştır. Öyle ki aynı web sitesinde 250den fazla kez "*circle on cavill*" veya benzeri kelimeleri kullandığı da olmuştur. Bu online pazarlama stratejisi, Tailly'nin, arama sonuçlarının ilk sayfasındaki web siteleri sıralamasında üstten 4. linke yükselmesine, ki bu durum tüketicilerin Tailly web sitelerine çok yüksek oranda tıklama sağlayarak ziyaret etmelerini sağlar, vesile olmuştur. Davada Mantra, Tailly'nin internet üzerinde bu şekildeki pazarlama ve reklamcılığından dolayı, "*circle on cavill*" markasını ihlal ettiğini, tüketiciler üzerinde Tailly'den ziyade Mantra ile işlem yapıyorlarmış kanısı uyandırarak

[47] Drew ve Godfrey, "When Will Domain Names Be Considered.

tüketicilerin yanılma ve aldatılmalarına neden olarak TPA[48] (Ticari Uygulamalar Kanunu)'na aykırı davranışta bulunduğunu beyan etmiştir. Davada Tailly, gayrimenkul yönetimi ve konaklama hizmetleri ile ilgili olarak '*circle on cavill'* ticari markalarıyla özdeş veya aldatıcı şekilde benzer olan kelimeleri kullandığını kabul etmekle birlikte sunulan konaklama hizmetleri ile Tailly arasındaki bağlantıyı belirtmek üzere '*circle on cavill'* kelimesini ve alan adını ticari marka yahut menşe işareti olarak kullandığı iddiasına karşı çıkmıştır.

Davalı Tailly, *circle on cavill* ve benzeri kelimelerin, hizmetlerin menşeini göstermekten ziyade evlerin bulunduğu kompleksin adını göstermek üzere ve iyi niyetle konaklama hizmetlerinin coğrafi menşeini belirtmek için kullanıldığını, ki bu şekilde kullanım Avustralya hukukunda Ticari Markalar Kanunu 122 (1)(b)(i) hükmü[49] uyarınca ticari marka ihlalinin bulunmadığı durumlardan kabul edilmiştir, iddia etmiştir.[50] Davada Tailly'nin internet sitelerinde '*circle on cavill'* kelimelerinin markanın işlevlerinden olan tanımlayıcı işlevde kullanılmadıkları, ancak bu durumun site dışı hizmetlerin menşei olarak Tailly'i göstermesi dikkate alındığında, kelimelerin markanın tanımlayıcı işlevinde kullanılıp kullanılmadıkları analizinin önemini kaybettiği belirtilmiş ve Tailly'nin savunması reddedilmiştir. Ayrıca Avustralya Ticari Markalar Kanunu 122 (1)(b)(i) hükmünde geçen 'hizmetlerin coğrafi menşei' ibaresi hakim tarafından bir ülkenin, bölgenin, şehrin, kasabanın ismini ifade ettiği, özel mülkiyete tabi bir bina ismini kapsamadığı şeklinde yorumlanmış ve Tailly'nin bu savunması da kabul edilmemiştir. İyi niyet konusunda ise hakim Reeves J, '*circle on cavill'* kelimelerinin alan adında bulunan ve internet sitesinin kaynak kodunda 250den fazla kez *metatag* olarak kullanılması ve Tailly'nin web tasarımcısının arama motoru optimizasyonu amacıyla Tailly'nin internet sitesinde '*circle*

---

48 İlgili yasanın orijinal adı Trade Practices Act'tır.

49 İlgili hükmün orijinali (sub-section 122 (1)(b)(i) Trade Marks Act 1995 (Cth) ("TMA") şeklindedir.

50 Martin O'Connor, "Australia: The Mantra Decision: Strata Titled Properties: Registered Trade Marks," *Mondaq Business Briefing*, Mayıs 2010, erişim tarihi Şubat 03, 2019. http://www.mondaq.com/australia/x/99714/Trademark/ The+Mantra+ Decision+Strata+Titled+Properties+Registered+Trade+Marks.

on cavill' kelimelerini birçok defa kullanması dolayısıyla iyi niyet unsurunun ortadan kalktığına hükmetmiştir.[51]

Sonuç olarak mahkeme, Tailly'nin internet üzerindeki bu tür kullanımlarının '*circle on cavill'* kelimesinin ticari marka olarak kullanılması olduğuna hükmetmiş[52] ve Tailly'nin kullanmakta olduğu ve '*circle on cavill'* yahut benzeri kelimeleri içeren alan adlarının '*circle on cavill'* markası sahibi Mantra'ya aktarılmasına ve Tailly'nin '*circle on cavill'* ve türevi kelimeleri konaklama rezervasyonlarında reklam, tanıtım gibi amaçlarla yahut da alan adının bir parçası, metatag, arama motoru anahtar kelimesi, işletme adı vb. şekillerde ticari marka olarak kullanımının kalıcı olarak ve tamamen kısıtlanmasına yönelik ihtiyari tedbir kararı alınmasına ve Tailly'nin bu şekilde Mantra'nın marka hakkını ihlal ederek kullandığı internet sitelerinden elde ettiği kazançları Mantra'ya ödemesine hükmetmiştir.[53]

C. Türk Hukukunda

Türk hukukunda 6769 sayılı Sınai Mülkiyet Kanunu marka tescilinden doğan hakların kapsamı ve istisnaları başlığı altında düzenlenen 7nci madde hükmü uyarınca tescilli marka sahibinin kendisinden izinsiz olarak; kullanma hakkı veya marka ile herhangi bir meşru bağlantısı olmayan kimsenin marka işaretinin aynısını veya benzerini internet ortamında ticari etki yaratacak biçimde alan adı, yönlendirici kod, anahtar sözcük ya da benzeri biçimlerde kullanması halinde marka sahibi, bu mutlak hakkını kullanarak markasının bu şekilde kullanılmasının engellenmesini talep edebilir[54]. Bu şekilde internet ortamında kullanılan işaretler, harfler, kelimelerle ilgili olarak ortaya çıkan uyuşmazlıklarda öncelikli değerlendirilmesi gereken birtakım konular bu-

---

51 Drew ve Godfrey, "When Will Domain Names Be Considered."

52 Michael Morris, "Real Estate Marketing on the Internet: Using Registered Trade Marks Online," *Mondaq Business Briefing*, Şubat 2010, erişim tarihi Şubat 03, 2019, http://www.mondaq.com/australia/x/104392/Trademark/Real+Estate+Marketing+on+the+Internet+Using+Registered+Trade+Marks+Online.

53 Drew ve Godfrey, "When Will Domain Names Be Considered."

54 "Sınai Mülkiyet Kanunu," Mevzuat Bilgi Sistemi, erişim tarihi Ocak 05, 2018, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6769.pdf.

lunmaktadır. Nitekim öncelikle uyuşmazlığa kapı aralamış olan işaretin marka olarak kullanılabilip kullanılamayacağının belirlenmesi gerekir. Eğer söz konusu işaretin marka olarak kullanılabilecek türden bir işaret olduğu kanısına varılırsa, işaretin kullanıldığı ortamın marka olarak kullanıma uygun olup olmadığı belirlenmelidir. Burada söz konusu işaretin, tescilli markanın kapsadığı mutlak hak sınırları içerisine girip girmediği de ayrıca belirlenmelidir.

6769 Sayılı Sınai Mülkiyet Kanunu'nun 7nci maddesinin

"*(3) Aşağıda belirtilen durumlar, işaretin ticaret alanında kullanılması hâlinde, ikinci fıkra hükmü uyarınca yasaklanabilir*:

…

d) İşareti kullanan kişinin, işaretin kullanımına ilişkin hakkı veya meşru bağlantısı olmaması şartıyla işaretin aynı veya benzerinin internet ortamında ticari etki yaratacak biçimde alan adı, yönlendirici kod, anahtar sözcük ya da benzeri biçimlerde kullanılması..."[55]

şeklindeki 3/d fıkrasında geçen işaretin aynı veya benzerinin internet ortamında kullanımıyla ilgili olarak işaretin benzer mi, aynı mı olduğunun belirlenmesi önemlidir. Nitekim işaretin aynı değil fakat benzer olması durumunda bu benzerliğin iltibasa yol açıp açmayacağının ayrıca değerlendirilmesi gerekecektir. Bunla ilgili olarak tescilli markanın benzerinin internet alan adı olarak kullanılması ile bir başkası tarafından marka olarak kullanılması farkı yorumlanabilmektedir. Örneğin daha önce tescil edilmiş Alpi markası ile Alba markasının iltibası yani bunlar arasındaki benzerliğin ayırt edilemeyeceği kabul edilebilirken, Alba sözcüğünün internet alan adı olarak kullanılmasının Alpi markası ile iltibas oluşturmayacağı düşünülmektedir.[56]

Yapılması gereken bir diğer inceleme, madde hükmünde geçen *'işaretin kullanımına ilişkin hakkı veya meşru bağlantısı olmaması'* ibaresi dolayısıyla kişinin meşru bağlantısının olup olmadığının tespitidir. Bu tespitin yapılmasında, WIPO tahkim ve arabuluculuk merkezi gibi markanın internet alan adı olarak kullanılmasına ilişkin uyuş-

---

55 Mevzuat Bilgi Sistemi, "Sınai Mülkiyet Kanunu."

56 İsmail Kırca, "Tescilli Markanın Üçüncü Kişi Tarafından Alan Adı Olarak Kullanılması," *Prof. Dr. Ömer Teoman'a 55. Yaş Günü Armağanı* içinde (İstanbul: Beta, 2002) , 536, 537.

mazlıkları çözen merkezlerin kuralları dikkate alınmalıdır.[57] İşareti kullanma hakkının, marka sahipliğinden başka şekillerde de mümkün olduğu görülmektedir. Zira o işaret için lisans, acentelik, tek satıcılık, *franchising*, *know-how* gibi fikri haklara yönelik sözleşmelerin yapılmış olması halinde yahut kanun yolu ile devrolunan devlet kurumunun sahip olduğu markaların devrolunan kurumca kullanılabilmesinde olduğu gibi kanundan doğan bir hak sonucu işaretin kullanılması hakkı haiz olunabilir.

