TBB Dergisi 2023 (167) s.83-132

MESAJLAŞMA UYGULAMALARI İLE BULUT VE SOSYAL MEDYA ORTAMLARINDAN SAYISAL DELİLLERİN ELDE EDİLMESİ

OBTAINING DIGITAL EVIDENCES FROM MESSAGING APPLICATIONS, CLOUD AND SOCIAL MEDIA

Burak MELEMEZ*

Özet: Bilişim teknolojilerindeki gelişmeler sonucu bilişim cihazlarının çeşitliliğinin artması ve kullanımının yaygınlaşması bilişim suçları ile bilişim sistemleri vasıtasıyla işlenen suçların sayısındaki artışı beraberinde getirmiştir. Bu suçların aydınlatılmasını sağlayacak sayısal deliller çeşitli adli bilişim yöntemleriyle elde edilebilmektedir. Elde edilen bu delillerin bir anlam ifade edebilmesi için hukuka uygun olarak elde edilmesi gerekir. CMK m. 134 ve m. 135'te bilişim cihazlarındaki sayısal delillerin elde edilebilmesi için iki farklı koruma tedbirine yer verilmiştir. Ancak bu tedbirler günümüz bilişim ve yazılım teknolojilerinin ihtiyaçlarına tam anlamıyla karşılık verememekte ve bu durum uygulamada tereddütlere sebep olmaktadır. Çalışmamızda bu ihtiyaçtan yola çıkılarak, CMK m. 134 ve m. 135 bağlamında elektronik posta ve anlık mesajlaşma uygulamaları ile bulut ve sosyal medya ortamlarında bulunan sayısal delillerin elde edilmesi konusu incelenmiştir.

Çalışmada öncelikle CMK m. 134 ve m. 135 hükümlerinin kapsam ve özelliklerine değinilerek bu koruma tedbirlerinden hangisine, ne zaman başvurulması gerektiği hususu tespit edilmeye çalışılmıştır. Daha sonra ise bu tespitten yola çıkılarak yaygın kullanımları nedeniyle sayısal deliller için önemli birer kaynak teşkil eden mesajlaşma uygulamaları ile bulut ve sosyal medya ortamlarındaki delillerin hukuka uygun olarak nasıl elde edilmesi gerektiği hususu incelenmiştir. Bu inceleme sırasında söz konusu program ve ortamların sahip oldukları özellikler dikkate alınmıştır. Son olarak, e-posta ve anlık mesajlaşma uygulamalarına nazaran daha yeni bir teknoloji ürünü olan bulutta bulunan delillerin elde edilmesindeki güçlükler nedeniyle başvurulan veri yerelleştirme/veri ikameti konusuna değinilmiştir. Çalışmada mevzuatımızın yanı sıra Avrupa Konseyi Siber Suç Sözleş-

* Ar. Gör., Ankara Üniversitesi Sosyal Bilimler Enstitüsü, bmelemez@ankara.edu.tr, ORCID: 0000-0001-8768-7535, Makalenin Gönderim Tarihi: 20.03.2023, Kabul Tarihi: 17.07.2023

mesi (ASSS) ve Avrupa Konseyi'nin sayısal delillerin elde edilmesine ilişkin faaliyetleri kapsamında değerlendirmelerde bulunulmuştur.

Anahtar Kelimeler: Bilgisayarlarda Arama, İletişimin Denetlenmesi, Bulutta Arama, Siber Suç Sözleşmesi, E-posta, WhatsApp, Sosyal Medya

Abstract: As a result of the developments in information technologies, the spread of the diversity and use of information devices has brought about an increase in the number of cyber crimes and crimes committed through information systems. Digital evidence to detect these crimes can be obtained by various forensic methods. In order for these evidences to be legitimate, they must be obtained in accordance with the law. In Art. 134 and Art. 135 of Turkish Criminal Procedure Code, two different measures of protection are included in order to obtain digital evidence on information devices. However, these measures cannot fully cover the needs of today's information and software technologies, therefore this situation cause hesitations in enforcement of law. Based on this need in our study, in the context of Art. 134 and Art. 135 Turkish Criminal Procedure Code, the issue of obtaining digital evidence in electronic mail and instant messaging applications, cloud and social media environments were examined.

In the study, first of all, the scope of Art. 134 and Art. 135 of Turkish Criminal Procedure Code are mentioned and it is tried to determine which and when of these measures of protection should be applied. Then, based on this determination, it is examined how to obtain evidence from messaging applications, cloud and social media environments in accordance with law through which are important sources for digital evidence due to their widespread use. During this research, the features of the mentioned programs and environments were taken into consideration. Finally, cloud database, which is a newer technology compared to e-mail and instant messaging applications is addressed due to the difficulties in accordance with obtaining evidence in data localization/data residency. In this study, in addition to Turkish legislation, evaluations were made within Council of Europe Convention on Cyber Crime and the scope of activities of the Council of Europe on obtaining digital evidence.

Keywords: Search on Computers, Inspection of Communication, Search on Cloud, Convention on Cybercrime, Digital Evidence, Email, WhatsApp, Social Media

GİRİŞ

Günlük hayatımızın bir parçası haline gelen bilişim cihazları hem bilgisayarlar gibi veri depolayarak işleyebilmekte hem başkalarıyla iletişim kurulmasına aracılık etmekte hem de internet erişimine imkân sağlamaktadır. Bu fonksiyonların hepsini bünyesinde barındıran ve en çok kullanılan bilişim cihazı türü şüphesiz ki akıllı telefonlardır.

Akıllı telefonlar bu özellikleri itibariyle günümüzde sayısal deliller[1] için eşsiz birer kaynak haline gelmişlerdir. Akıllı telefonlardan elde edilen delillerin bilgisayarlar veya diğer bilişim cihazlarından elde edilen delillerden farkı bu delillerin doğrudan kullanıcıyla ilişkilendirilebilir olmasıdır.[2] Kullanıcının kiminle görüştüğü, sosyal medya hesapları, e-postaları, fotoğraf, video ve ses kaydı gibi birçok veriye bu yolla ulaşılabilir. Bu cihazlar müşterek kullanımdan ziyade şahsi kullanıma tahsisli olduklarından akıllı telefonlardan elde edilen delillerin kullanıcısıyla bağlantısının ortaya konulması da oldukça kolay olacaktır. Bu nedenle akıllı telefonlar maddi gerçeğe ulaşılmasını sağlayacak temsil edici ve ispat gücü yüksek delillerin elde edilmesi bakımından oldukça önemli birer kaynaktır.

Teknolojinin gelişimiyle bağlantılı olarak bilişim cihazlarındaki sayısal delillerin büyük bir kısmına çeşitli adli bilişim inceleme ve yöntemleriyle kolaylıkla erişilebilmektedir. Ancak unutulmamalıdır ki, bir delil maddi vakıa bakımından ne kadar önemli olursa olsun hukuka uygun olarak elde edilmediği takdirde hükme esas alınamaz (CMK m. 217/2). Dolayısıyla sayısal delillerin elde edilmesinde teknik boyut kadar hukuki boyut da önemlidir. Teknik eksiklikler delilin elde edilememesine, hukuki hatalar ise elde edilen delilin hukuka aykırılığına yol açar.[3] Adli bilişim yöntemleri ne kadar ilerlerse ilerlesin bilişim cihazlarından elde edilen delillerin hukuka aykırı olmaması için öncelikle kanunda öngörülen usule göre alınmış bir karar bulunmalı ve bu karar hukuka uygun bir şekilde icra edilmelidir. Bu doğrultuda bilgisayar, bilgisayar kütükleri ve programlarında arama yapılabilmesi için CMK m. 134, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi için ise CMK'nın 135 vd. maddeleri kapsamında bir karar alınması gerekir. Ancak akıllı telefonların birden fazla fonksiyona sahip olması ve bu cihazların her geçen gün farklı şekil ve amaçlarla

---

1 Elektronik delil, sayısal delil kavramını da kapsayan bir üst kavramdır. Çalışmamızda bir elektronik delil türü olan analog delillerin günlük hayatımızdan her geçen gün silinmesi ve çalışmamızın konusunu teşkil eden elektronik delil türünün sayısal deliller olması sebebiyle sayısal delil kavramının kullanılması tercih edilmiştir. Elektronik ve sayısal delil kavramları hakkında ayrıntılı bilgi için bkz. Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin Yayıncılık, Ankara, 2014, s. 125 vd.

2 Değirmenci, Sayısal Delil, s. 147.

3 Değirmenci, Sayısal Delil, s. 311.

kullanılabiliyor olması uygulamada bu koruma tedbirlerinden hangisine başvurulacağına ilişkin tereddütler yaratmaktadır.[4] Bu konuda yapılacak yanlış bir tercih sonucu, elde edilen delil kanuna aykırı olacağından reddedilecek (CMK m. 206/2-a) ve temel hak ve özgürlüklerin ihlali gündeme gelebilecektir. Teknolojiye başvurmanın zorunlu olduğu bu gibi hallerde temel hak ve özgürlüklerin ihlal edilmemesi gerekliliği hiçbir zaman göz ardı edilmemelidir.[5]

Çalışmamızda bu bağlamda akıllı telefon, tablet, bilgisayar gibi bilişim ve iletişim amaçlı kullanılabilen cihazların sahip oldukları özellikler ve kullanım amaçları dikkate alınarak bu cihazlardan hukuka uygun bir şekilde delil elde edilebilmesi için CMK m. 134 ve m. 135 hükümlerinden hangisi veya hangilerine başvurulması gerektiği hususu tarafı olduğumuz Avrupa Konseyi Siber Suç Sözleşmesi (ASSS) ve mevzuatımızdaki hükümler çerçevesinde incelenecek, böylece mevzuatımızdaki hükümlerin bu konudaki ihtiyaca ne derece karşılık verdiği tespit edilmeye çalışılacaktır.

I. CMK m. 134 ve m. 135 HÜKÜMLERİNİN KAPSAMI

Bilişim teknolojilerindeki baş döndürücü hızdaki gelişmeler bilişim suçları olarak adlandırılan yeni suç tiplerinin doğmasına ve klasik anlamdaki bazı suçların ise bilişim araçlarıyla işlenebilmesine yol açmıştır.[6] Bilişim suçlarında elle tutulur, gözle görülür klasik deliller yerini soyut nitelikteki sayısal delillere bıraktığından[7] bu suçların izini sürerek delil elde edilebilmesi için geleneksel yöntemler yetersiz kalmıştır.[8] Dolayısıyla bilişim suçlarıyla mücadele etmek ve bilişim sis-

---

4 Ersan Şen, "Bilgisayar Aramasında ve İletişimin Denetlenmesinde Hukuka Aykırılık Soruları", https://www.hukukihaber.net/bilgisayar-aramasinda-ve-iletisimin-denetlenmesinde-hukuka-aykirilik-sorulari-makale,7344.html (Erişim Tarihi: 28.02.2023).

5 Muharrem Özen/İhsan Baştürk, Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara, 2011, s. 165.

6 A. Caner Yenidünya/Olgun Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 2003, s. 14.

7 Muharrem Özen/Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi (CMK m. 134)", Ankara Barosu Dergisi, Y. 73, S. 2015/1, s. 59; Olgun Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi", *Bilişim Hukuku Dergisi*, C. 2, S. 1, s. 58.

8 Feridun Yenisey/Ayşe Nuhoğlu, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2022, s. 453.

temlerinin bu suçların işlenmesinde kullanılıp kullanılmadığını tespit etmek amacıyla yapılacak çalışmaların[9] hukuki bir zemine oturtulması için CMK'da bazı yeni koruma tedbirlerine yer verilmiştir. Teknolojik imkanların ve altyapının kullanılmasını gerektiren adli bilişime ilişkin bu tedbirler CMK m. 134'te düzenlenen bilgisayarlarda arama ve CMK m. 135'te düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınmasıdır.[10] Sayısal delillerin elde edilmesinde bu koruma tedbirlerinden hangisine başvurulması gerektiğine doğru olarak karar verilebilmesi için öncelikle bu tedbirlerin kapsam ve özelliklerinin belirlenmesi gerekir.

CMK m. 134 sadece bilgisayar, bilgisayar kütükleri ve programlarında arama, kopyalama ve elkoymaya izin vermektedir. Dolayısıyla bu tedbire başvurabilmek için öncelikle incelemenin yapılacağı bilişim sisteminin bu üç kavramdan birinin kapsamına girmesi gerekir. Buradaki bilgisayar kavramı geniş anlamda kabul edilmeli ve veri[11] işleme, saklama ve iletme özelliğine sahip tüm cihazlar bu kapsamda değerlendirilmelidir. Bilgisayar olarak adlandırılmamasına rağmen geniş anlamda bilgisayar tanımının kapsamına giren her türlü aygıt hakkında bu tedbire başvurulabilir.[12] Dolayısıyla akıllı telefon[13] ve tablet

---

9 Bu çalışmaların tümü bir bütün olarak adli bilişim olarak adlandırılmaktadır. Ayrıntılı bilgi için bkz. Türkay Henkoğlu, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, İstanbul, 2014, s. 1 vd.

10 Madde kenar başlığındaki bu ibare yerine "uzakla haberleşmenin denetlenmesi" teriminin kullanılmasının daha doğru olacağına ilişkin görüş ve eleştiriler için bkz. Veli Özer Özbek, "Türk Hukukunda İletişimin Adli/İdari Amaçla Denetlenmesi ve Uygulamadaki Sorunlar", Ceza Muhakemesi Hukukunda Güncel Konular, İstanbul 2015, ss. 178-179.

11 Veri, bilişim sistemlerinde yer alan ve formatlanarak sistem tarafından okunabilir hale getirilen her türlü bilgidir. Bilişim sistemlerinde yer alan veriler maddi gerçeğin ortaya çıkması için kullanıldığı takdirde sayısal delil niteliği kazanacaktır. Maddi olayla bağlantılı her türlü veri muhakeme sürecinde sayısal delil olarak kullanılabilir. Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği", *Terazi Hukuk Dergisi*, C. 9, S. 97, Eylül 2014, s. 16.

12 Değirmenci, Sayısal Delil, s. 328, 329; CMK m. 134'ün veri yerine, veriyi depolayan cihazı esas alan bir düzenlemeye tabi tutulmasının hatalı olduğuna dair görüş için bkz. Olgun Değirmenci, "Sayısal (Dijital) Verilerde Yakalama Sonrası Arama: Amerikan Yüksek Mahkemesinin Riley v. California Kararı Sonrası Amerikan Hukukunun Değerlendirilmesi", *TAAD*, Y. 7, S. 24, Ocak 2016, s. 81

13 "CMK 134. maddesindeki 'bilgisayar kütükleri' ifadesi teknik anlamda sadece masaüstü ve dizüstü bilgisayarlarda bulunanları değil, CD, DVD, flash disk, disket, harddisk vs. tüm çıkarılabilir bellekler, telefon vb. dijital tabanlı mobil cihazlarda dahil olmak üzere herhangi bir bilgi işlem veya veri toplama araç ya da gerecinde bulunabilecek tüm dijital dosyaları kapsamaktadır." Yargıtay 16. C.D. E. 2015/3, K. 2017/3, T. 24.04.2017.

ile akıllı saat ve bileklik gibi giyilebilir teknoloji ürünleri de bilgisayar kavramı kapsamındadır.[14]

CMK m. 134 kapsamında yapılan arama bilgisayarın fiziki varlığına yöneliktir. Yani doğrudan bilgisayarda depolanan verilerin kopyalanması veya bilgisayara el konulması söz konusudur.[15] Bilişim sistemlerinde depolanan veya depolandığı sistem içinde işlenen bu tür veriler durağan veridir.[16] Bilişim sistemlerinden elektronik veri olarak iki tür sayısal delil elde edilebilir. Bunlar akış halindeki veriler ve durağan verilerdir. Bazı veriler akış halindeyken durağan hale gelebilir.[17] Durağan haldeki sayısal delillerin elde edilmesi için CMK m. 134 hükmüne başvurulması gerekir.[18]

CMK m. 135'te iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi (CMK m. 135/1), mobil telefonun yerinin tespiti (CMK m. 135/5) ve iletişimin tespiti (CMK m. 135/6) olmak üzere birden fazla tedbire yer verilmiştir. Bu tedbirler ilgili bölüm başlığında belirtildiği üzere telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ilişkindir. CMK m. 135'e başvurulabilmesi için ortada telekomünikasyon[19] yoluyla gerçekleştirilen bir iletişimin olması gerekir.[20] Telekomünikasyon araçlarıyla yapılmayan iletişim bu tedbirin konusu-

---

14 Tezcan vd., Dijital Ceza Muhakemesi Hukuku, (Editörler: Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem), Seçkin Yayıncılık, Ankara, 2022, s. 564; Osman Yaşar, Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu, Cilt I, Seçkin Yayıncılık, Ankara, 2018, s. 1227.

15 Veli Özer Özbek/Koray Doğan/Pınar Bacaksız, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2021, s. 359.

16 Değirmenci, Sayısal Delil, s. 382.

17 Değirmenci, Sayısal Delil, ss. 309-310; Avrupa Konseyi Siber Suç Sözleşmesi Komitesi bünyesinde kurulan Bulut Delil Grubu (Cloud Evidence Group) tarafından yapılan bir çalışmada, buradaki tasnife benzer şekilde, bilgisayarda depolanan içerik verisi (stored content data) ve iletişime müdahale etmek gibi bir yöntemle toplanması gereken gelecekteki içerik verisi (future content data) şeklinde bir ayrıma gidilmiştir. Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: challenges (Discussion paper prepared by the T-CY Cloud Evidence Group), 26 Mayıs 2015, s. 9.

18 Değirmenci, Sayısal Delil, ss. 309-310.

19 Telekomünikasyon kavramı hakkında ayrıntılı bilgi için bkz Seydi Kaymaz, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Seçkin Yayıncılık, Ankara, 2015, ss. 51-54.

20 CMK m. 135 açısından önemli olan ortada bir iletişimin olup olmadığı ve bunun bir telekomünikasyon aracıyla yapılıp yapılmadığıdır. Yener Ünver/Hakan Hakeri, Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara, 2020, s. 432.

na girmez.[21] İletişimin dinlenmesi ve kayda alınması koruma tedbirine ileriye dönük olarak başvurulabilir.[22] İletişimin denetlenmesinden iletişimin yapıldığı anda dinlenmesi, kayda alınması veya okunması anlaşılmaktadır.[23] CMK m. 135 geleceğe yönelik, canlı iletişime ilişkindir.[24] Buradaki veri durağan değil, akış halindedir.[25] Bir başka ifadeyle telekomünikasyon yoluyla yapılan iletişimin denetlenmesiyle aktif veri trafiği tespit edilmektedir.[26] Geçmişte yapılan eş zamanlı iletişime ilişkin kayıtlar ise CMK m. 135'in konusuna girmez.[27] CMK m. 135'te telekomünikasyon araçları vasıtasıyla gerçekleştirilen eşzamanlı iletişimin denetlenmesi suretiyle akış halindeki sayısal verilerin elde edilmesi söz konusudur.[28] Bu tedbir uygulanırken çalışmakta olan bir cihaza kullanıcının haberi olmaksızın girilmekte[29] ve iletişimi denetlenmektedir. Yani bu koruma tedbiri mahiyeti icabı gizli bir koruma tedbiridir.[30] Aksi takdirde delil elde edilmesi mümkün değildir.

---

21 Dinleme yapılırken haberleşmenin gizliliğini sağlayan önlemlerin üstesinden gelinerek iletişimin içeriğini ortaya çıkaracak teknik araçlar kullanılmalıdır. Kapının arkasından kulak misafiri olunarak yapılan bir dinleme iletişimin denetlenmesi koruma tedbiri kapsamına girmez. Paolo Tonini, Manuale di procedura penale, Giuffrè, Milano 2010, s. 378. Örneğin, kişilerin bir araya gelerek herhangi bir araç kullanmadan gerçekleştirdikleri iletişim CMK m. 139'daki gizli soruşturmacı ve teknik araçlarla izleme koruma tedbiri kapsamında tespit edilebilir. Kaymaz, s. 56.

22 Sinyal bilgilerinin değerlendirilmesine ise ileriye veya geriye dönük olarak başvurulabilir. Nur Centel/Hamide Zafer, Ceza Muhakemesi Hukuku, Beta Basım Yayım, İstanbul, 2020, s. 497.

23 Kaymaz, ss. 47-49.

24 Mehmet Saydam, Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Oniki Levha Yayınları, İstanbul, 2011, s. 88; Yusuf Yaşar/İsmail Dursun, "Bilgisayarlar, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", *MÜHF-HAD*, C. 19, S. 3, s. 23.

25 Resul Göksoy, Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması, Seçkin Yayıncılık, Ankara, 2019, s. 194.

26 Frank Saliger, "Alman Ceza Muhakemesi Hukuku'na göre Telekomünikasyonun Denetlenmesi" (Çev. Murat Ceyhan), Ceza Muhakemesi Hukukunda Güncel Konular, İstanbul 2015, s. 135.

27 Kaymaz, ss. 47-49.

28 Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2020, s. 581; Değirmenci, Sayısal Delil, s. 382 vd.

29 Cumhur Şahin/Neslihan Göktürk, Ceza Muhakemesi Hukuku- I, Seçkin Yayıncılık, Ankara, 2021, s. 357; Ali Parlar/Ahmet Çetin, Ceza Muhakemesinde Soruşturma Evresi ve Uygulaması, Aristo Yayınları, İstanbul, 2017, s. 435.

30 Tonini, s. 378; Saydam, s. 156; İbrahim Şahbaz, "Koruma Tedbiri Olarak İletişim Denetlenmesi", Ceza Yargılaması Hukukunda Son Gelişmeler Sempozyumu, Ankara 2016, s. 32.

II. MESAJLAŞMA UYGULAMALARI

Günümüzde mesajlaşmak için e-posta ve sms (short message service)'in yanı sıra çeşitli anlık mesajlaşma uygulamaları da kullanılmaktadır. WhatsApp, Facebook Messenger, Bip, Instagram Direct Message (DM), Skype, Snapchat gibi internet tabanlı anlık mesajlaşma uygulamalarının GSM operatörleri tarafından sunulan konuşma ve mesajlaşma hizmetlerine ilave olarak ses, görüntü ve video paylaşımı, görüntülü konuşma, fotoğraf filtreleme gibi bazı ilave hizmetler sunması ve ücretsiz olması[31] bahse konu uygulamaların oldukça fazla tercih edilmesine sebep olmaktadır. Dolayısıyla bu uygulamalar vasıtasıyla gönderilen ve suçun aydınlatılması için gerekli olan mesaj, görüntü, ses kaydı ve/veya videoların hukuka uygun bir şekilde elde edilmesi önem kazanmaktadır. Ayrıca anlık mesajlaşma uygulamalarına nazaran daha köklü bir geçmişe sahip olan ve kullanım amacı ve şekli bakımından bu uygulamalarla benzer özellikler gösteren e-postalarda arama da günümüzdeki yaygın kullanımı dikkate alındığında halen önemini korumaktadır.

Kişiler arası iletişim kurulmasını sağlayan bu uygulamaların ortak özelliği, haberleşmenin baz istasyonları aracılığıyla değil internet üzerinden gerçekleştirilmesidir. İnternet üzerinden yapılan iletişimde, mobil telefonla baz istasyonu arasında olduğu gibi bir sinyal alışverişi değil, veri alışverişi söz konusudur. Maddenin CMK Tasarısındaki[32] gerekçesinde belirtildiği üzere, kişiler arası iletişimin her türlü kablolu veya radyo ve elektromanyetik sistemler gibi kablosuz sistemlere girilerek elde edilmesi mümkündür. Dolayısıyla CMK m. 135 internet üzerinden gerçekleştirilen iletişimin denetlenmesini de kapsar.[33]

---

31 Bu uygulamaların kullanılabilmesi için sadece internet bağlantısı yeterlidir. Operatörler tarafından sunulan sms hizmetinde olduğu gibi atılan her bir mesaj kullanıcının tarifesine tanımlı olan limitten düşmemekte veya atılan her bir mesaj için ücretlendirme yapılmamaktadır. Anlık mesajlaşma uygulamalarının bu kadar yaygınlaşmasının altında yatan önemli nedenlerden bir diğeri de budur.