Hükümde yer alan 'meşru bağlantı' şu şekilde örneklendirilebilir: Bir şirketçe 10 yılı aşkın süredir kullanılmakta olan bir alan adında geçmekte olan ve tescilli olmayan bir işaret için yahut yine uzun süre kullanılmak şartı ile anahtar kelime olarak yahut *spamming* için kullanılan bir işaret için meşru bir bağlantının varlığından bahsedilebilir. Ayrıca marka hakkına tecavüz oluşturmamak kaydıyla tescilli ticaret unvanının esaslı unsurunun alan adı olarak kullanılması durumu da kullanıcı ile işaret arasında meşru bir bağlantı olduğu şeklinde değerlendirilmektedir.[58] Özetlemek gerekirse, markanın internette kullanımına yönelik bir uyuşmazlık çıkması halinde ilgili hüküm uyarınca öncelikle kullanıcının kullanma hakkı yahut meşru bağlantısı olup olmadığı ve marka olarak kullanılması mümkün işaretin ticari alanda marka olarak kullanıldığının tespit edilmesi; ardından marka ihlaline yönelik unsurların oluşup oluşmadığının değerlendirilmesi gerekir. Bir başka deyişle, alan adı, yönlendirici kod yahut anahtar sözcük faaliyetleri gibi işlemlerde marka hakkına tecavüz olmadığı sürece işaretler serbestçe kullanılabilecektir.[59]

Diğer taraftan, marka ile iltibas oluşturabilecek türden alan adı kullanılması marka hakkına tecavüz olarak değerlendirilecektir. Bu durumda markanın sahip olduğu etkiden dürüstlük kuralına aykırı ve aldatıcı şekilde yararlanılması yani haksız rekabet söz konusu olacaktır. Sadece markanın değil, benzer şekilde unvan, işletme adı

---

[57] Kemal Şenocak, "Tescilli Markanın Aynısının veya Benzerinin Alan Adı (Domain Name) Olarak Kullanılması Suretiyle Marka Hakkının İhlali." *Banka ve Ticaret Hukuku Dergisi* 25, no. 3 (2009): 89.

[58] Uğur Çolak, *Türk Marka Hukuku* (İstanbul: XII Levha, 2012), 581.

[59] Eser Rüzgar, *Marka Hakkının İnternet Reklamcılığı Yoluyla İhlali ve Sorumluluk Rejimi* (İstanbul: XII Levha, 2013), 67 – 69.

gibi ayırt edici ad ve işaretlerle karışıklığa neden olabilecek haksız alan adı kullanımlarında da haksız rekabet gündeme gelecektir. Gerek Türk Ticaret Kanunu (TTK) 54üncü maddesi gereği haksız rekabet, gerekse Türk Borçlar Kanunu (TBK) 49uncu maddesi gereği haksız fiil söz konusu olacak ve zarara uğrayan kişi dilediği hükme dayanabilecektir.[60] Ancak TTK 54 ve devamı kapsamında zarar görme tehlikesinin varlığı yeterli iken, TBK 49uncu maddesi için TBK 50nci maddesi dolayısıyla zarar verenin kusurunun ve zararın ispatı gerekmektedir. Konuyla ilgili haksız rekabete yönelik 11 HD. 2007/7270 E, 2008/9135 K. sayılı Yargıtay kararı örnek verilebilir. Bu kararda; 'Erkoç Mühendislik-Erol Koç' ticaret unvanının ve 'şekil' ve 'erkoç' markalarının sahibinin, www.erkocmuh.info ve www.erkocmuhendislik.com şeklinde alan adları ile iki ayrı web sitesi kuran davalının bu web sayfalarında ticari faaliyetler yürütmesinin tüketicinin yanıltılmasına neden olarak marka hakkına tecavüz olduğunu ileri sürdüğü davada mahkeme, davalının söz konusu alan adlarının, davacının tescilli ticaret unvanı ve markaları ile iltibas oluşturacak şekilde olduğuna ve haksız rekabet ve marka hakkına tecavüz bulunduğuna ve bu nedenle haksız rekabet ve marka hakkına tecavüzün durdurulması ile men'ine ve manevi tazminata hükmetmiş, Yargıtay'ca mahkeme kararı onanmıştır.[61]

VII. SONUÇ

1990lı yıllarda dünya genelinde 1 milyondan az kullanıcısı olan internetin yalnızca on yıl içerisinde kullanıcı sayısı 100 milyonun üzerine ulaştığı düşünüldüğünde[62] düzenlemelerin 90lı yılların sonuna doğru niçin hız kazandığı sorusu, online ortamın ekonomik değerindeki devasa büyüme dolayısıyla cevaplanabilir. Özellikle günümüzde bir işletmenin markasının alan adı olarak kaydedilmesi durumunda interneti ticaret için kullanma yeteneğinin, tüketicilere markası üzerinden ulaşabilme hakkının ve elektronik ticaretin büyümesinin engel-

60 Mehmet Emin Bilge, *Ticari Ad ve İşaretler Arasında Karıştırılma Tehlikesi* (Ankara: Yetkin, 2014), 37.

61 Yar. 11 HD, E.2007/7270, K. 2008/9135.

62 Springer, "Master of the Domain," 324.

lenmiş olacağı göz önüne alındığında, *cybersquatting* olayının ne kadar ciddi bir tehdit oluşturmakta olduğu daha iyi anlaşılabilir.[63] Nitekim markaların alan adı olarak başkalarınca kullanılması; marka hukukunun koruduğu temel işlevlerden olan 'tüketicinin alışveriş maliyetini düşürme' ve 'neyi satın alacağına özgürce karar verebilme' işlevlerine karşı tehdit oluşturmaktadır. Ticari markalar, bir alıcıya, o markayı haiz ürünün kalitesini, geçmişini ve güvenilirliğini hızlı ve kolay bir şekilde tespit etme imkânı sağlar. Öyle ki bir tüketici, belirli bir markayı taşıyan X öğesini satın alıp bu satın alımdan fayda sağladıysa, bu tüketici gelecekte aynı işareti taşıyan Y ögesinin satın alınmasında rahat hissedecektir. Bu durum markaların hak sahibi olmayanlarca alan adı olarak kullanılmasına yönelik üzerinde durulması gereken önemli bir konudur. Zira alan adı kayıtlarında prosedürün herhangi bir belge ibare etmeksizin, alan adında kullanılmak istenen ibareler üzerinde bir meşru bağ yahut hak olup olmadığı sorgulanmaksızın 'önce başvuran alan adını alır' şeklinde uygulanması, başkasına ait markanın doğrudan ya da benzer bir şekilde alan adı olarak kaydedilerek markanın itibarı üzerinden marka hakkı sahibine zarar verdiği gibi ayrıca müşteriyi yanıltarak aslında o markaya ait olmayan web sitesi üzerinden o markaya duyduğu güven ile alışveriş yapmasını ve böylece yanılgı dolayısıyla aslında yapmak istemediği bir ticari işlemde bulunmasına neden olarak tüketiciye zarar vermekte ve tüketicinin korunması kurallarına da aykırılık oluşturmaktadır.[64]

ICANN'ın 'ilk başvuran alan adını tescil ettirir' şeklindeki uygulaması da birçok *cybersquatting* olayına neden olmaktadır. Bu şekilde gerek marka sahiplerinin gerekse tüketicilerin haklarının korunmasına yönelik hem uluslararası kuruluşların sunduğu raporlar ve anlaşmalar hem de ülkelerin ulusal hukuklarında getirdikleri düzenlemeler önem arz etmekle birlikte tüm dünyadan erişime açık bir yapıyı haiz olan internet üzerinde *cybersquatting* işlemlerinin önlenerek marka sahiplerinin ve tüketicilerin haklarını korumaya yönelik gerekli ve yeterli adımlar henüz atılmış bulunmamaktadır.

---

63 Springer, "Master of the Domain," 324.

64 Springer, "Master of the Domain," 325.

KAYNAKÇA

Bal, Nurullah. "İnternet Alan Adları ve İnternet Alan Adı Uyuşmazlıklarının Tahkim Yoluyla Çözümlenmesi." *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17, no. 1-2 (2013): 315 - 351.

Bilge, Mehmet Emin. *Ticari Ad ve İşaretler Arasında Karıştırılma Tehlikesi.* Ankara: Yetkin, 2014.

Chandler, Daniel ve Rod Munday. *A Dictionary of Social Media.* Oxford University Press, 2016.

Chen, Wei-erh. "Optimizing Online Trademark Protections Given the Proliferation of Generic Top Level Domains." *The Journal of Corporation Law* 38, no. 3 (2013): 586 - 606.

Clarke, Osborne. *A Practical Guide to E-commerce and Internet Law.* London: ICSA Publishing, 2002.

Çolak, Uğur. *Türk Marka Hukuku.* İstanbul: XII Levha, 2012.

Davison, Mark, Ann Monotti, ve Leanne Wiseman. *Australian Intellectual Property Law.* Melbourne: Cambridge University Press, 2015.

Drew, Ian, ve Elizabeth Godfrey. "When will Domain Names Be Considered "Use" of a Trade Mark?" *Davies Collison Cave Intellectual Property.* 10 Aralık 2010. Erişim tarihi Nisan 28, 2017. http://www.davies.com.au/ip-news/when-will-domain-names-be-considered-use-of-a-trade-mark.

Federal Court of Australia. "Mantra Group Pty Ltd v Tailly Pty Ltd (No 2) (includes Corrigendum dated 31 August 2010) [2010] FCA 291 (26 March 2010)." Erişim tarihi Şubat 7, 2019. http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2010/291.html?stem=0&synonyms=0&query=Mantra%20Group%20Pty%20Ltd.

—. "Sports Warehouse, Inc v Fry Consulting Pty Ltd [2010] FCA 664 (25 June 2010)." Erişim tarihi Şubat 7, 2019. http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2010/664.html?query=.

Gaming Law Review. "Ellerman Investments Ltd and Another v. C-Vanci and Another Chancery Division." (Mary Ann Liebert, Inc) 10, no. 5 (2006): 514 - 518.

Gençer, Mustafa. "Markanın İnternet Ortamında Alan Adı (Domain Name), Yönlendirici Kod (Metatag) veya Anahtar Sözcük (Keyword) Olarak Kullanılması Sonucu Oluşabilecek Marka İhlallerinin İncelenmesi." Uzmanlık Tezi, Ankara: T. C. Patent Enstitüsü Markalar Dairesi Başkanlığı, 2014.

Golinveaux, Jennifer. "What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?" *University of San Francisco Law Review* 33, no. 4 (1999): 641 - 672.

Janis, Mark D, ve Peter K Yu. "International and Comparative Aspects of Trademark Dilution." *Transnational Law & Contemporary Problems* 17, no. 3 (2008): 603 - 610.

Karadenizli, Başak. "Marka Tescilinde Ayırt Edicilik, Tanımlayıcılık ve Yanıltıcılık Değerlendirmelerinin Türkiye ve Yurt Dışındaki Uygulamaları ile Bunların Karşılaştırılması." Uzmanlık Tezi, Ankara: T.C. Türk Patent Enstitüsü Markalar Dairesi Başkanlığı, 2008.

King, Stacey H. "The "Law That It Deems Applicable": ICANN, Dispute Resolution, and the Problem of Cybersquatting." *Hastings Communications and Entertainment Law Journal* 22, no. 3 & 4 (1999 - 2000): 453 - 507.

Kırca, İsmail. "Tescilli Markanın Üçüncü Kişi Tarafından Alan Adı Olarak Kullanılması." *Prof. Dr. Ömer Teoman'a 55. Yaş Günü Armağanı* içinde, 527 - 544. İstanbul: Beta, 2002.

Lipton, Jackueline D. "Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy." *Wake Forest Law Review* 40, no. 4 (2005): 1361 - 1440.

Manzone, Ughetta. "Panavision International, L. P. v. Toeppen." *Berkeley Technology Law Journal* 13, no. 1 (1998): 249 - 264.