32 Maddenin CMK Tasarısındaki gerekçesi ve Adalet Komisyonu Raporu için bkz. Cumhur Şahin, Ceza Muhakemesi Kanunu Gazi Şerhi, Seçkin Yayıncılık, Ankara, 2005, ss. 376-381.

33 Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi – Yargıtay Kararları Çerçevesinde Bir Değerlendirme", GÜHFD, C. 11, S. 1-2, Y. 2007, s. 1099; Değirmenci, Sayısal Delil, s. 385; Kaymaz, s. 151; Saydam, s. 88; Göksoy, s. 174; Yaşar/Dursun, s.24; Ersan Şen, Türk Hukuku'nda Telefon Dinleme Gizli Soruşturmacı X Muhbir, Seçkin Yayıncılık, Ankara, 2013, s. 85; İnternet üzerinden gerçekleştirilen canlı konuşma ve yazışmaların takibinin dinleme olarak nitelendiri-

E-postalar iki sunucu arasında akış halindeyken, alıcı hesabına ulaştığı anda durağan hale gelir.[34] ASSS'nin "Saklanan bilgisayar verilerinin aranması ve bunlara el konulması" kenar başlıklı 19. maddesine ilişkin açıklayıcı memorandumun 190. maddesinde elektronik postaların bu özelliği dikkate alınarak, e-postaları saklı bilgisayar verisi (durağan veri) veya akış halindeki veri olarak belirleme yetkisi taraf devletlere bırakılmıştır.[35] ASSS'yi onayladığımız[36] 9 Ağustos 2014 tarihinden beri mevzuatımızda bu konuda bir düzenlemeye gidilmediğinden bu konudaki çözüm öğreti ve uygulamaya bırakılmış gözükmektedir.

Öğretideki bir görüşe göre, e-posta yoluyla yapılan iletişim üç safhada gerçekleşir. İlk aşamada ileti, göndericinin e-posta hizmetini kullandığı araçtan (tablet, telefon, bilgisayar vs.) hizmet sağlayıcının posta sunucusuna (mail-server) gelir. İkinci aşamada hizmet sağlayıcının sunucusuna kaydedilen ileti gönderilmek üzere kısa bir süre bekletir. Üçüncü ve son aşamada ise ileti hizmet sağlayıcının ara sunucusundan alıcının posta sunucusuna gönderilir.[37] Elektronik posta ikinci aşamada, yani hizmet sağlayıcısının sunucusunda iken e-posta göndericinin posta kutusundan alıcının posta kutusuna nakledilmektedir. İletişimin bu aşamasında elektronik veri akış halindedir.[38] Dola-

lebileceğine ilişkin görüş için bkz. Asuman Aytekin İnceoğlu, "Türk Hukukunda Adli Amaçlı İletişimin Denetlenmesi", Uğur Alacakaptan'a Armağan Cilt-1, İstanbul 2008, ss. 109-110.

34 Değirmenci, Sayısal Delil, s. 310.

35 "Madde 19 saklı bilgisayar verileri için geçerlidir. Bu açıdan, alıcı kendi bilgisayar sistemine indirinceye kadar bir İnternet hizmet sağlayıcının posta kutusunda bekleyen e-posta mesajlarının saklı bilgisayar verisi olarak mı yoksa aktarım halindeki veri olarak mı değerlendirilmesi gerektiği sorusu ortaya çıkmaktadır. Bazı Taraf Ülkelerin mevzuatında bu e-posta mesajları iletişimin bir parçasıdır ve dolayısıyla içerikleri ancak müdahale yetkisini uygulayarak temin edilebilir. Bazı hukuk sistemlerinde ise bu mesajlar Madde 19'un kapsamına giren saklı veriler olarak görülür. Bu nedenle, Taraflar hangisinin kendi ulusal hukuk sistemlerine uygun olduğunu belirlemek için yasalarını incelemelidir". Siber Suç Uzmanları Komitesi, Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı (Çev. İnternet ve Hukuku Platformu), Ankara 2008, s. 206.

36 Türkiye'nin 10 Kasım 2010 tarihinde imzaladığı Avrupa Konseyi Siber Suç Sözleşmesi, "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak 29083 sayılı ve 9 Ağustos 2014 tarihli Resmî Gazete'de yayınlanarak onaylanmıştır.

37 Yenisey/Nuhoğlu, s. 459; Kaymaz, s. 44.

38 Değirmenci, Sayısal Delil, s. 333.

yısıyla CMK m. 135'e başvurulmalıdır.[39] Üçüncü aşamada, ara sunucudaki ileti alıcı tarafından çağrılarak açılır ve iletişim sona erer. Bu işlem özellikle kamu veya özel kurum ve kuruluşlarda kullanılması tercih edilen mailbox üzerinden gerçekleştirilebileceği gibi webmail üzerinden de gerçekleştirilebilir. Mailbox üzerinden okunan e-posta açıldığı anda bilgisayara kaydedilerek durağan veri haline geldiğinden artık bu aşamadan sonra CMK m. 134'ün konusunu teşkil eder. Ancak webmail hizmetinde alıcı, kullanıcı adı ve şifresini girmek suretiyle herhangi bir yer ve bilgisayardan kendine ait posta kutusuna girerek herhangi bir iletiyi bilgisayara kaydetmeksizin okuyabilmektedir.[40] Dolayısıyla e-posta hizmetinin sadece webmail üzerinden sunulduğu hallerde, kişinin bu iletinin içeriğini kullandığı bilgisayara kaydettiği haller ayrık kalmak üzere, ileti internet üzerindeyken elde edilirse iletişimin denetlenmesi söz konusudur.[41]

Öğretide yer alan ikinci bir görüşe göre ise, elektronik posta kutularında saklanan ve silinmiş bile olsa bilgisayarda yapılacak arama sonucu ele geçirilebilecek iletilerin CMK m. 134 kapsamında değil, CMK m. 135 kapsamında denetlenmesi gerekir. Burada iletişimin sona ermesi gerekçe gösterilerek CMK m. 135'in uygulanamayacağı, ayrıca bu durumun telekomünikasyon yoluyla yapılan iletişimin gizliliği ile de bağdaşmayacağı ileri sürülebilir. Ancak iletişimin özel olarak korunması ihtiyacına yanıt vermek için bu postalara CMK m. 135 kapsamında müdahale edilmesi şarttır.[42] Bu görüşün, iletişimin gizliliğinin özel olarak korunması ihtiyacına katılmakla birlikte, kanaatimizce burada CMK m. 135'te düzenlenen koruma tedbirinin ileriye dönük bir iletişimin varlığı ve gizlilik özelliklerini de dikkate alarak bir sonuca

---

39 Yenisey/Nuhoğlu, s. 460; Değirmenci, Sayısal Delil, s. 333; Özbek'e göre, e-posta haberleşmesinin ikinci aşamasında iletişimden söz edilemez. Dolayısıyla iletişimin denetlenmesi söz konusu olamaz. Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", *DEÜHFD*, C. 4, S. 1, Y. 2002, s. 132; Alman Federal Temyiz Mahkemesi de posta kutusundaki açılmamış e-postaların elde edilmesini iletişimin denetlenmesi kapsamında değerlendirmektedir. Kaymaz, s. 44.

40 Yenisey/Nuhoğlu, ss. 459-460; Bilgisayarda bulunan sabit veri şeklindeki e-postaların Alman Ceza Muhakemesi Kanundaki arama ve elkoyma hükümleri kapsamında elde edilebileceğine ilişkin bkz. Saliger, s. 135.

41 Yenisey/Nuhoğlu, s. 460; Sunucular arasında nakledilen e-postalar (ikinci aşama), paket toplama programları sayesinde toplanarak elde edilebilir. Değirmenci, Sayısal Delil, s. 333.

42 Tezcan vd., s. 612.

ulaşmak gerekir. Bu nedenle e-posta yoluyla yapılan iletişim denetlenmesinde bu iletişim türünü üç safhaya ayıran ve e-posta hizmetinin kullanıldığı platformların (mailbox-webmail) özelliklerini dikkate alarak bir sonuca ulaşan ilk görüşü benimsemek kanaatimizce daha yerinde olacaktır.

Mailbox, kullanılan bilgisayarda kurulu olan ve e-posta gönderip almaya yarayan bir programdır.[43] Mailbox üzerinden gönderilen e-postalar göndericinin bilgisayarındaki mailbox programının kurulu olduğu klasöre kaydedilmektedir. Aynı şekilde gönderilen e-posta alıcı tarafından mailbox üzerinden açılarak okunduğu zaman alıcının bilgisayarına kaydedilmektedir. E-postaların gönderilip alınmasının mailbox üzerinden gerçekleşerek bilgisayara kaydedildiği bu hallerde e-postalar durağan veri haline geldiklerinden bizce de CMK m. 134'ün konusunu teşkil ederler.[44] E-posta içeriğinin iletişimin yapıldığı sırada elde edilmesi bakımından ise CMK m. 135'te düzenlenen koruma tedbirine başvurulacaktır.[45] E-posta göndericiden hizmet sağlayıcının posta sunucusuna, hizmet sağlayıcının posta sunucusundan ise alıcıya nakledilirken akış halindedir. Verilerin akış halinde olduğu sunucular arasında gerçekleşen bu nakil sırasında, e-postalar bazı paket toplama programları aracılığıyla elde edilebilir. Bu kapsamda elde edilen delillerin hukuka uygun olması için iletişimin denetlenmesi koruma tedbirine başvurulmalıdır.[46] Ancak e-postayla yapılan iletişimin ikinci aşamasında, yani gönderilen e-postanın mail-server üzerinde kısa süre de olsa beklediği aşamada kanaatimizce CMK m. 134'e başvurulması gerekir. Bu aşamada e-posta mail-sunucusunda kayıtlı durağan veri haline gelerek iletişim sona ermiş ve alıcıya nakledilmeyi beklemektedir. Ayrıca hizmet sağlayıcının posta sunucusunun bulut depolama

43 Microsoft Outlook buna örnek gösterilebilir.

44 E-posta okunarak bilgisayara kaydedildiği anda iletişim sona ermiştir. Dolayısıyla CMK m. 134'e başvurulmalıdır. Kaymaz, s. 47; Öğretide Alman Anayasa Mahkemesinin bir kararından yola çıkılarak, ele geçirilen cep telefonundaki mesajların arama ve elkoyma kararına istinaden okunamayacağı, arama ve elkoyma ile iletişimin denetlenmesi kararlarının icrasının birbirinden farklı hak ve menfaatleri ihlal ettiği, e-posta gönderilerinin okunmasının iletişime yönelik bir müdahale olduğu bu nedenle e-postaların içeriğinin okunması gerekiyorsa iletişimin denetlenmesine ilişkin karar alınması gerektiği ifade edilmektedir. Aytekin İnceoğlu, ss. 110-111.