Martin, Neil L. "The Anticybersquatting Consumer Protection Act: Empowering Trademark Owners, but not the Last Word on Domain Name Disputes." *The Journal of Corporation Law* 25, no. 3 (2000): 591 - 611.

Morris, Michael. "Real Estate Marketing on the Internet: Using Registered Trade Marks Online." *Mondaq Business Briefing*, Şubat 2010. Erişim tarihi Şubat 03, 2019. http://www.mondaq.com/australia/ x/104392/ Trademark/ Real+Estate+Marketing+on+the+Internet+Using+ Registered+ Trade+Marks+Online

Murray, Andrew. *Information Technology Law.* New York: Oxford University Press, 2013.

O'Connor, Martin. "Australia: The Mantra Decision: Strata Titled Properties: Registered Trade Marks." *Mondaq Business Briefing*, Mayıs 2010. Erişim tarihi Şubat 03, 2019. http://www.mondaq.com/australia/x/99714/Trademark/The+Mantra+Decision+Strata+Titled+Properties+Registered+Trade+Marks.

Oğuz, Sefer. "İnternet Alan Adı (Domain Name) Haklarının Korunması." Doktora Tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2011.

Rüzgar, Eser. *Marka Hakkının İnternet Reklamcılığı Yoluyla İhlali ve Sorumluluk Rejimi.* İstanbul: XII Levha, 2013.

Soysal, Tamer. *İnternet Alan Adları Hukuku (Domain Name Law).* Ankara: Adalet Yayınevi, 2014.

Springer, Colby B. "Master of the Domain : a History of Domain Name Litigation and the Emergence of the Anticybersquatting Consumer Protection Act and Uniform Dispute Resolution Policy." *Santa Clara Computer and High-Technology Law Journal* 17, no. 2 (2001): 315 - 363.

Şanal, Osman. *Markanın Hükümsüzlüğü.* Ankara: Adalet Yayınevi, 2004.

Şarlak, Zeynep. "İnternet Alan Adının (Domain Name) Hukuki Niteliği ve Marka Hakkı Üzerindeki Etkisi." Yüksek Lisans Projesi, Ankara: T. C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Ticaret Hukuku) Anabilim Dalı, 2006.

Şenocak, Kemal. "Tescilli Markanın Aynısının veya Benzerinin Alan Adı (Domain Name) Olarak Kullanılması Suretiyle Marka Hakkının İhlali." *Banka ve Ticaret Hukuku Dergisi* 25, no. 3 (2009): 89 - 141.

Tahmassebi, Sam K. "Panavision International v. Toeppen." *The Journal of Contemporary Legal Issues* 12, no. 1 (2001): 513 - 518.

Uzunallı, Sevilay. *Markanın Korunmasının Kapsamı ve Tazminat Talebi.* Ankara: Adalet Yayınevi, 2012.

WIPO. "Final Report of the First WIPO Internet Domain Name Process." Erişim tarihi Şubat 03, 2019. https://www.wipo.int/amc/en/processes/process1/report/index.html.

Zorluoğlu, Ayça. "Alan Adlarında Kötü Niyet Kavramı." *Hacettepe Hukuk Fakültesi Dergisi* 2, no. 1 (2012): 67 - 84.

BRICKS AND CLICKS: ONLINE DISPUTE RESOLUTION MECHANISMS AND IMPLEMENTATION OF ONLINE ARBITRATION IN TURKEY FOR CROSS-BORDER BUSINESS TO CONSUMER E-COMMERCE DISPUTES

Çevrimiçi Uyuşmazlık Çözüm Yöntemleri ve Sınır Ötesi İşletmeden Tüketiciye Elektronik Ticaret Uyuşmazlıklarında Çevrimiçi Tahkimin Türkiye'de Uygulanması

Cemre Çise KADIOĞLU[*]

Abstract

The lack of effective legal remedies builds barriers before business to consumer (hereinafter B2C) electronic commerce. In this regard, online dispute resolution (hereinafter ODR) mechanisms remedy this need through offering alternative ways to craft a more reliable market by increasing the confidence of consumers to enter into cross-border electronic commerce. With this feature, ODR mechanisms accord Turkey valuable opportunities to attract more businesses and consumers. Particularly, within the ambit of arbitration, online arbitration may be more easily implemented in Turkey because the current arbitration regulations of the country satisfy the necessity international standards that are sought for efficient and efficacious arbitration procedure. There are, of course, some challenges to online arbitration, such as arbitrability, enforceability, and determining a *lex arbitri*. These issues mainly

[*] Georgetown Üniversitesi Hukuk Fakültesi Yüksek Lisans Öğrencisi, cemrekadioglu@gmail.com, ORCID: 0000-0002-9573-777X.

Makale Gönderim Tarihi: 08.01.2019

Makale Kabul Tarihi: 06.03.2019

arise out of courts' efforts to interpret laws in a way most favorable to consumers. As an initial step to promote online arbitration, arbitral institutions may incentivize this mechanism *via* their rules. Further, to broaden the scope of Turkish institutions' availability to cross-border users, negotiations for Turkey's accession to ODR platform provided within the European Union should be furthered.

Keywords: Online Dispute Resolution, Online Arbitration, Business to Consumer, Electronic Commerce, Cross-Border.

Öz

Tarafların başvurabilecekleri etkili hukuki yolun bulunmaması, işletmeden tüketiciye elektronik ticaretin gelişmesine engel olmaktadır. Çevrimiçi uyuşmazlık çözüm yolları tüketicilerin sınır ötesi elektronik ticarete olan güvenlerini artırarak daha güvenilir bir pazar oluşturmak adına seçenek sunmaktadır. Çevrimiçi uyuşmazlık çözüm yollarının benimsenmesi, dünyada en çok internet kullanıcısının olduğu ülkelerden biri olan Türkiye'nin daha çok işletme ve tüketiciyi çekmesini sağlayabilecektir. Diğer çevrimiçi uyuşmazlık çözüm yollarına kıyasla Türkiye'de çevrimiçi tahkimin uygulanması tahkim kanunlarının uluslararası standartlara uygun olması; diğer yöntemlerin benimsenmesini zorlaştıran kültürel ve teknolojik engellerin olması nedeniyle daha kolay olacaktır. Çevrimiçi tahkimin önünde de tahkime elverişlilik, tenfiz ve tahkim yerinin belirlenmesi gibi sorunlar bulunmaktadır. Bu sorunlar mahkemelerin kanunları tüketici yararına yorumlamaya çalışmalarından kaynaklanmaktadır. Çevrimiçi tahkim, tüketici yanlısı bir yöntem olduğundan Türk mahkemelerinin yorumlarını ve bakış açılarını değiştirmelerini gerektirmektedir. Bu uyuşmazlık çözüm yöntemini teşvik etmek için tahkim kuruluşları kendi kuralları uyarınca çevrimiçi tahkimi destekleyebilirler. Sınır ötesinde bulunan tüketicilerin bu kurumlara erişimini artırmak için Türkiye'nin Avrupa Birliği'nin sağladığı çevrimiçi uyuşmazlık çözüm platformuna katılımını sağlamak yönünde müzakerelerin ilerletilmesi gerekmektedir.

Anahtar Kelimeler: Çevrimiçi Uyuşmazlık Çözüm Yöntemleri, Çevrimiçi Tahkim, İşletmeden Tüketiciye, Elektronik Ticaret, Sınır Ötesi.

I. INTRODUCTION

High accessibility to the internet, availability of more options for every budget, and its easiness in modern lifestyle increase the number of individuals engaging in electronic commerce (hereinafter e-commerce). Various goods and services for architecture, medicine, education, justice, travel, or accounting are purchased and supplied through the internet. For instance, a student may order a pair of sneakers, enroll in an online certificate program for vocational training, or book a flight for a winter break. From a different perspective, however, the student's engagement in these transactions carry a concomitant risk for her, such never getting the sneakers or getting the wrong ones, not benefitting from the online classes. When she efforts to reach out the customer service, they may never respond. At the end, she might be destined to file a lawsuit or have recourse to alternative dispute resolution.

Things get more complicated when the company and the student are located in different countries. Now, she has to deal with traveling or hiring an attorney in that country. Language barriers, territoriality, jurisdictional questions, and the evidentiary matters will also be added to the increased cost and duration. At the end, the absence of effective legal remedies that would overcome these obstacles builds barriers around international trade and obstructs its harmony. To make the market more reliable and to increase the confidence of the consumers to enter into cross-border e-commerce, an effective dispute resolution mechanism becomes a necessity.[1]

ODR refers to the alternative dispute resolution (hereinafter ADR) methods that are facilitated by technology and conducted through the internet.[2] ODR amalgamates the advantages of out-of-the-court resolution mechanisms with technology and accordingly

---

1 Veijo Heiskanen, "Dispute Resolution in International Electronic Commerce," *Journal of International Arbitration* 16, no. 3 (1999): 38.

2 Maria Mercedes Albornoz, and Nuria González Martin, "Feasibility Analysis of Online Dispute Resolution in Developing Countries," *University of Miami Inter-American Law Review* 44, no. 1 (2012): 46.

provides a quick and effective remedy for the disputes that could arise out of international e-commerce.[3] ADR has gained significant importance, especially in international commercial disputes as it provides autonomy, flexibility, expertise, and confidentiality for businesses. Despite all the advantages of it, ADR does not respond to the needs of consumer disputes, which are generally in small amounts. In this respect, ODR has potential not only to eliminate the relatively high legal costs of cross-border ADR and litigation,[4] but also to minimize the legal risks. Particularly, in terms of e-commerce disputes, which are generally cross-border in nature, ODR is far more reasonable and better adaptable.[5] ODR is more suitable for B2C disputes. As far as business-to-business (hereinafter B2B) transactions are concerned, ODR may not be a viable option because businesses prioritize confidentiality and the preservation of their trade secrets. Thus, parties to B2B disputes predominantly prefer the physical aspects of conventional methods in terms of evidence-taking, witnesses, and holding hearings.

This article examines how ODR may be implemented, particularly for B2C disputes in Turkey. Turkey is an emerging market for international e-commerce platforms with its high internet penetration[6] and its highest mobile usage rates in the world.[7] An ODR mechanism that effectively integrates with national law would supplement international commerce as developed countries could attract more customers from Turkey. At the same time, with the increased reliability of e-commerce, Turkey may invite more businesses and foreign consumers. The article demonstrates that among other ODR mechanisms,

---

3 Heiskanen, "Dispute Resolution," 38.

4 Heiskanen, "Dispute Resolution," 39.

5 Albornoz, and Martin, "Feasibility Analysis," 48.

6 The rate of internet penetration in Turkey is 46.3% as of December 2013, the world average is 54.9%. "Usage and Population Statistics," Internet World Stats, accessed December 11, 2018, https://www.internetworldstats.com/top20.htm.

7 Turkey is the eighteenth out of the top twenty countries with highest number of internet users as of December 31, 2017. The number of internet users in Turkey is approximately 56 million. Internet World Stats, "Usage and Population Statistics."

Turkey should give more attention to online arbitration because it may be implemented more easily compared to other ADR mechanisms in terms of cultural and technological challenges, and existing arbitration laws that are aligned with international regulations.