45 Kaymaz, s. 61.

46 Değirmenci, Sayısal Delil, s. 333.

alanı niteliğinde olan bir veri depolama birimi olduğuna işaret etmekte fayda vardır. Örneğin, Google'ın sunduğu bulut depolama hizmeti olan Google One, kendi e-posta hizmeti olan Gmail'deki e-postaları da burada depolamaktadır.[47] Çalışmamızın bulut bilişime ilişkin kısmında detaylı olarak açıklanacağı üzere, bulutta depolanan verilerin elde edilmesi bakımından verinin saklandığı yere bakılarak bir sonuca ulaşılması gerekir. Hizmet sağlayıcısının posta sunucusu (mail-server), yani gönderilen e-postanın saklandığı depolama merkezi yurt içinde bulunabileceği gibi yurt dışında da bulunabilir. Hizmet sağlayıcının mail sunucusunun yurt dışında bulunduğu hallerde CMK m. 134 kapsamında arama yapılması başka bir devletin yargılama yetkisine müdahale niteliğinde olacaktır. Aynı şekilde e-posta hizmetinin webmail üzerinden kullanıldığı hallerde e-postayla gerçekleştirilen iletişim hangi aşamada olursa olsun gönderilen ileti gönderici veya alıcının kullandığı bilgisayar, akıllı telefon veya tabletin dahili hafızasında değil hizmet sağlayıcıya ait bulut depolama alanında bulunmaktadır. Dolayısıyla webmail vasıtasıyla gönderilen iletilerin elde edilmesi bakımından da bulut bilişimin özelliklerinin dikkate alınması gerekir.

Anlık mesajlaşma uygulamaları, sms ve elektronik posta yoluyla gerçekleştirilen iletişim türlerinde olduğu gibi haberleşme özgürlüğü kapsamında değerlendirilmelidir. Dolayısıyla anlık mesajlaşma uygulamaları veya kısa mesaj yoluyla gerçekleştirilen iletişim de e-posta gibi değerlendirilerek CMK m. 135 kapsamında denetlenebilir.[48] Alınan dinleme kararında CMK m. 135/4'te ifade edildiği üzere, tedbirin uygulanacağı kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodun belirtilmesi gerektiğinden usulüne uygun olarak alınan bir karar kapsamında telefonu dinlenen şüphelinin, bu uygulamalar vasıtasıyla internet üzerinden de iletişime geçtiği tespit edildiğinde bu konuda ayrı bir kararın alınması gerekir. Çünkü artık iletişimin gerçekleştirildiği araç ve ortam değişmiştir. Alınan bu yeni karar önceki karar üzerinde değişiklik yapan bir karar olduğundan internet üzerinden yapılan iletişimin

47 Gmail'in yanı sıra Google Photos ve Google Drive'da kayıtlı olan veriler de bu depolama alanına kaydedilmektedir. Bkz. https://one.google.com/about (Erişim Tarihi: 28.02.2023).

48 Göksoy, s. 175; Şen, X Muhbir, s. 85.

denetlenmesine ilişkin bu yeni kararın süresi önceki karardaki dinleme süresinin bitiş tarihini geçemeyecektir.[49]

Sms ve elektronik posta yoluyla gerçekleştirilen iletişimde olduğu gibi anlık mesajlaşma uygulamaları bakımından da geçmişte gerçekleştirilen iletişimin içeriğine nasıl erişilmesi gerektiği hususu öğretide tartışmalıdır. WhatsApp, Facebook Messenger, Bip, Skype gibi bu uygulamaların anlık mesajlaşma uygulaması olarak adlandırılması tercih edilse de[50] bu uygulamalarla yazılı olarak mesajlaşmanın[51] yanı sıra sesli ve/veya görüntülü iletişim ve dosya, görüntü, ses veya video paylaşımı yapılabilmektedir. Dolayısıyla geçmişte gerçekleştirilen iletişimin içeriğine hukuka uygun olarak erişebilmesi için bu uygulamalarının kendilerine özgü çalışma prensipleri ve özelliklerini de dikkate alarak bir sonuca ulaşılması gerekir.

Doktrinde aksi ileri sürülse de[52] bir kez daha ifade etmek gerekir ki geçmişe dönük haberleşmenin dinleme ve kaydetme şeklinde denetiminin yapılması mümkün değildir.[53] Ancak iletişim sona erdikten sonra bu uygulamalar iletişimin içeriğine ilişkin bilgileri kullanılan telekomünikasyon aracının hafızasında veya kendilerine ait sunucularda depolayabilmektedir. Öğretideki depolanmış iletişimin CMK m. 129'da düzenlenen postada elkoyma hükümlerine göre elde edilmesine ilişkin görüş, bu sorunun çözümü için yetersizdir. Çünkü CMK m. 129'un konusu mektup gibi maddi varlığı bulunan gönderilere ilişkin-

49 Kaymaz, ss. 357-358.

50 Göksoy, s. 103.

51 Öğretide yer alan bir görüşe göre, CMK m. 135 hükmünde yazılı iletişimin denetlenebileceğine ilişkin açık bir hüküm bulunmamaktadır. Madde metni ve bu konudaki yönetmelik dikkatlice okunduğunda sürekli konuşma üzerine odaklanıldığı görülmektedir. Madde gerekçesinde her ne kadar elektronik posta yoluyla yapılan iletişimin CMK m. 135'e tabi olduğu ileri sürülse de madde metni yazılı iletişimin denetlenmesine imkân vermemektedir. Dolayısıyla elektronik posta, sms veya anlık mesajlaşma uygulamalarıyla yapılan yazışmalar CMK m. 135 kapsamında denetlemeye konu olamaz. Bunun için yasal düzenleme yapılması gerekir. Yaşar, ss. 1280-1281.

52 "…CMK'nın 135. maddesi sadece ileriye dönük iletişimin denetlenmesini değil, aynı zamanda usule uygun karar almak şartıyla geçmişe yönelik iletişimin denetlenmesine de imkân tanımaktadır. 135. madde, denetimin fiilen mümkün olması kaydıyla ileriye veya geriye doğru iletişim denetlenmesi arasında bir ayrıma gitmemiş ve engel de koymamıştır." Şen, X Muhbir, s. 229.

53 Kaymaz, s. 43.

dir.[54] Depolanmış iletişimin içeriğine ulaşılması CMK m. 135 kapsamına da girmez.[55] Çünkü iletişim yapılarak bitmiş ve artık bu iletişimin içeriği bilgisayarda, kullanılan cihazın hafızasında veya uygulamanın sunucusunda kayıtlı bir veri haline gelmiştir.[56] Dolayısıyla burada tartışılması gereken husus CMK m. 134'teki koruma tedbirine başvurularak bu verilerin elde edilip edilemeyeceğidir. Ayrıca durağan veri haline gelmiş iletişim içeriklerinin nerede depolandığının tespiti de bu konu bakımından önem arz etmektedir.

Öğretide yer alan bir görüşe göre, CMK m. 134 kapsamında alınan arama kararına istinaden yapılan arama neticesinde elde edilen iletişim içerikli verilerin delil olarak kullanılabilmesi için bu verilerin kişi tarafından ayrıca bilgisayara kaydedilmiş olması gerekir. İletişim içerikli bu verilerin bilgisayar tarafından otomatik olarak kaydedildiği ya da kişinin özgür iradesiyle kaydedilmediği hallerde bilgisayarda arama sonucu elde edilen bu verilerin delil olarak kullanılabilmesi için CMK m. 135 uyarınca ayrıca karar alınmış olması gerekir. Ancak yazar bu görüşün aksinin de savunulabileceğini, yani kullanıcının iradesi dışında kaydedilen iletilerin haberleşme özelliğini kaybederek bilgisayara kayıtlı bir veri haline geldiği ve bu yüzden CMK m. 134'ün kapsamına girdiği görüşünün de ileri sürülebileceğini ifade etmektedir.[57] Kanaatimizce bu konuda iletinin kullanıcının iradesiyle veya ira-

---

54 Kaymaz, s. 50; Almanya'da verilen bir kararda, Facebook üzerinden gönderilen mesajlar, posta yoluyla mektup veya telgraf göndermeye benzetilmiş ve Facebook'taki mevcut ve kalıcı sohbet içerikleri hakkında postada elkoyma hükümleri kıyasen uygulanmıştır. Saliger, s. 144.

55 Kaymaz, s. 49.

56 Ünver/Hakeri'ye göre, iletişim ve ileti kavramlarını aynı şeylermiş gibi ele alarak ileti kaydedilmeden önceki işlemleri CMK m. 135-138 kapsamında, kaydedildikten sonra ise CMK m. 134 kapsamında gören bu görüş yerinde değildir. Burada önemli olan verinin kaydedilmesi değil, bir iletişimin varlığıdır. Eğer halihazırda bir iletişim mevcut ise CMK m. 135, iletişim sona ermişse CMK m. 160 ve devamındaki hükümler uygulanabilir. CMK m. 135 açısından önemli olan telekomünikasyon aracıyla gerçekleştirilen bir iletişimin olmasıdır. Ünver/Hakeri, s. 432; Aynı yönde bkz. Bahri Öztürk/Behiye Eker Kazancı/Sesim Soyer Güleç, Ceza Muhakemesi Hukukunda Koruma Tedbirleri Seçkin Yayıncılık, Ankara, 2022, s. 303; Aksi görüşe göre, iletişim bitmiş olsa da bu verilere erişimle kişinin temel hak ve hürriyetlerine müdahale edildiğinden bunun kanunda açıkça düzenlenmesi gerekir. Dolayısıyla anlık mesajlaşma uygulamalarıyla veya kısa mesaj olarak gönderilen iletiler e-posta gibi değerlendirilerek iletişim anında delil elde etmek için CMK m. 135, iletişim sona erdikten sonra ise CMK m. 134 uygulanmalıdır. Göksoy, s. 175.

57 Şen, X Muhbir, ss. 228-229.

desi dışında kaydedilmiş olması arasında bir ayrıma gidilmesine gerek yoktur. Öncelikle anlık mesajlaşma uygulamasının kullanıldığı tablet, akıllı telefon veya bilgisayarın hafızasına kaydedilen iletinin kullanıcının iradesiyle mi yoksa iradesi dışında mı kaydedildiğini tespit etmek her zaman için mümkün olmayabilir. Adli bilişimdeki ilerlemeler dikkate alınarak bunun oldukça kolay bir şekilde tespit edilebileceği düşünülse bile, kullanıcı bu iletilerin otomatik olarak kaydedildiğini bilmesine rağmen bunun aksini ileri sürebilir ve böylece elde edilen delilin hukuka aykırılığı gündeme gelebilir. Örneğin, CMK m. 134 kapsamında yapılan bir arama sonucu elde edilen WhatsApp'tan gönderilen bir videonun kullanıcının iradesi dışında kaydedildiği ve haberleşme özgürlüğü kapsamında değerlendirilmesi gereken bu iletinin hukuka uygun delil sayılabilmesi için CMK m. 135 kapsamında elde edilmesi gerektiği ileri sürülebilir. Bu tarz istenmeyen durumların önüne geçebilmek adına bilişim ve iletişim fonksiyonlarına sahip cihazlarda yapılacak aramalarda bu koruma tedbirlerinin her ikisine birden başvurulması düşünülebilir.[58] Ancak bu ihtimalde de CMK m. 134'ün uygulama alanı CMK m. 135'te sayılan katalog suçlarla sınırlanmış olacaktır. Oysa bilgisayarlarda arama koruma tedbirine herhangi bir sınırlamaya tabi olunmaksızın işlenen her türlü suç için başvurulabilir. Ayrıca bu konudaki bir diğer eksiklik, bilişim suçlarına CMK m. 135'te sayılan katalog suçlar arasında yer verilmemiş olmasıdır. Bilişim suçlarında genellikle başka türlü delil elde etme imkânı bulunmaz.[59] Dolayısıyla bilişim suçları hakkında hukuka uygun olarak delil elde edilebilmesi için CMK m. 134 ve m. 135'teki tedbirlere aynı anda başvurulması mümkün değildir. Öğretide haklı olarak bilişim suçlarına katalog suçlar arasında yer verilerek bu eksikliğin giderilmesi gerektiği ifade edilmektedir.[60] Netice itibariyle kullanıcının ister kendi iradesiyle ister iradesi dışında kaydedilmiş olsun anlık mesajlaşma uygulamalarındaki iletişim içeriği eğer bu uygulamanın kullanıldığı

58 Bu görüş için bkz. Dülger, ss. 593-594.

59 Bilişim suçlarında genellikle başka türlü delil elde edilemeyeceğinden CMK m. 134'teki tedbire son çare olarak başvurulması muhakemenin amacına ulaşmasını riske atacak, fail ve delillere ulaşılması oldukça güçleşecektir. Dülger, s. 585.