Summarily, this paper, first, discusses different types of ODR mechanisms and suggests that online arbitration is the most suitable method to resolve cross-border B2C disputes, second, articulates upon the operation of online arbitration works, third, discusses challenges to online arbitration, and, finally, concludes by demonstrating how online arbitration may be the best fit for B2C disputes under Turkish law.

II. TYPES of ODR MECHANISMS

ODR is a post-dispute resolution method that consists of mechanisms using either automated systems or technology-assisted mechanisms.[8] Automated systems are the online platforms that deal with monetary disputes with the assistance of technology. Automated systems help parties save money and circumvent complex jurisdictional problems, while demanding high-level technological investment and raising questions regarding cybersecurity. Furthermore, automated systems do not address non-monetary claims.[9] Addi-

---

8 E-commerce disputes may be prevented before they arise by online dispute prevention mechanisms. This article does not address pre-dispute methods for avoiding disputes. See Suatip Yuthayotin, *Access to Justice in Transnational B2C E-Commerce: A Multidimensional Analysis of Consumer Protection Mechanisms* (Switzerland: Springer International Publishing, 2015), 229 for more information on online prevention.

9 Mohamad Salahudine Abdel Wahab, "The Global Information Society and Online Dispute Resolution: A New Dawn for Dispute Resolution," *Journal of International Arbitration* 21, no.2 (2004): 150. Artificial intelligence eliminates the human involvement. Platforms offer various solutions. For instance, the parties bid and try to find a common ground (*e.g.* Cybersettle, MARS, Intersettle, SmartSettle, Dispute Manager, Esettle.co.uk, WeCanSettle, and SettleOnline); the platform offers optimization programs that proposes solutions and mathematically provides the optimum one after it is exchanged between parties (*e.g.* Computer Aided Negotiation-Web International Network (CAN-WIN) offered by the Resolution Forum) or the platform works through solution sets where the parties answer a set of questions. The program provides possible solutions and parties may agree on that. The database evolves with each dispute entered into the system (*e.g.* SquareTrade used by Ebay).

tionally, it should not be disregarded that a dispute that is not resolved by a human adds a psychological barrier between physically-distant parties.[10] At the outset, it may be more plausible for Turkey to espouse legally and technically more available technology-assisted mechanisms, rather than embracing automated systems as part of its implementation of ODR.

Unlike automated systems, in technology-assisted mechanisms, the human factor is not eliminated. The parties and neutral, who is the person deciding on the dispute, are actively involved in the dispute resolution process. The technology is used to provide adequate and appropriate means of communication.[11] The procedures follow the traditional rules to a larger extent. Some examples of technology-assisted mechanisms are as follows: online negotiation, mediation, arbitration, mediation-arbitration ("Med-Arb"), online ombudsmen proceedings, and cyber courts.

Technology-assisted mechanisms consensually bring parties together. Online negotiation and mediation are preferred as they enhance party autonomy and arrive at conclusions that are satisfactory for both parties.[12] These ODR methods, however, ineffective because they are enforced as regular contracts or settlement agreements and their outcomes are not final and binding. This adds an additional step if the parties do not voluntarily comply with the results. In the face of these downsides of online negotiation and mediation, online arbitration becomes the crown jewel of the ODR methods.

Online arbitration makes the dispute resolution process more operative by eliminating territoriality questions of the courts and conforming to the global character of the cyberspace.[13] Not only

---

[10] Joseph W. Goodman, "The Pros and Cons of Online Dispute Resolution: An Assessment of Cyber-Mediation Websites," *Duke Law and Technology Review* 4 (2003): 11.

[11] Wahab, "The Global Information Society," 147.

[12] Dafna Lavi, "Three is not a Crowd: Online Mediation-Arbitration in Business to Consumer Internet Disputes," *University of Pennsylvania Journal of International Law* 37, no. 3 (2016): 893.

[13] Gabrielle Kaufmann-Kohler, Thomas Schultz *Online Dispute Resolution: Challenges for Contemporary Justice*, (The Hague: Kluwer Law International, 2004), 27.

does it promote efficiency and efficacy, but also overrides automated systems by not taking human element of the dispute resolution process out of the equation.[14] Finally, the escalating number of institutions that offer online arbitration leads to infer that online arbitration is gaining ground among the users.[15]

The pioneers in ODR arena, such as Katsh and Rifkin, state that online arbitration is not yet the best ODR mechanism mainly because of the legal framework and formalities that should be followed.[16] Online arbitration responds to these criticisms by introducing an instrument called "non-binding online arbitration" that brings arbitration and flexibility of non-adjudicative procedures together.[17] Non-binding online arbitration is more frequently preferred over binding online arbitration as it is not subject to strict procedural requirements.[18] Although this sounds paradoxical, non-binding online arbitration may indicate either referral of a dispute to arbitration or outcome of the process.[19] Regardless of its legal classification, non-binding online arbitration is adopted by institutions and users.[20] Depending on the nature of the outcome, it can be enforced as either an arbitral award or a settlement agreement.

Binding online arbitration is preferred to have a certain level of the procedural framework; increased formality enables predictability.[21] The legal certainty and the predictability increase the trust in

---

14 Ayelet Sela, "Can Computers Be Fair: How Automated and Human-Powered Online Dispute Resolution Affect Procedural Justice in Mediation and Arbitration," *Ohio State Journal on Dispute Resolution* 33, no. 1 (2018): 115; *See* Mohammed Salahudine Abdel Wahab, *ODR and E-arbitration, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution* (Eleven International Publishing, 2012), 390.

15 Wahab, "The Global Information Society," 153.

16 Ethan Katsh, and Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace* (San Francisco (CA): Jossey-Bass Publishers, 2001), 56.

17 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 33.

18 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 153.

19 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 154.

20 Uniform Domain-Name Dispute-Resolution Policy and Chartered Institute of Arbitrators offer non-binding arbitration systems with different adjustments.

21 *See* Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 82.

the system and attracts more consumers.[22] Either binding or non-binding, online arbitration is attractive for the parties who would like to tailor the procedure and the outcome.

III. THE FUNCTIONING OF ONLINE ARBITRATION

There are different stakeholders of ODR, such as governments, businesses, consumer organizations, and dispute resolution organizations. Their motives behind supporting ODR differ. Governments would like to promote access to justice and e-commerce and to decrease burden on the courts; businesses would like to build up consumer confidence by implementing such mechanisms that expedite dispute resolution; consumer organizations want ODR to enforce consumer rights, and, finally, dispute resolution institutions consider ODR as a new service to provide in the competitive market.[23]

Online arbitration is facilitated by private and public institutions that provide platforms for the parties. United Nations Commission on International Trade Law (UNCITRAL) Technical Notes on Online Dispute Resolution (Technical Notes) provides non-binding guidelines for ODR stating that ODR services should be provided by a "technology-based intermediary" and no *ad hoc* basis should be involved.[24]

There are several government initiatives, such as those in Mexico,[25] Canada,[26] and the Republic of Korea,[27] that provide ODR me-

---

[22] *See* Yuthayotin, *Access to Justice in Transnational B2C E-Commerce,* 22-25.

[23] Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 83.

[24] "UNCITRAL Technical Notes on Online Dispute Resolution (2017), Section V, para.26", accessed December 11, 2018, http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf.

[25] *See generally* Gustavo Alcocer Lugo, and, Abraham Diaz Arceo, "Digital Business in Mexico: Overview," *Thomson Reuters Practical Law,* accessed November 3, 2018, https://uk.practicallaw.thomsonreuters.com/w-012-0309?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1. ("The Federal Bureau of Consumer Protection (PROFECO) offers an ODR service (CONCILIANET), but suppliers of goods and services must have in place an existing agreement with PROFECO to allow their customers to use the ODR service. So far, only a limited number of companies have executed the agreement with PROFECO.").

chanisms. The advantages of government involvement in ODR is dubious. On the one end of the spectrum, the public sector may not meet the high-level sophistication of the technologies, but, on the other end of the spectrum, private providers may hamper the justice as they may have "legal, privacy, budgetary, accessibility, and logistical demands."[28] Most importantly, these national mechanisms are not suitable for cross-border disputes.[29]

On the private side, there is a limited number of institutions that offer online arbitration. For instance, China International Economic and Trade Arbitration Commission (CIETAC) adopted Online Arbitration Rules in 2009 and these Rules became effective in 2015.[30] These Rules are applicable to the resolution of e-commerce disputes. Online Arbitration Rules of Russian Arbitration Association (RAA) became effective in 2015 to facilitate independent, impartial, and efficient resolution of commercial disputes arising out of contractual and non-contractual relations, by electronic means of transfer and storage of information.[31]

The regional organizations developed an interest in the area of ODR as well. The primary rationale behind their interest is to accord consumers protection. Organization of American States (OAS) considers establishing regional ODR platform with the rules aiming to regulate procedures, including online arbitration, and drafted a model

---

26 *See* Shannon Salter, "Online Dispute Resolution and Justice System Integration: British Columbia's Civil Resolution Tribunal," *Windsor Yearbook of Access to Justice 34 (2017):* 112-129.

27 *See* E-Commerce Mediation Committee. E-Commerce Mediation Committee that is established under Chapter 6 of Framework Act on Electronic Documents and Transactions offers only mediation for disputes arising out of e-transaction or e-documents.

28 Salter, "Online Dispute Resolution," 128.

29 Yuthayotin, *Access to Justice in Transnational B2C E-Commerce,* 96.

30 "CIETAC Online Arbitration Rules, 2015", accessed December 11, 2018, http://bj.cietac.org/index/rules/4760665e7716e27f001.cms.

31 See generally Russian Arbitration Association (RAA), accessed November 3, 2018, https://arbitration.ru/en/. website_for reasons behind adopting online arbitration rules.

law/cooperative framework.[32] In 2016, Inter-American Juridical Committee of OAS adopted the resolution for the protection of consumers in cases of online disputes arising from cross-border transactions and decided to focus on mechanisms for online settlement of disputes.[33] Asia-Pacific Economic Cooperation (APEC) has a work plan to promote ODR to enhance e-commerce. Accordingly, APEC aims to continue promoting harmonization of the pertinent laws with respect to ODR through using existing international instruments, such as the New York Convention on Recognition and Enforcement of Foreign Arbitral Awards (hereinafter the New York Convention),[34] UNCITRAL Model Law on International Commercial Arbitration (UNCITRAL Model Law),[35] UNCITRAL Model Law on Electronic Commerce (E-commerce Model Law),[36] UN Convention on the Use of Electronic Communication in International Contracts (E-communication Convention),[37] and UN Convention on Contracts for the International Sale of Goods

---

[32] Organization of American States, "Draft Electronic Resolution of Cross-Border E-Commerce Consumer Disputes," accessed November 3, 2018, http://www.oas.org/dil/esp/CIDIPVII_proteccion_al_consumidor_united_states_guia_legislativa_anexo_A.pdf.