60 Düzenlemedeki bu eksiklik uygulamada, bilişim suçlarının örgüt faaliyeti çerçevesinde işlendiği varsayılmak suretiyle giderilmekte ve katalog suçlar arasında sayılan TCK m. 220 hükmüne dayanılarak iletişimin tespiti, dinlenmesi ve kayda alınması kararı alınmaktadır. Dülger, s. 594.

cihazın hafızasına kaydedilmişse CMK m. 134'e göre karar alınması yeterli olacaktır. Hafızadan kastımız kullanılan cihazda veri depolanması için ayrılmış dahili hafıza ile cihazın haricen takılacak kartlarla yükseltilebilir hafızasıdır.

CMK m. 135'in ileriye dönük iletişimin denetlenmesine imkân vermesi ve bu koruma tedbirinin kullanıcıdan habersiz gizli bir koruma tedbiri olması özelliklerini dikkate alarak geçmişe dönük iletişim içeriklerinin tespiti için bu iletilerin bilgisayara kaydedilip kaydedilmemesini dikkate alarak ulaştığımız sonuç yukarıda izah edilmiştir. Ancak anlık mesajlaşma uygulamaları bu içerikleri kurulu olduğu cihaza kaydetmiyor ve bu iletiler anlık mesajlaşma hizmetini sunan kuruluşun sunucusunda depolanıyorsa ne yapılması gerektiği hususunun cevaplanması gerekir.

Anlık mesajlaşma uygulamaları web üzerinden de hizmet vermektedir. Yani bu uygulamalar herhangi bir uygulama yüklenmeden hizmetin sağlandığı internet adresinin girilmesi suretiyle de kullanılabilir. Örneğin, sosyal medya platformlarından Facebook'un anlık mesajlaşma uygulaması olan Messenger'a ya da bir diğer popüler mesajlaşma uygulaması olan WhatsApp'a web tabanı üzerinden erişilebilmektedir.[61] Bu uygulamalara web üzerinden erişilerek gerçekleştirilen iletişimin içeriği kullanılan cihazın hafızasına değil hizmet sağlayıcının veri depolama merkezlerine kaydedilmekte, daha sonra mobil uygulama vasıtasıyla erişim sağlandığında hizmet sağlayıcının serverlarında kayıtlı bulunan bu veriler internet aracılığıyla senkronize edilerek uygulamanın yüklü bulunduğu mobil cihazda kayıtlı bir veri haline gelmektedir.[62] Kanaatimizce web tabanlı anlık mesajlaşma uygulamaları ile webmail üzerinden sunulan elektronik posta hizmetleri birbirleriyle benzerlik göstermektedir. Dolayısıyla WhatsApp, Facebook Messenger gibi mesajlaşma platformlarının kullanılan cihaza

---

61 Facebook Messenger uygulamasına www.messenger.com adresinden, WhatsApp uygulamasına web.whatsapp.com adresinden herhangi bir uygulamaya ihtiyaç duyulmadan erişilebilir.

62 Örneğin, WhatsApp uygulamasına herhangi bir internet tarayıcı üzerinden (Google Chrome, Mozilla Firefox, Microsoft Edge, Yahoo vb.) erişim sağlanarak gerçekleştirilen görüşmeler, gönderilen ses, video veya görüntü içerikleri internet tarayıcı kapatıldıktan sonra kaybolmamakta, yapılan görüşmelere ait bu içerik WhatsApp'ın veriyi depoladığı yerden internet aracılığıyla senkronize edilerek uygulamanın kullanıldığı mobil cihaza da aktarılmaktadır.

yüklenen bir uygulama ile değil de web tabanı üzerinden kullanıldığı hallerde webmail üzerinden gönderilen e-posta içeriğinin tespitiyle aynı sonuca ulaşmak gerekir. Bu platformlardan gerçekleştirilen geçmişe yönelik iletişimin içeriği ancak kullanılan cihaza kaydedildiği takdirde CMK m. 134 kapsamında elde edilebilir. İletişimin kullanılan cihaza kaydedilmediği hallerde ise, iletişimin içeriğine ilişkin bilgiler kullanılan mesajlaşma platformuna ait depolama biriminde kayıtlı bir veri olarak kalacaktır. Bu verilere erişilmesi bulut depolama birimlerinde kayıtlı verilerle benzerlik gösterdiğinden çalışmamızda bulutta depolanan verilerin elde edilmesiyle ilgili ulaştığımız sonuçlar, iletişimin hizmet sağlayıcıya ait depolama birimlerinde depolandığı bu haller bakımından da geçerli olacaktır.

Anlık mesajlaşma uygulamaları üzerinden gerçekleştirilen iletişimin tespit edilmesinin önündeki en büyük engel bu uygulamalardan bazıları tarafından kullanılan uçtan uca şifreleme özelliğidir. Uçtan uca şifreleme özelliği,[63] gönderilen mesaj, video veya ses kaydı gibi içeriklerin sadece gönderici ve alıcı tarafından görülmesini sağlayan bir özelliktir. Bu özellik sayesinde gönderilecek ileti göndericinin cihazından çıkmadan şifrelenmekte ve bu şifreyi çözecek anahtar sadece alıcıda bulunmaktadır. Mesajların iletilmesine aracılık eden hizmet sağlayıcı hiçbir surette şifrelenmiş iletilerin içeriğini göremeyeceği gibi yapılan aramaları da dinleyemez. Uçtan uca şifreleme kişisel verilerin yasadışı yollardan elde edilmesini önleyerek kullanıcıları korumak adına getirilen bir özellik olsa da bu özellik anlık mesajlaşma uygulamalarından sayısal delil elde edilmesini neredeyse imkânsız hale getirdiğinden kötüye kullanılmaya müsaittir. Uçtan uca şifreleme özelliği bulunan anlık mesajlaşma uygulamalarıyla gerçekleştirilen geleceğe yönelik canlı iletişim, CMK m. 135 kapsamında tespit edilemeyeceği gibi bu iletişimin içeriğinin uygulamayı kullanıma sunan hizmet sağlayıcısından elde edilmesi de zor gözükmektedir. Çünkü akış halindeki veri şifrelidir ve bu şifreyi çözecek anahtar sadece alıcı da bulunmaktadır. Dolayısıyla CMK m. 135 kapsamında tespit edilen şifreli ileti adli bilişim yöntemleriyle çözülmedikçe dinlemeyi gerçekleştiren kolluk kuvvetleri tarafından iletinin içeriğine erişilemez. Aynı

63 WhatsApp'ın kullandığı uçtan uca şifreleme özelliği hakkında ayrıntılı bilgi için bkz. https://faq.whatsapp.com/791574747982248/?helpref=uf_share (Erişim Tarihi: 28.02.2023)

şekilde hizmet sağlayıcının da elinde şifrelenmiş gönderiden başka bir şey bulunmadığından talep edilmesi halinde adli makamlarla paylaşabilecek tek veri şifreli iletiler olacaktır. Kaldı ki uçtan uca şifreleme özelliğini kullanan WhatsApp teslim edilen mesajlar ve bu mesajlara ilişkin log kayıtlarını saklamamakta, teslim edilemeyen mesajları ise 30 gün sonra sunucularından silmektedir. Bu nedenle gerçekleştirilen iletişime ilişkin kayıtların şifreli de olsa WhatsApp'tan temini mümkün olmayabilir. WhatsApp tarafından yapılan bilgilendirmede kolluk kuvvetleri ile profil fotoğrafı, varsa hakkımda bilgisi, grup bilgileri ve telefon rehberlerinin paylaşılabileceği ifade edilmektedir. Yani WhatsApp'ın sunucularından elde edilebilecek veriler bu sayılanlardan ibarettir.[64] Uçtan uca şifreleme özelliğinin sayısal delillerin elde edilmesi bakımından yarattığı bu sorunların çözümü toplum ve bireylerin suça ve suçluya karşı korunması gerekliliği bakımından büyük önem arz etmektedir.

III. BULUT BİLİŞİM ve SOSYAL MEDYA

A. Genel Olarak

Bulut bilişim, bilgisayar tabanlı hizmet ve uygulamaların internet üzerinden paylaşılması ve bu kaynakların internet bağlantısı olan her yerden erişilmesi ve çalıştırılmasını sağlayan[65] dış kaynak kullanımına dayalı bir bilgi teknolojisidir.[66] Dünya üzerinde 4.62 milyar insanın

---

64 WhatsApp'ın kolluk kuvvetlerine yönelik bilgilendirmesi için bkz. https://faq.whatsapp.com/800085810452992/?helpref=uf_share (Erişim tarihi: 28.02.2023).

65 Murat Topaloğlu/Harun Özkişi/Egemen Tekkanat, Bulut Bilişim, Seçkin Yayıncılık, Ankara, 2017, s. 19; Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bulut bilişimi şu şekilde tanımlamıştır: "Bulut bilişim, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza, uygun koşullarda ve isteğe bağlı olarak her zaman, her yerden erişime imkân veren bir modeldir. Söz konusu kaynaklar (bilgisayar ağları, sunucular, veri tabanları, uygulamalar, hizmetler vb.) asgari düzeyde yönetimsel çaba ve hizmet alıcı-hizmet sağlayıcı etkileşimi gerektirecek kolaylıkta tedarik edilebilmekte ve elden çıkarılabilmektedir." BTK, Bulut Bilişim, Ankara 2013, s. 3, https://www.btk.gov.tr/uploads/pages/slug/bulut-bilisim.pdf (Erişim Tarihi: 28.02.2023); NIST'in tanımı için bkz. NIST, Cloud Computing Standards Roadmap, Temmuz 2013, s. 8, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf (Erişim Tarihi: 28.02.2023).

66 bkz. Metin Turan, Bulut Bilişim, Seçkin Yayıncılık, Ankara 2019, s. 72.

aktif olarak kullandığı[67] sosyal medya ise web 2.0 teknolojisi[68] sayesinde kullanıcıların kendi içeriklerini oluşturabildiği ve aralarında etkileşime geçebildiği çift yönlü bir medya alanıdır.[69] Bulut bilişimdeki üç farklı hizmet modelinden[70] sayısal delillerin elde edilmesi bakımından en önemli olanı veri depolama hizmetinin sunulduğu IaaS hizmet modelidir.[71] Ayrıca sosyal ağ hizmetleri gibi çeşitli yazılım ve uygulamaların, genellikle web tarayıcısı aracılığıyla kullanıcıların hizmetine sunulduğu SaaS[72] da sosyal medyanın yaygın kullanımı dikkate alındığında bir diğer önemli sayısal delil kaynağıdır. Sosyal medya bir iletişim aracı olmakla birlikte yapılan paylaşımlar ilgili platformun sunucusunda kayıtlı olduğu için aynı zamanda verilerin bulutta depolanması söz konusudur.[73] Dolayısıyla sağladığı avantajlar[74] sayesinde kullanımı giderek artan bulut bilişim ile halihazırda oldukça geniş bir kullanıcı kitlesine sahip olan sosyal medya mecralarındaki sayısal delillerin hukuka uygun surette elde edilmesi hususuna açıklık kazandırılması gerekir. Burada üzerinde durulan hususun farklı bulut yazılımları veya sosyal medya ortamlarıyla internet üzerinden gerçek-

---

67 We are Social'ın Dijital 2022 Raporuna göre, 7.91 milyarlık dünya nüfusunun 4.95 milyarı internete erişim sağlamakta ve bunların 4.62 milyarı sosyal medyayı aktif olarak kullanmaktadır. https://wearesocial.com/us/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ (Erişim Tarihi: 28.02.2023).

68 Web teknolojileri sırasıyla web 1.0, web 2.0, sosyal medya, bulut bilişim ve web 3.0 şeklinde gelişim göstermiştir. Turan, ss. 103-104.

69 Sosyal medya ve web 2.0 hakkında ayrıntılı bilgi için bkz. Turan, s. 59 vd.

70 Bulut bilişimdeki hizmet modelleri hakkında bkz. Henkoğlu, ss. 215-217; Peter Mell/Timothy Grance, The NIST Definition of Cloud Computing, NIST Special Publication, 2011, ss. 2-3.