[33] The Inter-American Juridical Committee Res. CJI/ RES. 227 (LXXXIX-O/16) (Oct. 3-14, 2016). See generally Rule, Colin, Vikki Rogers, and Louis Del. Duca "Designing Global Consumer Online Dispute Resolution (ODR) System for Cross-Border Small Value-High Volume Claims – OAS Developments." *Uniform Commercial Code Law Journal* 42 (2010): 221-264 for analysis of the proposed solution by the OAS.

[34] "Convention on the Recognition and Enforcement of Foreign Arbitral Awards, 1958," UNCITRAL, accessed December 11, 2018, **http://www.uncitral.org/uncitral/**en/uncitral_texts/arbitration/NYConvention.html.

[35] "Model Law on International Commercial Arbitration 2006," UNCITRAL, accessed December 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html.

[36] "Model Law on Electronic Commerce 1996," UNCITRAL, accessed December 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html.

[37] "Convention on the Use of Electronic Communication in International Contracts, 2005," UN, accessed December 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

(CISG).[38] Finally, UNCITRAL's Technical Notes on Online Dispute Resolution of 2016 lays out the principles that may be followed by States and other stakeholders while designing and implementing ODR systems for cross-border commercial transactions.[39]

The EU established ODR platform in January 2016 with the intention to be an interactive and user-friendly website that is open to any customer or trader in the EU and is available in all EU official languages for free of charge.[40] The platform brings consumers and businesses together and offers consumers to choose an arbitration provider from a list to resolve their dispute between parties from EU member states, and Lichtenstein, Iceland and Norway.[41] This system also necessitates all European businesses to integrate online arbitration clause into their contracts.[42]

Government initiatives at a national level do not respond to the complications arising out of cross-border disputes, such as increased costs, duration, and communication disturbances due to the long distance.[43] It is difficult to establish a global ODR system considering

---

38 "Convention on Contracts for the International Sale of Goods, 1980," UN, accessed December 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/ sale_goods/1980CISG.html

39 "UNCITRAL Technical Notes on Online Dispute Resolution 2016."

40 Regulation 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), O.J. (L 304/1); Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests O.J. (L 304/1).

41 See "Online Dispute Resolution," European Commission, accessed November 11, 2018, https://ec.europa.eu/consumers/odr/main/?event=main.home2.show website to observe how the platform works.

42 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests O.J. (L 304/1) para 30. ("In order to ensure broad consumer awareness of the existence of the ODR platform, traders established within the Union engaging in online sales or service contracts should provide, on their websites, an electronic link to the ODR platform.").

43 *See* Yuthayotin, *Access to Justice in Transnational B2C E-Commerce,* 97; *See* Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 71.

the technological gaps amongst jurisdictions. The regional agreements and partnerships may be the solution for promoting ODR as they resolve multinational disputes and accommodate the advanced technology that is needed for the proper operation of ODR.

Striking a balance between consumers' right to access to justice and courts' workload is a difficult task to accomplish. As a step towards striking this balance, Turkey initiated an online platform for applications lodged for consumer to consumer arbitration in 2018.[44] Consumers upload their documents to system, agree on the procedure and applicable law, and notification process.[45] Turkey's this attempt to simplify the resolution of the disputes between consumers illustrate its volition to promote access to justice while simultaneously relieving courts from their heavy workload.[46]

The participation in the EU's ODR platform may be another plausible step for Turkey in course of achieving the aforementioned goals of the country. Turkey is a signatory of the EU's Customs Union Agreement, which is in effect since 1995.[47] The agreement provides a free circulation of goods. Turkey and the EU have been seeking ways to improve bilateral relations. In this respect, there have been efforts to facilitate e-commerce and introduce a digital agenda that establishes free movement of digital data.[48] To fulfill these efforts, focusing on

---

[44] T.C. Gumruk ve Ticaret Bakanligi Karar No: 77002794-405 Konu: Tuketici Hakem Heyetlerinin Yeniden Yapilandirilmasi, 9.07.2018 [Republic of Turkey Ministry of Customs and Commerce Decree No: 77002794-405 Subject: Restructuring Consumer Arbitral Tribunals, July 9, 2018][Restructuring Decree].

[45] The consumers can file their complaints through the e-government system.

[46] Uyap Bilisim Sistemi, accessed December 13, 2018, http://istatistikler.uyap.gov.tr/. Restructuring Decree. There are approximately two million new civil law disputes before the courts each year. In 2017, 590,736 and in the first half of 2018 272,933 small-value consumer disputes were brought before the consumer arbitral tribunals.

[47] Decision No 1/95 of the EC-Turkey Association Council of 22 December 1995 on Implementing the Final Phase of the Customs Union O.J. (L 35).

[48] Opinion 2017/C 075/22 of the European Economic and Social Committee on Enhancement of EU-Turkey Bilateral Trade Relations and Modernization of the Customs Union O.J. (C 75) 1.12.

ODR mechanisms and increasing consumers' and businesses' confidence in these mechanisms may be a good place to start. This may be done by Turkey's inclusion in EU's ODR platform. For this inclusion, as a first step, Turkey is required to appoint an institution for ODR in its jurisdiction. Turkey's newly established Istanbul Arbitration Center (hereinafter ISTAC) may be a possible candidate in this regard and the existing arbitration regulations will be sufficient until the institution or the government finds it necessary to reform the rules and the legislation or incorporate online arbitration rules.

IV. CHALLENGES TO ONLINE ARBITRATION

The challenges to online arbitration could be cultural, technological or regulatory. For instance, in Middle Easterner or Asian countries that represent collectivist cultures, the process is expected to be more relationship-based compared to individualist countries like the US.[49] This puts emphasis on the importance of the human involvement in online arbitration within the framework of Turkey. The technological challenges are related to information and communication technologies that the platforms should provide assistance to the procedure. This article focuses on the main regulatory challenges that may come up regarding online arbitration in Turkey, leaving other categories aside for further research.

A. Arbitrability of E-commerce Disputes

Arbitration is a dispute resolution mechanism that predominantly revolves around freedom of contract. Accordingly, arbitration does not come alive unless parties consent to submit their dispute to arbitration. This prerequisite naturally exists for online arbitration as well. As a general rule, the parties may agree on arbitration before or after the occurrence of the dispute as a separate contract or in a clause integrated

[49] Daniel Rainey, *ODR and Culture, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*, eds., Mohammed Salahudine Abdel Wahab et al. eds. (Eleven International Publishing, 2012), 189.

into the main agreement. In practice, arbitration agreements are most frequently concluded as a clause of main agreement and before any dispute arises.[50] In e-commerce disputes, while arbitration agreements that are concluded after the dispute are generally allowed, pre-dispute arbitration agreements are greeted with suspicion as they impact the arbitrability of the dispute under different national laws.[51]

While in some jurisdictions, such as the United States, the United Kingdom, Germany, Portugal, and Spain, consumer disputes are arbitrable, in some other jurisdictions, such as Italy, Finland, and Switzerland,[52] national laws do not allow consumer disputes to be submitted to arbitration for the sake of protecting the interests of consumers in the face of stronger adversaries. Whilst the European Union countries have different approaches, under the European Council Directive on Unfair Terms in Consumer Contracts, the pre-dispute arbitration agreements may be considered unfair[53] due to the possibility that a consumer is coerced to enter into the arbitration agreement. Under Turkish law, the status of the pre-dispute arbitration agreements is debatable.[54]

Under Turkish law, non-arbitrable issues are broadly defined as the "issues that are not at parties' disposal."[55] As far as the arbitrability of consumer disputes is concerned under Turkish law, the Tur-

---

50 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 173.

51 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 172.

52 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 171.

53 Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts O.J. (L95/29) para Q of the annex; Contra De Boisséson, Matthieu, and Thomas Clay. "Recent Developments in Arbitration in Civil Law Countries." *International Arbitration Law Review* 1 (1998): 151 citing resolution of European Parliament encouraging resolution of consumer disputes by arbitration.

54 Tuketici Sozlesmelerindeki Haksiz Sartlar Hakkinda Yonetmelik [Regulation on Unfair Terms in Consumer Contracts], Resmi Gazete [RG] [Official Gazette] 29033, Jan. 17, 2014 Annex 1, para. 1(n). Parties cannot agree on going to an arbitration other than mandatory arbitration in their contract before the dispute. Such provisions are considered as unfair terms.

55 6100 Hukuk Muhakemeleri Kanunu[Code of Civil Procedure], Art. 408, 4686 Milletlerarası Tahkim Kanunu [MTK] [Code of International Arbitration], Art.1, para.4. Disputes that are not subject to parties' discretion are non-arbitrable.

kish Court of Appeals held that consumer disputes are related to public policy; therefore, parties cannot freely submit to the arbitration.[56] On the other hand, some of the ADR mechanisms are explicitly accepted as a viable means to resolve consumer disputes. For instance, mediation is defined as a mechanism that the parties may opt for resolution of disputes that are on their disposal.[57] It is argued that arbitration should not be treated any differently if a consumer can freely submit its case to any other ADR method.[58] It should not be forgotten that, as a cost and time efficient method, online arbitration is a more convenient solution than court litigation for the consumers.

In light of these advantages, it is suggested that the concept of arbitrability should be interpreted in a broader context by Turkish courts and consumer disputes should be deemed to be arbitrable. Here, it should also be noted that judgments of courts are only binding for the parties. There is no *stari decisio* under Turkish legal system. They may constitute a persuasive authority, but the courts are

---

[56] Yar. 13. HD, E. 2008/6195, K. 2008/12026, 20.10.2008 [13th Civil Chamber of Court of Appeals, Application No 2008/6195, Decision No 2008/12026, Oct. 20, 2008]. Consumer claims under certain amount is subject to "mandatory arbitration" that is resolved before a tribunal composed of lawyer and non-lawyer members. Parties do not have autonomy and do not decide on procedure or applicable law. Claims above the threshold is resolved by courts specialized in consumer disputes. Here, the Court of Appeals reasons that because the jurisdiction of mandatory tribunals are bestowed by law, parties' voluntary arbitration agreement is against public policy. The legal status of consumer arbitration is ambiguous. The procedure is *sui generis* and cannot be categorized as ADR or litigation. Yar. 13. HD. 2008/3492, K. 2008/11120, 25.09.2008 [13th Civil Chamber of Court of Appeals, Application No 2008/3492, Decision No 2008/11120, Sept. 25, 2008]. In this case, the Court of Appeals held the arbitration agreement between a consumer and tourism agency invalid for the public policy concerns.

[57] 6325 Hukuk Uyusmazlıklarında Arabuluculuk Kanunu [Code of Mediation in Law Civil Disputes], Art. 1, para. 2.

[58] Yesilova, Bilgehan. "6502 sayılı Yeni Tuketicinin Korunmasi Hakkinda Kanun'a Gore Tuketici Uyusmazliklarinin Çozumu Usulu ve Yargilama Kurallari [Resolution Procedure and Rules for Consumer Disputes under the Code of Protection of Consumer numbered 6502]." *Terazi Hukuk Dergisi* 9 (2014): 118.

not obliged to embrace rationale of adopted by another court.[59] This allows courts to embrace an innovative role and enforce online arbitration agreements until the statutes are amended and recognizes the arbitrability of consumer disputes.