71 Değirmenci, Sayısal Delil, s. 158.

72 Turan, s. 80, 92; Sosyal medya ortamlarını SaaS olarak değerlendiren görüş için bkz. Bo-Wen Yang vd.: "Cloud Computing Architecture for Social Computing – A Comparison Study of Facebook and Google", 2011 International Conference on Advances Social Networks Analysis and Mining, 2011, s. 741; Bulut bilişimin hizmet türlerinden biri olan SaaS'ta kullanıcı bir yazılımı satın almak yerine onu hizmet sağlayıcıdan kiralamaktadır. Windows Live, Hotmail, Google Docs uygulamaları buna örnek olarak gösterilebilir. Johndavid Kerr/Kwok Teng, "Cloud Computing: legal and privacy issues", Journal of Legal Issues and Cases in Business, Vol. 1, 2012, s. 3.

73 Aynı yönde bkz. Göksoy, s. 105.

74 Bulut bilişimin avantajları hakkında bkz. TBMM, Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu, Haziran 2012, https://acikerisim.tbmm.gov.tr/xmlui/handle/11543/2781 (Erişim Tarihi: 28.02.2023), s. 262-263; Topaloğlu/Özkişi/Tekkanat, ss. 21-23.

leştirilen iletişimin içeriğini tespit etmek olmadığını belirtmekte yarar vardır. Zira bu konu yukarıda etraflıca tartışılmıştır. Bu başlık altında bulut bilişimin karakteristik yapısı dikkate alınarak bulutta veya sosyal medyada depolanan, yani akış halinde olmayan ses, görüntü veya video gibi sayısal delil niteliğindeki verilerin elde edilme yöntemleri ve bu yöntemlerin hukuka uygunluğu üzerinde durulacaktır.

B. Bulutta Depolanan Verilere Erişim Yöntemleri

1. Genel Olarak

Bulutta depolanan sayısal delil niteliğindeki veriler farklı yöntemlerle elde edilebilir. Bu yöntemler; CMK m. 134'te düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama koruma tedbirine başvurmak, karşılıklı adli yardımlaşmaya başvurmak ve bulut hesabına ait kullanıcı bilgilerinin girilmesi suretiyle bulutta depolanan verilerin elde edilmesi olarak tasnif edilebilir. Bunlarla ilgili açıklamalara geçmeden önce bulutta depolanan verilere erişim yöntemlerinin hukuka uygunluğuna ilişkin öğretideki görüşlerin şekillenmesinde referans noktalarından biri olan buluttaki verilerin nerede depolandığına[75] ilişkin sorunun çözüme kavuşturulması gerekir.

Bulut veya bulut özelliğine sahip sosyal medya platformlarındaki veriler bulut hizmet sağlayıcısına ait yurt içi veya yurt dışında bulunan veri merkezlerinde depolanmaktadır.[76] Söz konusu veriler sabit olarak bu veri merkezlerinden herhangi birinde depolanabileceği gibi verilerin bulut hizmet sağlayıcısına ait veri merkezleri arasında sürekli hareket halinde olması da mümkündür. Bulutta depolanan verilerin sürekli hareket halinde olması verilerin depolandığı yerin tespit

---

75 Öğretide bulutta depolanan verilerin konumu ve bu verilere erişim noktasındaki farklılıklardan yola çıkılarak bulut hizmetlerinin geleneksel sınıflandırmasına alternatif teşkil edecek bir sınıflandırmaya gidilmiştir. Bu sınıflandırmaya göre, data shard, data localization ve data trust olmak üzere üç farklı bulut yönetim modeli vardır. Bu ayrımın data localization olarak adlandırdığı modele çalışmamızın ilerleyen kısımlarında tekrar değinilecektir. Söz konusu sınıflandırma hakkında detaylı bilgi için bkz. Paul M. Schwartz, "Legal Access To The Global Cloud", *Columbia Law Review*, Vol. 118, No. 6, s. 1694 vd.

76 Mesut Orta, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), Yetkin Yayınları, Ankara, 2015, s. 213; Topaloğlu/Özkişi/Tekkanat, s. 80.

edilmesini güçleştirir.[77] Veriler sabit bir merkezde depolansa bile yargı yetkisinin bulut hizmet sağlayıcısının merkezinin bulunduğu yer, verilerin depolandığı yer veya şüphelinin vatandaşı olduğu ya da bulunduğu yerlerden hangisine ait olacağı hususu tartışmalı kalacaktır.[78] Ayrıca bulut hizmet sağlayıcının merkezi ile verilerin depolandığı yer farklı yargı bölgelerinde olabileceği gibi verilerin bulut hizmet sağlayıcısı tarafından ceza adaletini önlemek için sistematik olarak farklı yargı bölgelerine taşınması da mümkündür.[79] Bu sorunları aşabilmek için bulut hizmet sağlayıcıların veri depolama merkezlerinde bulunan sayısal delil niteliğindeki verilerin bütünlüğünün ve geçerliliğinin nasıl sağlanacağı ve verilerin elde edilmesine ilişkin yargı yetkisinin nasıl belirleneceği,[80] bir başka ifadeyle buluttaki verilere hukuka uygun olarak nasıl erişilebileceğinin bulut bilişimin özellikleri dikkate alınarak cevaplanması gerekir.

2. Koruma Tedbirine Başvurmak Suretiyle

Bulutta depolanan verilerin elde edilmesi için başvurulacak yöntemlerden ilki delil elde etmenin klasik yöntemlerinden olan koruma tedbirine başvurulmasıdır. Burada CMK m. 134'te düzenlenen koruma tedbirinin bulutta arama yapmak için kullanılıp kullanılamayacağının üzerinde durulması gerekir.[81] CMK m. 134'te *"şüphelinin kullandığı bilgisayar, bilgisayar programları ile bilgisayar kütüklerinde"* arama yapılmasından bahsedilmektedir. Bulut bilişimde fiziken kullanılan bilgisayardan bir web tarayıcı, yazılım geliştirme ortamı veya sanal alt yapı yöneticisi aracılığıyla hizmet sağlayıcının dünyanın herhangi bir yerinde bulunan sunucularına erişim sağlanmaktadır. Örneğin, alt yapı hizmetinin sunulduğu IaaS'ta kullanıcı bu hizmete bağlandığı bilişim aracının donanımsal özelliklerinden bağımsız olarak bulut sağlayıcısından ihtiyaçları doğrultusunda kiraladığı sanal donanımlar

77 Bulut bilişimin en önemli dezavantajlarından biri verilerin nerede olduğunun bilinmemesidir. Henkoğlu, s. 219, 220.

78 T-CY, Discussion Paper, ss. 10-11.

79 Cybercrime Convention Committee (T-CY), Criminal justice Access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (Final report of the T-CY Cloud Evidence Group), 26 Eylül 2016, para. 40, s. 15.

80 T-CY, Discussion Paper, s. 14.

81 Olgun Değirmenci, "Bulut Bilişim ve Beraberinde Getireceği Hukuksal Sorunlar Üzerine Görüşler", *Terazi Hukuk Dergisi*, C. 12, S. 136, Y. Aralık 2017, s. 110.

(depolama alanı, işlemci, ram vs.) doğrultusunda işlem gücüne sahip olmaktadır.[82] Yani bulut bilişimde fiziki değil, sanal[83] bir kullanım söz konusudur. Dolayısıyla madde metnindeki *"şüphelinin kullandığı"* ibaresindeki kullanma kavramı hem fiziki hem de sanal kullanım olarak anlaşılmalıdır.[84]

Sanal kullanımın CMK m. 134'ün madde metninde yer alan *"şüphelinin kullandığı"* ibaresi kapsamına girdiğini belirledikten sonra bulut bilişimin bilgisayar, bilgisayar kütüğü veya programı kavramlarından herhangi birinin kapsamına girip giremeyeceğini tespit etmek gerekir. Öğretide yer alan bir görüşe göre, bilgisayar kütüğü kavramı bulut formunda depolama hizmeti sunan sistemleri de kapsamaktadır.[85] Bu görüşle örtüşen bir başka görüşe göre ise, Google Drive, Yandex Disk gibi internet ortamında depolama hizmeti sunan bulut depolama alanları Adli ve Önleme Aramaları Yönetmeliği (Yönetmelik) m. 17/3'te geçen *"uzak bilgisayar kütükleri"* kavramı kapsamında değerlendirilmekte ve CMK m. 134 kapsamında bulutta arama yapılabileceği ileri sürülmektedir.[86] Bilgisayar kütükleri, insan müdahalesi ile bilişim sistemi tarafından oluşturulup saklanan dosyalardır.[87] Bu tanım dikkate alındığında, kanaatimizce de bulut ortamlarını bilgisayar kütüğü kavramı kapsamında değerlendirmek gerekir. Ancak Yönetmelik m. 17/3 hükmüne dayanarak bulutta arama yapılabileceğine ilişkin görüşe katılmamız mümkün değildir. CMK m. 134 ve Yönetmelik m. 17 hükümleri kıyaslandığında bilgisayarlarda aramaya ilişkin kayda değer tek farkın, elkoyma sırasında yapılacak olan sistemdeki verilerin yedeklenmesi işleminin *"bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları"* hakkında da uygulanması gerektiğine dair ibare olduğu görülmektedir. Öğretide yer alan bir görüşe göre, kanundaki yetersiz düzenlemeye ilişkin eksiklik Yönetmeliğe eklenen bu ibareyle gide-

82 Topaloğlu/Özkişi/Tekkanat, s. 53.
83 Bulut bilişimde kullanılan sanallaştırma teknolojisi için bkz. Turan, ss. 99-102.
84 Değirmenci, Sayısal Delil, ss. 321-322.
85 Bu görüşe göre, CMK m. 134'teki "bilgisayar, bilgisayar programları ve bilgisayar kütükleri" kavramı yerine TCK'da kullanılan "bilişim sistemi" ibaresinin kullanılması daha yerinde bir tercih olacaktır. Dülger, s. 585.
86 Yaşar/Dursun, s. 16, 20; Yaşar, s. 1228; Yönetmelik'te yer alan bu hükmün her hal ve şart altında uzaktan arama veya onun bir türü olan bulutta aramaya izin veren bir düzenleme olarak değerlendirilmemesi gerekir. Değirmenci, "Bulut Bilişim", s. 110.
87 Değirmenci, Sayısal Delil, s. 53.

rilmeye çalışılarak yasanın uygulama alanı genişletilmiştir.[88] Kanaatimizce bu hususta, verilerin bilişim sistemlerinin yapı taşı olduklarını[89] unutmamak gerekir. Çalışmamızın başında da belirttiğimiz üzere, CMK m. 134 ve 135'teki koruma tedbirlerine yer verilmesinin nedeni maddi gerçeğin ortaya çıkarılmasını sağlayacak sayısal verileri elde etmektir. Devletlerin toplumu ve bireyleri bilişim suçlarına ve aydınlatılması için sayısal delil elde edilmesi gereken diğer suçlara karşı koruma yükümlülüğü bulunmaktadır.[90] Dolayısıyla ister bilgisayarda isterse bilgisayara bağlanabilen bir USB veya hard diskte ya da bir bilgisayar ağı ya da uzak bilgisayar kütüğünde depolansın elektronik ortamda kayıtlı her türlü veriye erişilebilmesi gerekir.[91] Kullanıcıya ait verilerin bilgisayarda veya bulutta bulunması arasında bir fark yaratılmamalıdır.[92] Ancak bunu yaparken Anayasa m. 13 hükmünde yer alan temel hak ve hürriyetlerin kanunla sınırlanması gerekliliği gözden kaçırılmamalı, gerekli yasal zemin hazırlanmalı ve belirlilik ilkesine riayet edilmelidir. Aksi halde bu tarz tartışmalarının ve uygulama kaynaklı farklılıkların oluşması kaçınılmazdır. Ayrıca CMK m. 134 hükmü, AİHS m. 8 ile güvence altına alınan özel hayata saygı hakkını ilgilendirdiğinden bu hakka yönelik müdahaleler AİHS m. 8/2'de ifade edildiği üzere hukuka uygun olmalıdır. Hukuka uygunluk ibaresi yapılan müdahalenin yasayla öngörülmesini, açık ve öngörülebilir olmasını gerektirir.[93] Anayasa m. 13 ve AİHS m. 8/2 hükümleri dikkate alındığında, bulutta arama ve elkoymanın sınırlarının kanunla net bir şekilde belirlenmesi gerektiği sonucuna ulaşılmaktadır.[94] Temennimiz bu yönde olmakla birlikte arzu edilen yasal düzenleme yapılana kadar öğretide ileri sürüldüğü üzere