B. Online Arbitration Fees

Upon agreeing on submitting their dispute to arbitration, parties should figure out how fees will be dealt by the platform. It is important to eliminate obstacles originating from fee to increase user-friendliness and popularity of online arbitration. There are different mechanisms to finance online arbitration. Both parties may bear the costs (bilateral), only one party, which is generally the business, may bear the costs (unilateral),[60] or the process may be financed *via* public funds.

Bilateral funding would discourage consumers to bring their small claims. But, if the quantum of claims is medium to large, bilateral funding would also prevent frivolous claims.[61] The most common fee allocation model that is adopted for B2C commerce is the unilateral model.[62] This model provides that a business party bears the full costs. The business can make annual contributions to the institution or pay for each case individually. This may create a risk

---

[59] *See generally* 2797 Code of Court of Appeals [Yargıtay Kanunu]. A chamber should follow the same precedence. If the court wish to rule otherwise creating conflict with the precedence, the General Assembly of the Civil Chamber [Hukuk Genel Kurulu] shall decide. The conflicting decisions between the chambers are resolved by the General Assembly on the Unification of Judgements [Ictihadi Birlestirme Kurulu]. Its decisions have the same effect as a law. There is no unified judgement on the arbitrability of the consumer disputes.

[60] Unconventionally, CIETAC Online Arbitration Rules requires small fee to be paid by the claimant that is generally the consumer.

[61] Pablo Cortés, *Online Dispute Resolution for Consumers, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*, Mohammed Salahudine Abdel Wahab et al. eds. (Eleven International Publishing, 2012), 145.

[62] Karim Benyekhlef, "Online Dispute Resolution," *Lex Electronica* 10, no. 2 (2005): 82; Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 66.

of bias in favor of the businesses that finance the proceedings and may lead potential consumers, who are inclined to submit their dispute to online arbitration, to have recourse to litigation.[63] In this respect, it is important to promote transparency to ensure impartiality and neutrality.[64] As an external financing, public funds may be transferred to online arbitration platforms. This model will probably reduce institutional partiality concerns and yet, will put extra pressure upon texpayers.[65] Online arbitration providers may consider a combination of public and private funds to make use of the best sides of each method.[66]

Another solution is the deduction of fee from the final outcome once the dispute is resolved.[67] This would discourage the frivolous claims and, at the same time, does not prevent the consumers from bringing their claims. There are some jurisdictions like Spain, where all dispute resolution services ought to be non-profit.[68] Turkey does not disallow for-profit ODR mechanisms, but there are certain rules for legal fees in consumer cases before the courts.

Consumer disputes that are below 6,860 TL should be resolved before consumer arbitral tribunals.[69] Only consumers can bring claims before these tribunals; sellers/providers are not entitled to apply.[70] The consumers are exempt from any legal fees.[71] Both the

---

63 *See* Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 66.

64 Cortés, *Online Dispute Resolution,* 145.

65 Jonathan Hill, *Cross-Border Consumer Contracts* (Oxford Private International Law Series, 2008), 318.

66 Benyekhlef, "Online Dispute Resolution," 83; see Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 65 suggesting that public funding can be used in combination with other models.

67 Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 65.

68 Cortés, *Online Dispute Resolution,* 145.

69 6502 Tuketicinin Korunması Hakkında Kanun [Code on Consumer Protection] Art. 68.1.

70 Tuketici Hakem Heyetleri Yonetmeligi [Regulation on Consumer Arbitral Tribunals], Resmi Gazete [RG] [Official Gazette] 29188, Nov. 27, 2014 Art. 11.

71 Tuketici Hakem Heyetleri Yonetmeligi [Regulation on Consumer Arbitral Tribunals], Resmi Gazete [RG] [Official Gazette] 29188, Nov. 27, 2014, Art. 30.

consumers and seller/provider may object the decision of the tribunal at the consumer courts.[72] The consumer is again exempt from legal fees, but the seller/provider has to deposit the fees.[73] Since litigation is free of charge for consumers in Turkey, online arbitration may not attract consumers if it compels them to pay fees. Online arbitration should be publicly funded or the hybrid solution should be adopted. The businesses should pay the fees even if it is the consumer who complains to increase accessibility and reputation of online arbitration among consumers.

C. Lex Arbitri

The seat of arbitration does not lose its significance for online arbitration. It affects arbitrability, determination of the governing law, whether substantive or procedural and determination of the place for the annulment proceedings of the arbitral award.[74] Parties can determine the seat of arbitration in their agreements[75] as part of the party autonomy principle and flexibility of online arbitration. However, from time to time the parties, especially the consumer as the weaker party may end up with the seat that they do not have any connection.[76]

Determining the seat of online arbitration by traditional means is challenging. The arbitrators may consider the enforceability of arbitration agreement under national laws, the nationality of the parties and physical convenience on a case-by-case basis.[77] Some

---

72 *See* Code on Consumer Protection Art. 73.1.

73 Code on Consumer Protection. 73.2.

74 Alexander J. Belohlavek, "Importance of Seat of Arbitration in International Arbitration: Delocalization and Denationalization of Arbitration as an Outdated Myth," *ASA Bulletin* 31, no. 2 (2013): 262.

75 UNCITRAL Model Law, *supra* note 36, Art. 20 (1); MTK, *supra* note 57, Art.9.

76 Maurice Schellekens, "Online Arbitration and E-commerce." Electronic *Communication Law Review* 9 (2002): 123.

77 Arnold Vahrenwald, "Joint Research Centre of the EC Report on Out-of-Court Dispute Settlement Systems for E-Commerce," *Report on Legal Issues: Part IV—*

scholars suggest other criteria such as the location of the servers, place of the computers or where the emails of the arbitrator are sent and collected.[78] This makes online arbitration delocalized and detached from a physical place of arbitration.[79] This seems to be farfetched given the traditional legal framework that is drawn by the New York Convention.[80]

CIETAC Online Arbitration Rules give precedence to parties' agreement, in the absence thereof seat of online arbitration shall be the location of CIETAC.[81] RAA Online Arbitration Rules provides the seat of arbitration to be in Moscow, Russia unless parties agree otherwise.[82] Both sets of rules do not mention the discretion of the arbitrators; however, it is generally accepted that in the absence of an agreement, the arbitrators should have the discretion to determine the seat.

Turkey does not have an online arbitration legislation. As suggested, online arbitration may become applicable by Turkey's participation to the EU ODR platform that does not require Turkey to enact online arbitration rules right away. The seat of online arbitration under Turkish law would be determined per arbitration rules that are in force.[83]

Arbitration. Out-of-Court Dispute Settlement Systems for E-Commerce (Italy: 2000), 89.

78 Wahab, "The Global Information Society," 163.

79 See Hong-Lin Yu, and Motassem Nasir, "Can Online Arbitration Exist Within the Traditional Arbitration Framework?" *Journal of International Arbitration* 20, no. 5 (2003): 464 for more information on delocalization.

80 *Yu*, Nasir, "Can Online Arbitration Exist," 464.

81 "CIETAC Online Arbitration Rules," Art. 8.

82 "RAA Online Arbitration Rules," Art. 1.4.

83 MTK, *supra* note 57, Art.9. The seat of arbitration shall be determined by the parties or the arbitration institution selected by the parties. In the absence of an agreement, the seat of arbitration shall be determined by the arbitrators with regards to the relevant circumstances.

D. Applicable Law

Applicable law is another murky area with respect to online arbitration. Parties are free to choose the law applicable to the procedure and substance of their dispute. If the parties fail to determine the applicable law, arbitrators are vested with broad discretionary authority that may be used to fill the voids that are left by the parties.[84] A consumer may not possess sufficient knowledge to know or decide the applicable law. This is another advantage of online arbitration over other dispute resolution methods as arbitrators are able decide the applicable law in accordance with the circumstances of each case.[85]

Another advantage is the involvement of human effect in the process. Implementation of UNCITRAL instruments is suggested for identification of e-business usages and interpretation purposes.[86] If there is no choice of law, arbitrators should observe the equality of the parties while determining the applicable law.[87] They may supplement applicable rules *via* the International Institute for the Unification of Private Law (UNIDROIT) principles. For instance, the *contra proferentem* rule suggests that unclear terms to be interpreted against the party that supplied the terms.[88] It is unlikely for an e-commerce

---

84 *See* "RAA Online Arbitration Rules," Article 4.1.1.

85 Sela, "Can Computers Be Fair," 115. ("Indeed, the idea of "machine made justice" typically evokes inherent resistance, because it is at odds with the perception that fairness and justice are distinctly human traits that cannot be generated even by the most advanced artificially intelligent software.").

86 Ujjwal Kacker, and Saluja Taran, "Online Arbitration For Resolving E- Commerce Disputes: Gateway To The Future," *Indian Journal of Arbitration Law* 3, no.1 (2014): 34.

87 See for example UNCITRAL Model Law, *supra* note 36, Art. 28 (2), UNCITRAL Arbitration Rules (2013) http://www.uncitral.org/uncitral/en/uncitral_texts/ arbitration/2010Arbitration_rules.html Art. 17(1) for the generally accepted principle.

88 UNIDROIT Principles (2016) https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016 Art. 4.6. UNIDROIT Principles recognizes the significance of e-commerce contracts and reviews rules to include issues that may arise in connection with them.

consumer to supply the terms. In case of any ambiguity, the choice of law can be interpreted in favor of the consumer. This balance should be struck by online arbitrators as it would require human judgment within the context of fairness.

E. Effective Remedy and Enforcement of an Online Arbitration Award

Arbitrators should render an award within the time limits set by online arbitration platforms. Generally, the duration for rendering an award varies between a few days and two weeks, but time extension may be granted if an award is not rendered within the time limit.[89] After parties receive an award, they may want to enforce it if the counter-party does not comply with the award voluntarily.

Online arbitration is preferred over other ODR mechanisms due to its relative simplicity in enforcement in jurisdictions that are signatory to the New York Convention. For recognition and enforcement, written arbitration agreement and duly authenticated arbitral award should be provided. These two requirements will be addressed as they may restrict online arbitration since everything is carried out by electronic means.

1. Written and Signed Arbitration Agreement

Article II of the New York Convention requires arbitration agreements to be in writing and signed by the parties. This is to ensure that the parties have consented the arbitration agreement after having full knowledge of its existence. Online arbitration agreements are, however, not written on a paper, nor hand-signed by physically-distant parties. For instance, they may agree on arbitration by clicking the box "I agree to the terms and conditions".[90] They may exchange

---

[89] Kaufmann-Kohler, Schultz, *Online Dispute Resolution*, 59.