88 Yenisey/Nuhoğlu, s. 463.
89 Özbek/Doğan/Bacaksız, s. 362.
90 T-CY, Final Report, para. 17, s. 9.
91 Değirmenci'ye göre, kanun koyucunun iradesi veri merkezli düzenleme yapılmasına ilişkindir. Zira veri fiziki bir varlık olsaydı zaten CMK m. 116 hükmü arama yapılması için yeterli olacaktır. Ancak kanun koyucu verinin soyut yapısını dikkate alarak CMK m. 134'te özel bir düzenleme getirmiştir. Dolayısıyla CMK m. 134'ün odak noktasının veri olarak alınması gerekir. Değirmenci, Sayısal Delil, s. 331.
92 Değirmenci, Sayısal Delil, s. 243.
93 De Tommaso/İtalya, Başvuru Nu. 43395/09, 23.02.2017, para. 106-107.
94 Online aramanın kanunilik ilkesine aykırılık teşkil edeceği ve bunun için bir yasal düzenleme yapılması gerektiğine dair görüş için bkz. Candide Şentürk Akaner, Bir Koruma Tedbiri Olarak Online Arama ve Türk Hukukunda Uygulanabilirliği, Seçkin Yayıncılık, Ankara, 2022, ss. 185-186.

CMK m. 134/1'deki bilgisayar kütüğü kavramının bulut formunda depolanan verileri de kapsadığını[95] ve CMK m. 134 kapsamında alınan arama kararına istinaden bulutta arama yapılabileceğini[96] kabul etmek kanaatimizce de yerinde olacaktır. Ancak bu görüşümüz aşağıda açıklanacağı üzere, buluttaki verilerin saklandığı depolama birimlerine fiziki erişimin mümkün olduğu, bir başka deyişle fiziksel olarak arama ve elkoyma yapılabilen hallerle sınırlıdır.

Uygulamada CMK m. 134 kapsamında verilen arama kararlarında şüphelinin kullandığı bilgisayar, cep telefonu vb. dijital cihazlar üzerinde söz konusu karara istinaden arama yapılabileceğine ilişkin genel ibarelere yer verilmektedir.[97] Arama kararlarında genel ibarelere yer verilerek neyin, ne zaman, nerede aranacağının belirlilik ilkesi çerçevesinde sınırlandırılmaması aramayı bir keşif aramasına dönüştürmekte[98] ve bilgisayarlarda aramanın en son çare olarak başvurulması gereken ikincil nitelikte bir koruma tedbiri olması hususu göz ardı edilmektedir.[99] Kanaatimizce bu şekilde tanzim edilen bir arama kararı ile şüphelinin kullandığı bulut hesaplarında arama yapılamaz. Özel bir arama türü olan bilgisayarlarda aramaya ilişkin CMK m. 134'te arama kararında bulunması gereken hususlara ilişkin CMK m. 135/4'te olduğu gibi özel bir düzenlemeye yer verilmediğinden genel hüküm olan CMK m. 119'a gidilir. CMK m. 119/2-b'ye göre, arama kararında aramanın konusunun açıkça belirtilmesi gerekir.[100] Dolayısıyla bu konuda yukarıda belirttiğimiz kriterlerde bir düzenleme

---

95 Dülger, s. 585; Bulut bilişim sistemlerini "şüphelinin kullandığı bilgisayar kütükleri" kapsamında kabul eden benzer görüş için bkz. Dilek Özge Uğraş, "Bilgisayarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", *TBBD*, S. 154, Y. 2021, s. 116.

96 Değirmenci, Sayısal Delil, s. 243.

97 CMK m. 134 kapsamında verilen arama kararlarında, "El konulan bilgisayar, cep telefonu vb. dijital eşyalar üzerinde Ceza Muhakemesi Kanunu'nun 134. maddesinde belirtilen usule göre inceleme yapılmasına" ibaresine yer verilmektedir. Örnek arama kararı için bkz. Ahmet Aslan, Cumhuriyet Savcısı ve Soruşturma, Adalet Yayınevi, Ankara, 2018, s. 560.

98 Değirmenci, Triyaj, s. 68.

99 Olgun Değirmenci, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m. 134), 7145 sayılı Kanun'la Yapılan Değişikliklerin Değerlendirilmesi", *Terazi Hukuk Dergisi*, C. 13, S. 13, Kasım 2018, s. 151.

100 CMK m. 119/2-b'de aramanın yapılacağı eşyadan söz edilmektedir. Ancak bahsettiğimiz üzere bilgisayar kütükleri ve sayısal deliller soyut kavramlardır. Dolayısıyla bu ibareyi aramanın konusu olarak kabul etmek gerekir.

yapılana kadar CMK m. 134 kapsamında verilecek arama kararında, şüphelinin kullandığı bulut ve sosyal medya hesaplarında da inceleme yapılabileceği hususuna açıkça yer verilmesi yerinde olacaktır. Arama kararında sadece bilgisayar, harddisk veya cep telefonu gibi dijital cihazlardan söz edilmiş ve bu cihazlar üzerinde yapılan inceleme sonucu şüphelinin kullandığı bulut, sosyal medya ve e-mail hesaplarının kullanıcı adı ve şifrelerine erişilmişse[101] bu verilerin tesadüfen elde edilen delil olarak kabul edilmesi ve durumun derhal Cumhuriyet Savcılığına bildirilerek (CMK m. 138) CMK m. 134 kapsamında bu hesaplara erişilip bulutta arama yapılabilmesi için yeni bir karar talep edilmesi gerekir. Zira bulutta depolanan veriler aramanın konusunu teşkil eden dijital cihazın dahili hafızasında değil bulut hizmet sağlayıcısına ait veri depolama merkezlerinde, yani farklı bir bilişim cihazında bulunmaktadır.

Bulut bilişime ilişkin yapılan ayrımlardan bir diğeri dağıtım modelleri dikkate alınarak yapılan sınıflandırmadır. Bulut bilişim dağıtım modelleri genel (kamusal) bulut, özel bulut, hibrit bulut ve topluluk bulutu olmak üzere dörde ayrılır.[102] Hizmetin kullanıma sunulduğu kitle bakımından yapılan bu sınıflandırmada özel bulut ve genel bulut yapı itibariyle birbirlerinden ayrışmaktadır. Özel bulut, belirli bir kurum veya kuruluşun kullanımına tahsis edilen ve kurum dışından kişilerin erişimine kapalı olan bulut bilişim türüyken, genel bulut ise bulut bilişim altyapısının web tarayıcılar ve programlar vasıtasıyla internet üzerinden talep eden herkesin kullanımına sunulduğu dağıtım modelidir.[103] Genel bulut ile özel bulut arasındaki en önemli fark bulut bilişim altyapısı üzerindeki hakimiyete ilişkindir. Genel bulutta alt yapı hizmet sağlayıcının kendi veri merkezlerinde yer almaktayken,[104] özel bulutta kurulumun gerçekleştirileceği kuruluş altyapı hizmeti üzerinde sahiplik, yönetim ve işletme yetkilerine sahiptir.[105]

---

101 Ayrıca web tarayıcıları e-posta hesaplarıyla da ilişkilendirilebildiğinden, bu şifreler mail hesabıyla da senkronize edilebilmekte ve o e-posta hesabıyla giriş yapılan her cihazdan kaydedilen tüm şifrelere erişilebilmektedir.

102 Mell/Grance, s. 3.

103 Vanni Boncinelli, "Modelli tecnici e discipline giuridica del c.d. cloud computing", Rivista italiana di informatica e diritto, 3, 1 (lug. 2021), s. 31; Henkoğlu, s. 216.

104 Turan, s. 82; Topaloğlu/Özkişi/Tekkanat, s. 60.

105 Turan, s. 81; Kuruluşlar veri güvenliğine ilişkin nedenlerle çoğunlukla özel bulutu tercih etmektedirler. Boncinelli, s. 32.

Genel ve özel bulut dağıtım modellerinin söz konusu yapıları dikkate alınarak CMK m. 134 kapsamında bulutta arama yapılabileceğine ilişkin yukarıda ulaştığımız sonucun yeniden ele alınması gerekir. Öğretide dar kapsamlı ve özel bir ağda verilen bulut hizmetine ilişkin hesap bilgilerinin ve bu hesap bilgilerine ait verilerin hukuka uygun olarak verilen arama kararına istinaden elde edilebileceği ve bu surette bulutta depolanan verilere ulaşılıp kopya alınmasının mümkün olabileceği ileri sürülmektedir.[106] "Sunulana-özel" bulut bilişim hizmeti olarak da adlandırılan özel bulutta, bu hizmetten faydalanan kurum ve kuruluşların sistem üzerinde yüksek derecede kontrol imkânına sahip olması ve dışarıya kapalı olan bu özel ağın sadece ilgili kuruluşun kullanımına açık olması[107] dikkate alındığında kanaatimizce bu görüşe katılmak gerekir. Özel bulut alt yapısı, ilgili kişi veya kuruluşun kendi bünyesinde olduğundan[108] elde edilmek istenen delillerin bulunduğu depolama birimlerine fiziken erişim mümkündür. Dolayısıyla CMK m. 134 kapsamında alınan arama kararına istinaden özel buluttan delil elde edilebilir. Öğretide Yönetmelik m. 17/3'te yer alan uzak bilgisayar kütükleri ibaresinin ancak aramanın yapıldığı yerde bulunan yerel iletişim ağları üzerinde, yani özel bulutta, arama yapılmasına cevaz vereceği ifade edilmektedir.[109] Örneğin, bir şirket bünyesinde yapılan arama sırasında, şirket bilgisayarlarının bağlı olduğu ağdaki "ortak" klasörüne herhangi bir bilgisayardan erişim sağlanarak arama yapılabilir. Ayrıca özel bulutta, genel bulutta olduğu gibi birçok kullanıcıya ait verinin tek bir yerde depolanması söz konusu olmadığından soruşturmayla ilgisi olmayan kişilerin verilerine ulaşılarak bu kişilerin temel hak ve hürriyetlerinin ihlal edilmesi tehlikesi[110] de daha az olacaktır.

Genel bulut bakımından ise hizmet sağlayıcının yurt içinde veya yurt dışında olmasına göre ikili bir ayrıma gidilmelidir. Bu ayrıma

---

106 Değirmenci, Sayısal Delil, s. 242.

107 Topaloğlu/Özkişi/Tekkanat, ss. 61-62.

108 Özge Dereboylular, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği", CHD, S. 39, Y. 14, s. 170.

109 Örneğin, bir işyerinde yerel ağ bağlantısıyla birbirlerine bağlı olan bilgisayarlardan birine giriş yapılarak, ağa bağlı diğer bilgisayarlar üzerinde arama yapılabilir. Değirmenci, Sayısal Delil, ss. 365-366.

110 Bulutta birçok kişiye ait veri tek bir yerde depolandığından bulut depolama birimlerinin tamamının değil, sadece kullanıcının verilerinin depolandığı kısmın imajının alınması gerekir. Değirmenci, "Bulut Bilişim", s. 110; Dereboylular, s. 170, 176.

gidilmesinin nedeni, devletlerin yargı yetkisinin kendi coğrafi sınırlarıyla belirlenmesine ilişkin ülkesellik (mülkilik) ilkesidir. Bu ilkeye göre, kural olarak hiçbir devlet başka bir devletin topraklarında yargı yetkisini kullanamaz.[111] Uluslararası hukukun temel ilkelerinden biri olan ulusal düzenlenmeleri uygulama yetkisinin[112] ihlal edilmemesi için bu ayrıma gidilmesi bir zorunluluktur.