[90] The validity of pre-determined arbitration agreements and the arbitrability of the disputes are affected as discussed above under the section III.A.

emails and insert electronic signatures. The New York Convention accepts the exchange of letters,[91] but does not mention electronic communications. This requires interpretation of the treaty.[92]

It may be inferred that non-inclusion of e-communications was not intentional as electronic communications did not exist at the time when the New York Convention was drafted in 1958.[93] The rationale behind the written agreement is to prove parties' consent to arbitrate. With this rationale in mind, electronic agreements should be sufficient to demonstrate parties' intent to arbitrate their dispute.[94] As far as the consent is explicit, parties should meet the formal requirements of the arbitration agreement by clicking the box or indicating their names under the statement that they agree to submit their dispute to final and binding arbitration.[95] If the terms and conditions including the arbitration agreement are only accessed by a hyperlink, there is no indication of agreement.[96] The student buying the sneakers goes online only for shopping. She does not think about committing herself to a dispute resolution mechanism. She may click the box without reading the terms or she may never notice the hyperlink. Thus, in order for such agreements to be

---

91 The New York Convention, Art. II/2.

92 Vienna Convention on the Law of Treaties Art.31, 32, *opened for signature* May 23, 1969, 1155 U.N.T.S. 331. The articles set rules for the interpretation of treaties. First, ordinary meaning of the terms in their context and in light of their purpose and object is considered. If there is still obscurity, the circumstances of its conclusion should be taken into account. Here, the time of the conclusion is the relevant circumstance while interpreting its applicability on electronic means. Both the US and Turkey are not a party to the convention but the rules are closely observed under Turkish law. The Constitution of Turkey gives precedence to international agreements over national laws and they become part of the legal system. Rules for interpretation of laws require the evaluation of ordinary meaning, purpose and relevant circumstances.

93 Wahab, "The Global Information Society," 154.

94 Haitham A. Haloush, "The Authenticity of Online Alternative Dispute Resolution Proceedings," *Journal of International Arbitration* 25, no. 3 (2008): 361.

95 Haloush, "The Authenticity of Online Alternative Dispute Resolution Proceedings," 362.

96 Jeffrey H. Dasdeel, "Consumer Click Arbitration, A Review of Online Consumer Arbitration Agreements," *Arbitration Law Review* 9 (2017): 4.

valid, the consumer should be given proper notice about the e-xistence of an arbitration agreement.[97]

In addition to Article II of the New York Convention, most of the jurisdictions require an arbitration agreement to be in writing. In terms of online arbitration agreements, courts generally consider whether there is a consent of the consumer, if so how it is taken. The US case law requires case-by-case analysis to determine the validity.

In *Specht v. Netscape Communications Corp.*, the Court found that reasonably prudent user of the website would not have known the terms and conditions that are given on the next scrollable screen.[98] The users cannot be considered consented to the terms of the agreement. In *Nicosia v. Amazon.com, Inc.*, the Court investigated the layout of the website and how user agreed to the terms. The Court stated that the design of the website is important to bind customer by the agreement.[99] The plaintiff asserted that conditions of use that contain arbitration provision are not enforceable because he did not consent.[100] Amazon claimed that the plaintiff was bound by the agreement because he was given the notice "By placing your order, you agree to Amazon.com's privacy notice and conditions of use" before placing the order and conditions of use were hyperlinked.[101] The Court held that hyperlink was a conspicuous warning and the plaintiff is bound by the agreement because the plaintiff could not place the order without first clicking the terms.[102] The Court draws the distinction with the *Specht* case, where there was no reference to terms and conditions.[103] In another case, the Court deemed arbitrati-on agreement to be null because the consumer was not asked to agree on anything although there was a hyperlink to the conditions

---

97 Dasdeel, "Consumer Click Arbitration," 5.

98 Specht v. Netscape Communications Corp. 306 F.3d.17, 33 (2d Cir. 2017)(United States).

99 Nicosia v. Amazon.com, Inc. 84 F. Supp.3d 142, 153 (E.D.N.Y. 2016) (United States).

100 Nicosia v. Amazon.com, Inc., 150.

101 Nicosia v. Amazon.com, Inc., 150.

102 Nicosia v. Amazon.com, Inc., 150.

103 Nicosia v. Amazon.com, Inc., 151.

at the end of each page.[104] Under the US law, there is no clear rule to determine whether the user is bound by the agreement or not. The courts decide case-by-case basis. They look at whether the consumer could have known the existence of the arbitration agreement.

UNCITRAL Model Law also requires an arbitration agreement to be in writing. The Model Law defines what is meant by being in a written form and includes "electronic communication if the information contained therein is accessible so as to be usable for subsequent reference".[105] Turkey has enacted its international arbitration legislation based on the Model Law in 2001 and recognized electronic communication as a written form.[106] The Turkish Court of Appeals addressed the writing requirement in a case that is not related to an electronic arbitration agreement. The Court by referring to the arbitration law stated that arbitration agreements in electronic documents shall be valid and binding.[107] This decision suggests that the consumer and the business representative do not have to come together to hand-sign the arbitration agreement. They may use e-mails and electronic signature to agree on online arbitration.

Turkish cases are silent on e-commerce arbitration agreements. As mentioned above, the case law addresses the arbitrability of the consumer disputes, rather than the validity of the electronic arbitration agreements. One of the objectives of the Code on Electronic Commerce is to set rules on informing consumers about the ADR mechanisms.[108] When the laws are read together, consumer disputes should be resolved by online arbitration as an alternative or out-of-court method. The online arbitration agreement as a type of contract should be handled as other terms and should be valid if the consumer is properly notified.

---

104 Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1175 (9th Cir. 2014) (United States).

105 UNCITRAL Model Law, *supra* note 36, Art. 7(4).

106 MTK, *supra* note 57, Art.4.

107 Yar. 11. HD., E. 2015/1687, K. 2015/6696, 11.05.2015 [11th Civil Chamber of Court of Appeals, Application No 2015/1687, Decision No 2015/6696, Nov. 11, 2015].

108 6563 Elektronik Ticaretin Duzenlenmesi Hakkinda Kanun [Code on Regulation of Electronic Commerce] Art. 3, para.ç.

2. Authenticated Original Award

For recognition and enforcement of an award under the New York Convention, a duly authenticated original award or its certified copy should be supplied.[109] A document is authenticated if it bears the signature indicating that it is genuine. Signature formality impedes online arbitration. In a digital and paperless era, signing documents becomes redundant.[110] Echoing this view, E-Commerce Model Law sets out rules for an electronic signature to function and fulfill in a same way with traditional signatures.[111] E-communication Convention is another international document addressing this issue. Recognizing the restrictions under the New York Convention, it interprets the term contract in a manner that covers arbitration agreements that are concluded by electronic means.[112] Another document that works in harmony with these texts is the UNCITRAL Model Law on Electronic Signature that provides equivalence of hand-written and electronic signatures.[113]

---

[109] The New York Convention, Art. IV/1/a.

[110] Haloush, "The Authenticity of Online Alternative Dispute Resolution Proceedings," 362.

[111] UNCITRAL, "Model Law on Electronic Commerce", Art. 7. ("1) Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.").

[112] "United Nations Convention on the Use of Electronic Communications in International Contracts, 2005," accessed November 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html, Art.1. Only 11 countries are party to the Convention whose main objective is to promote electronic communications in international contracts by overcoming the formal obstacles set by some treaties such as the New York Convention and the CISG.

[113] "UNCITRAL Model Law on Electronic Signature, 2001," accessed November 11, 2018, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html html. Legislation based on or influenced by this Model Law has been adopted in 32 States.

Similarly, EU Directive on e-commerce[114] and e-signature[115] establishes that electronic contracts and signatures shall be given same legal status as paper contracts and hand-written signatures respectively. There is no explicit reference to arbitration agreements and awards however cross-border arrangements, development of international e-commerce and interoperability of the contracts are the reasons behind the e-signature rules.[116] The rules aim at increasing consumer confidence in e-communication and e-commerce.[117] The aim and the wording of the rules indicate that online arbitration agreements and awards are valid under EU law.

Institutional rules have different approaches. The CIETAC requires an arbitral award to be in writing and signed without detailing the signature requirements.[118] The RAA rules explicitly allow digital signature.[119]

Turkey is not a party to the E-communication Convention and did not adopt the model laws *verbatim*, but enacted parallel legislation. The law on e-signatures gives e-signature the same legal effect as the hand-written signature. The transactions that require official form or proceeding cannot be done by e-signature.[120] Arbitration agreement and award are not among them.[121] The laws and regulations on e-commerce and e-communications enacted pursuant to EU

---

114 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), O.J. (L 178) (EC).

115 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, O.J. (L13/12) (EC).

116 Directive 1999/93/EC, at Preamble para 23.

117 Directive 1999/93/EC, at Preamble para. 24.

118 "CIETAC Online Arbitration Rules," Art. 39.

119 "RAA Online Arbitration Rules," Art. 5.1.4.

120 5070 Elektronik İmza Kanunu [Code on Electronic Signatures], Art. 5.

121 Some transactions are subject to official form that should be carried out before a public officer as named by law. For instance sale of immovable property should be done before land registrar.

directives as a part of harmonization policy particularly mention the consumers and provide additional protection.[122]

Written form and authentication are the main challenges to online arbitration since they attack its most significant advantage, enforceability. Current international, regional and national rules try to address the issue in multiple facets and it seems like there is a convincing evidence that online arbitral awards are enforceable regardless of the formal requirements. These formalities are not considered as a factual obstacle for online awards anymore since arbitrators can always print out the award, sign, and send it to the parties even if it would be impractical.[123] Hybrid solutions bringing offline and the online world together should be accepted for online arbitration awards. Regardless of the abovementioned obstacles, if existing traditional legal rules are broadly interpreted harmoniously with modern technological advances, online arbitration is most likely to survive. [124]

V. CONCLUSION

Notwithstanding the challenges to online arbitration, Turkish law mechanisms show great adaptability to it. The most important challenge to overcome is the arbitrability of consumer disputes under Turkish law. The laws do not explicitly prohibit voluntary arbitration of consumer disputes. When the laws are read together, arbitration as one of the ADR mechanisms should be applicable to consumer disputes. Most and foremost, if the laws aim to protect the consumers, online arbitration should be made available for consumer disputes as it provides effective, quick, and budget-friendly remedies.

---

[122] *See* Code on Regulation of Electronic Commerce; *see* 5809 Elektronik Haberlesme Kanunu [Code on Electronic Communication]; see also Ticari Iletisim ve Ticari Elektronik Iletiler Hakkinda Yonetmelik [Regulation on Commercial Communication and Commercial Electronic Correspondence] Resmi Gazete [RG] [Official Gazette] 29417, Jan. 15, 2015 for reasons of legislation.

[123] Haloush, "The Authenticity of Online Alternative Dispute Resolution Proceedings," 362.

[124] Wahab, "The Global Information Society," 168.

The questions regarding the remaining challenges, such as writing requirement and authentication of agreements and awards are not answered under Turkish law. Approaches of courts from other jurisdictions, where online arbitration is practiced, may be taken as guidelines. The rules on e-communication, e-signatures, and e-commerce are in harmony with modern jurisdictions. To establish an online arbitration practice, Turkey does not necessarily have to enact additional legislation. However, in order to avoid conflicts and ambiguity, the statutes can be renovated to allow online arbitration for consumer disputes.

Being a part of a regional organization with established practice would minimize the precedence or regulation-related problems. The regional organizations offer a better solution since they address cross-border disputes for the countries that have necessary national legislation to establish online arbitration. Therefore, Turkey's accession to the EU ODR platform would make resolution of cross-border disputes within the region easier. Being a part of the platform, Turkey can provide services *via* ISTAC. ISTAC need not to implement new rules, as the EU ODR platform will cover the electronic management of the cases. The disputes can be resolved by current rules. By following the arbitration institutions that currently offer online arbitration rules, ISTAC may implement or reform its rules in the future if it finds appropriate.

BIBLIOGRAPHY

Secondary Resources

Albornoz, Maria Mercedes, and Martin, Nuria González. "Feasibility Analysis of Online Dispute Resolution in Developing Countries." *University of Miami Inter-American Law Review* 44, no. 1 (2012): 39-61.

Asia-Pasific Economic Cooperation Economic Committee Project in Implementation, Workshop for Developing a Collaborative Framework for Online Dispute Resolution, EC 05 2018A, 2018.

Belohlavek, Alexander J. "Importance of Seat of Arbitration in International Arbitration: Delocalization and Denationalization of Arbitration as an Outdated Myth." *ASA Bulletin* 31, no. 2 (2013): 262-292.

Benyekhlef, Karim. "Online Dispute Resolution." *Lex Electronica* 10, no. 2 (2005), 1-129.

Cortés, Pablo. *Online Dispute Resolution for Consumers, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*. Mohammed Salahudine Abdel Wahab et al. eds. Eleven International Publishing, 2012.

Dasdeel, Jeffrey H. "Consumer Click Arbitration, A Review of Online Consumer Arbitration Agreements." *Arbitration Law Review* 9 (2017): 1-19.

De Boisséson, Matthieu, and Thomas Clay. "Recent Developments in Arbitration in Civil Law Countries." *International Arbitration Law Review* 1 (1998): 150.

E-Commerce Mediation Committee. Accessed November 3, 2018. https://www.ecmc.or.kr/ecmceng/subIndex/228.do.

European Commission. "Online Dispute Resolution." Accessed November 11, 2018. https://ec.europa.eu/consumers/odr/main/?event=main. home2.show.

Goodman, Joseph W. "The Pros and Cons of Online Dispute Resolution: An Assessment of Cyber-Mediation Websites." *Duke Law and Technology Review* 4 (2003): 1-16.

Haloush, Haitham A. "The Authenticity of Online Alternative Dispute Resolution Proceedings." *Journal of International Arbitration* 25, no. 3 (2008): 355-364.

Haydock, R.S, and Henderson Jennifer D. "Arbitration and Civil Justice: An American Historical Review and Proposal for a Private/Arbitral and Public/Judicial Partnership." *Pepperdine Dispute Resolution Law Journal* 2, no. 2 (2002): 141-198.

Heiskanen, Veijo. "Dispute Resolution in International Electronic Commerce." *Journal of International Arbitration* 16, no. 3 (1999): 29-44.

Hill, Jonathan. *Cross-Border Consumer Contracts*, Oxford Private International Law Series, 2008.

Yu, Hong-Lin, and Motassem Nasir. "Can Online Arbitration Exist Within the Traditional Arbitration Framework?" *Journal of International Arbitration* 20, no. 5 (2003): 455-473.

Kacker, Ujjwal, and Saluja Taran. "Online Arbitration For Resolving E-Commerce Disputes: Gateway To The Future." *Indian Journal of Arbitration Law* 3, no.1 (2014): 31-44.

Katsh, Ethan, and Janet Rifkin. *Online Dispute Resolution: Resolving Conflicts in Cyberspace.* San Francisco (CA): Jossey-Bass Publishers, 2001.

Kaufmann-Kohler, Gabrielle, and Thomas Schultz. *Online Dispute Resolution: Challenges for Contemporary Justice.* The Hague: Kluwer Law International, 2004.

Kurtulan, Gokce. "Turk Hukukunda Tuketici Uyusmazliklarinin Tahkime Elverisliligi [Arbitrability of Consumer Disputes under Turkish Law]." *Turkiye Barolar Birligi Dergisi* 131 (2017): 239-260.

Lavi, Dafna. "Three Is Not a Crowd: Online Mediation-Arbitration in Business to Consumer Internet Disputes." *University of Pennsylvania Journal of International Law* 37, no. 3 (2016): 871-941.

Lugo, Gustavo Alcocer, and Abraham Diaz Arceo. "Digital Business in Mexico: Overview." *Thomson Reuters Practical Law.* Accessed November 3, 2018. https://uk.practicallaw.thomsonreuters.com/w-012-0309?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1.

Organization of American States. "Draft Electronic Resolution of Cross-Border E-Commerce Consumer Disputes." Accessed November 3, 2018. http://www.oas.org/dil/esp/CIDIPVII_proteccion_al_consumidor_united_states_guia_legislativa_anexo_A.pdf.

Rainey, Daniel. *ODR and Culture, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*, eds., Mohammed Salahudine Abdel Wahab et al. eds. Eleven International Publishing, 2012.

Rule, Colin, Vikki Rogers, and Louis Del. Duca "Designing Global Consumer Online Dispute Resolution (ODR) System for Cross-Border Small Value-High Volume Claims – OAS Developments." *Uniform Commercial Code Law Journal* 42 (2010): 221-264.

Russian Arbitration Association (RAA). Accessed November 3, 2018. https://arbitration.ru/en/.

Salter, Shannon. "Online Dispute Resolution and Justice System Integration: British Columbia's Civil Resolution Tribunal." *Windsor Yearbook of Access to Justice* 34 (2017): 112-129.

Schellekens, Maurice. "Online Arbitration and E-commerce." Electronic *Communication Law Review* 9 (2002): 113-125.

Sela, Ayelet. "Can Computers Be Fair: How Automated and Human-Powered Online Dispute Resolution Affect Procedural Justice in Mediation and Arbitration." *Ohio State Journal on Dispute Resolution* 33, no. 1 (2018): 91-148.

Internet World Stats. "Usage and Population Statistics." Accessed December 11, 2018. https://www.internetworldstats.com/top20.htm.

Vahrenwald, Arnold. "Joint Research Centre of the EC Report on Out-of-Court Dispute Settlement Systems for E-Commerce." *Report on Legal Issues: Part IV—Arbitration*. Out-of-Court Dispute Settlement Systems for E-Commerce. Italy, 2000. accessed November 11, 2018. https://tbplaw.com/data/part4.pdf.

Wahab, Mohamad Salahudine Abdel. "The Global Information Society and Online Dispute Resolution: A New Dawn for Dispute Resolution." *Journal of International Arbitration* 21, no. 2 (2004): 143-168.

Wahab, Mohammed Salahudine Abdel. *ODR and E-arbitration, in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*. eds., Mohammed Salahudine Abdel Wahab et al. Eleven International Publishing, 2012.

Yesilova, Bilgehan. "6502 sayılı Yeni Tuketicinin Korunmasi Hakkinda Kanun'a Gore Tuketici Uyusmazliklarinin Çozumu Usulu ve Yargilama Kurallari [Resolution Procedure and Rules for Consumer Disputes under the Code of Protection of Consumer numbered 6502]." *Terazi Hukuk Dergisi* 9 (2014): 107-148.

Yuthayotin, Suatip. *Access to Justice in Transnational B2C E-Commerce: A Multidimensional Analysis of Consumer Protection Mechanisms*. Switzerland: Springer International Publishing, 2015.

Rules and Regulations

4686 Milletlerarasi Tahkim Kanunu [MTK] [Code of International Arbitration].

5070 Elektronik Imza Kanunu [Code on Electronic Signatures].

5809 Elektronik Haberlesme Kanunu [Code on Electronic Communication].

6100 Hukuk Muhakemeleri Kanunu [Code of Civil Procedure].

6325 Hukuk Uyusmazliklarinda Arabuluculuk Kanunu [Code of Mediation in Law Civil Disputes].

6502 Tuketicinin Korunmasi Hakkinda Kanun [Code on Consumer Protectıon].

6563 Elektronik Ticaretin Duzenlenmesi Hakkinda Kanun [Code on Regulation of Electronic Commerce]

CIETAC Online Arbitration Rules, 2015. Accessed December 11, 2018. http://bj.cietac.org/index/rules/4760665e7716e27f001.cms.

UNCITRAL. "Convention on the Recognition and Enforcement of Foreign Arbitral Awards, 1958." Accessed December 11, 2018.

http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html.

Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts O.J. (L95/29) para Q of the annex.

Decision No 1/95 of the EC-Turkey Association Council of 22 December 1995 on Implementing the Final Phase of the Customs Union O.J. (L 35).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, O.J. (L13/12) (EC).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), O.J. (L 178) (EC).

Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests O.J. (L 304/1).

Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests O.J. (L 304/1) para 30.

Opinion 2017/C 075/22 of the European Economic and Social Committee on Enhancement of EU-Turkey Bilateral Trade Relations and Modernization of the Customs Union O.J. (C 75) 1.12.

Regulation 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), O.J. (L 304/1).

T.C. Gumruk ve Ticaret Bakanligi Karar No: 77002794-405 Konu: Tuketici Hakem Heyetlerinin Yeniden Yapilandirilmasi, 9.07.2018 [Republic of Turkey Ministry of Customs and Commerce Decree No: 77002794-405 Subject: Restructuring Consumer Arbitral Tribunals, July 9, 2018][Restructuring Decree].

The Inter-American Juridical Committee Res. CJI/ RES. 227 (LXXXIX-O/16), Oct. 3-14, 2016.

Ticari Iletisim ve Ticari Elektronik Iletiler Hakkinda Yonetmelik [Regulation on Commercial Communication and Commercial Electronic Correspondence] Resmi Gazete [RG] [Official Gazette] 29417, Jan. 15, 2015.

Tuketici Hakem Heyetleri Yonetmeligi [Regulation on Consumer Arbitral Tribunals], Resmi Gazete [RG] [Official Gazette] 29188, Nov. 27, 2014.

Tuketici Sozlesmelerindeki Haksiz Sartlar Hakkinda Yonetmelik [Regulation on Unfair Terms in Consumer Contracts], Resmi Gazete [RG] [Official Gazette] 29033, Jan. 17, 2014 Annex 1, para. 1(n).

UN. "Convention on Contracts for the International Sale of Goods, 1980." Accessed December 11, 2018. http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html.

UN. "Convention on the Use of Electronic Communication in International Contracts, 2005." Accessed December 11, 2018.

http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

UNCITRAL. "Model Law on Electronic Commerce 1996." Accessed December 11, 2018. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html.

UNCITRAL. "Model Law on Electronic Signature 2001." Accessed November 11, 2018. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html html.

UNCITRAL. "Model Law on International Commercial Arbitration 2006". Accessed December 11, 2018. http://www.uncitral.org/ uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html.

UNCITRAL. "Technical Notes on Online Dispute Resolution (2017), Section V, para.26." Accessed December 11, 2018. http://www. uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf.

"UNIDROIT Principles 2016." Accessed December 11, 2018. https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016.

"United Nations Convention on the Use of Electronic Communications in International Contracts, 2005." Accessed November 11, 2018. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

Vienna Convention on the Law of Treaties Art.31, 32, *opened for signature* May 23, 1969, 1155 U.N.T.S. 331.