Yurt içinde bulunan genel bulut hizmet sağlayıcısına ait olan ve iletişimin içeriğiyle ilgili olmayan IP adresi, hizmet türü ve hizmetin alındığı zaman dilimine ilişkin bilgiler CMK m. 135'te düzenlenen iletişimin tespiti hükümlerine göre elde edilir. Bulut hizmetinin kullanıldığı cihaz ile bulut hizmet sağlayıcısının alt yapısı arasında bir iletişim söz konusu olduğundan[113] bu bilgilere CMK m. 160 kapsamında[114] erişilemez. Bulutta depolanan ve kullanıcıya ait verilerin elde edilmesi için ise CMK m. 134'e göre alınan arama kararı yeterli olacaktır.[115] Örneğin, veri depolama merkezleri Türkiye'de bulunan[116] Turkcell Bulut hizmetini kullanan bir kullanıcının bulutta sakladığı ve ceza soruşturması kapsamında elde edilmesi gereken delil niteliğindeki bir veriye CMK m. 134 kapsamında erişilebilir. Ancak unutulmamalıdır ki, CMK m. 134 kapsamında yapılacak arama şüpheli tarafından kullanılan alanla sınırlı olacaktır.[117]

Yurt dışından sunulan genel bulut hizmetlerinde ise CMK m. 134 kapsamında arama yapılması başka bir devletin egemenlik alanına müdahale teşkil edeceğinden mümkün değildir.[118] Bir başka ifadey-

111 T-CY, Final Report, para. 42, s. 15.

112 Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş Birliği", MÜHF-HAD Prof. Dr. Nur Centel'e Armağan, C. 19, S. 2, Y. 2013, s. 1234.

113 Telekomünikasyon kavramının iki bilgisayar arasındaki veri alışverişini kapsamadığına, dolayısıyla telekomünikasyonun denetlenmesi koruma tedbiri kapsamında tespit edilemeyeceğine dair görüş için bkz.
Saliger, s. 141; İnternete bağlı bilgisayarın başka bir bilgisayarla iletişiminin CMK m. 135 kapsamında dinlenebileceğine ilişkin görüş için bkz. Değirmenci, Sayısal Delil, s. 386.

114 Cumhuriyet savcısının genel soruşturma yetkisi, şüphelinin temel hak ve hürriyetlerine müdahale teşkil edebilecek nitelikteki araçlara başvurulmasına müsaade etmez. Saliger, s. 138.

115 Değirmenci, Sayısal Delil, ss. 242-243.

116 Turkcell Bulut'un veri merkezleri Ankara, Gebze, İzmir ve İstanbul Avrupa yakasındadır. https://turkcellbulut.com/homepage (Erişim Tarihi: 28.02.2023).

117 Değirmenci, Sayısal Delil, ss. 330-331.

118 Değirmenci, "Bulut Bilişim", s. 110.

le, yurt dışından hizmet sunan ve veri depolama merkezleri yurt dışında bulunan genel bulut hizmet sağlayıcılarındaki veriler CMK m. 134 kapsamında alınan arama kararına istinaden elde edilemez. Yargı yetkisine tecavüzün yanı sıra elde edilmek istenen veriler yurt dışında bulunan bir bilgisayar kütüğünde depolandığından, bu kütüğe yurt içinden fiziken erişim imkânı da yoktur. CMK m. 134 kapsamında yapılan arama daha önce ifade ettiğimiz üzere bilgisayarın fiziki varlığına yönelik olduğundan yurt dışındaki bilgisayar kütüklerinde bulunan verilerin CMK m. 134 kapsamında elde edilemeyeceği aşikardır.

Farklı bir yöntem olarak yurt dışında depolanan verilerin uzaktan erişim yoluyla elde edilmesi düşünülebilir. Nitekim Alman hukukunda ASSS m. 19/2 hükmüne uyum sağlanması amacıyla uzaktan arama yapılabilmesine imkân sağlanmıştır.[119] ASSS'nin "*Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması*" kenar başlıklı 19. maddesinin 2. fıkrası hükmüne göre,[120] yetkili merciler kendi yargı yetkisi içerisinde bulunan bilişim sistemlerinde soruşturma kapsamında elde edilmesi gereken bir sayısal delil olduğuna ilişkin makul şüpheye ulaşırsa, arama kararının kapsamını genişleterek bu sistemler üzerinde de arama yapabilir.[121] ASSS m. 19/2 hükmü, taraf devletlerden her birine kendi ulusal sınırları içerisinde yapılacak aramaların kapsamını genişletmek için gerekli yasal düzenlemeleri yapma yetkisi tanımaktadır.[122] Bu hüküm doğrultusunda Alman Ceza Muhakemesi Kanununda (StPO) 2007 yılında yapılan değişiklikle, aranan verilerin kaybolma tehlikesinin bulunması ve söz konusu verilerin bulunduğu sisteme uzaktan erişimin mümkün olması halinde uzaktan arama yapılabilmesine ilişkin bir düzenleme yapılmıştır.[123] Vurgulamak gerekir ki, StPO m. 110 tarafından tanınan bu yetki genel bulut hizmet sağlayıcıların yurt içinde depoladığı veriler bakımından söz konusudur. Mevzuatımızda ise Alman hukukunda olduğu gibi, ASSS m. 19/2'un

119 Uğraş, s. 112.
120 ASSS m. 19 hükmü için bkz. https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf (Erişim Tarihi: 28.02.2023).
121 Yenisey/Nuhoğlu, s. 455.
122 ASSS m. 19 hükmü taraf devletlerin kendi ulusal sınırları içerisinde uygulayabilecekleri tedbirlere ilişkindir. Dereboylular, s. 194.
123 Uzaktan aramaya ilişkin StPO m. 110 hükmü hakkında bkz. Uğraş, s. 112.

verdiği yetki kapsamında uzaktan arama veya online arama[124] yapılmasına ilişkin herhangi bir düzenlemeye gidilmemiştir. Daha önce değinildiği üzere, Adli ve Önleme Aramaları Yönetmeliği m. 17/3'te geçen *"uzak bilgisayar kütükleri"* kavramına dayanarak uzaktan arama yapılabileceğine ilişkin görüşe de kanunilik ilkesi karşısında katılmamız mümkün değildir. Mevcut CMK m. 134 hükmü bilgisayar kütüklerine fiziken erişimin mümkün olduğu hallerde arama yapılmasına müsaade etmektedir. Bu nedenlerle gerekli yasal düzenleme yapılana kadar uzaktan arama yöntemiyle elde edilen deliller hukuka aykırı delil statüsündedir.[125]

Yukarıdaki açıklamalardan sonra yurt dışından hizmet sunan ve kullanıcılarına ait verileri yurt dışında depolayan genel bulut hizmet sağlayıcılarındaki verilerin elde edilmesi için başvurulabilecek tek yöntemin aşağıda detaylı olarak açıklanacağı üzere karşılıklı adli yardımlaşma olduğunu ifade etmek gerekir.[126] Avrupa Konseyi de özellikle içerik verileri için[127] karşılıklı adli yardımlaşmayı, farklı ülkelerin yargı yetkisinde bulunan delillerin elde edilmesinde başvurulacak temel yöntem olarak görmektedir.[128]

---

124 Kanaatimizce uzaktan arama ve online arama kavramları birbirlerinin yerine geçecek şekilde kullanılmamalıdır. Çünkü StPO m. 100 b/1'de düzenlenen online arama, çeşitli casus yazılımlardan faydalanarak şüphelinin kullandığı bilişim sistemine gizlice erişilip veri toplanması amacıyla başvurulan bir koruma tedbiridir. StPO m. 110/3'te düzenlenen uzaktan aramada ise; şüphelinin kullandığı ve aramanın konusunu teşkil eden bilişim sisteminden ayrı olduğu için fiziken erişilemeyen veri depolama alanına, uzaktan erişim sağlanarak aramanın kapsamı genişletilmektedir. Gizli bir soruşturma tedbiri olan online aramada tıpkı iletişimin denetlenmesinde olduğu gibi şüphelinin kullandığı bilişim sistemindeki tüm hareketleri eş zamanlı olarak izlenip kayıt altına alınmaktadır ve şüpheli bundan haberdar değildir. StPO m. 100 b/1'de düzenlenen online arama hükmü hakkında ayrıntılı bilgi için bkz. Şentürk Akaner, s. 70 vd.; Tezcan vd., ss. 565-567.

125 Aynı yönde bkz. Dereboylular, ss. 183-184.

126 "Bulut hizmetini sunan hizmet sağlayıcısının ülke sınırları dışında bulunması durumunda, bulutta arama yapılması ve verilere el konulmasının adli yardımlaşma hükümleri kapsamında yerine getirilmesi gerekecektir." Değirmenci, Sayısal Delil, s. 243.

127 T-CY, Final Report, para. 90, s. 35; Bir ceza soruşturmasında abone bilgileri, trafik verileri ve içerik verisi olmak üzere üç tür veriye ihtiyaç duyulur. Bu üç tür veriden elde edilmesi en ağır şartlara tabi tutulan veri türü içerik verisidir. T-CY, Discussion Paper, s. 7.

128 T-CY, Discussion Paper, s. 14.

3. Adli Yardımlaşma

Yurt dışındaki veri depolama merkezlerinde saklanan verilerin elde edilmesi için başvurulması gereken adli yardımlaşmaya ilişkin genel ilkelere[129] ASSS m. 25'te yer verilmiştir. Bu hükme göre; taraflar bilgisayar sistemleri ve verileriyle ilgili suçlara ilişkin soruşturma ve kovuşturmalar kapsamında sayısal delil toplanması için birbirlerine *"mümkün olan en geniş ölçüde"* gerekli kolaylıkları sağlayacaklardır. Taraf devletlere yüklenen bu yükümlülük bilgisayar sistemiyle işlensin veya işlenmesin sayısal delil toplanmasını gerektiren bütün suçlar için söz konusudur. Ayrıca acil durumlarda, adli yardımlaşma talebinde bulunmak için kullanılacak iletişim aracının güvenilir olması kaydıyla, faks ve elektronik posta gibi hızlı iletişim araçları kullanılabilir. Adli yardımlaşma süreci yürütülürken temel hak ve hürriyetlerin güvence altına alınması adına kural olarak taraflar arasındaki ikili antlaşma hükümleri ve kendisinden talepte bulunulan tarafın ulusal mevzuatı dikkate alınır. Adli yardımlaşma konusu fiilin her iki ülke mevzuatında suç olarak düzenlenmesi gerekir. Bu noktada önemli olan fiilin suç olarak düzenlenmesi olup taraf devletlerin söz konusu fiile ilişkin hukuki nitelendirmesinin farklı olması adli yardımlaşma talebinin olumsuz cevaplanmasını gerektirmez.[130]

ASSS'nin *"Saklanan bilgisayar verilerine erişilmesine ilişkin yardımlaşma"* kenar başlıklı 31. maddesinin 1. fıkrasına göre taraf devletlerden her biri, ASSS'ye taraf başka bir ülkenin sınırları içerisinde bulunan bilgisayar sistemleri aracılığıyla saklanan verilerin araştırılması, bu verilere erişilmesi, el konulması, elde tutulması ya da açıklanması amacıyla talepte bulunabilir. ASSS m. 31/2'ye göre, talepte bulunulan devlet ASSS ve karşılıklı adli yardımlaşma anlaşmaları uyarınca bu talebe cevap verecektir. İlgili verilerin kaybolma ya da değiştirilme tehlikesinin bulunduğu haller ile tarafların karşılıklı anlaşmaları gereği hızlı bir iş birliği yapılmasının öngörüldüğü hallerde adli yardımlaşma taleplerinin daha hızlı cevaplanması gerekir (ASSS m. 31/3). Hızlı

---

129 Adli yardımlaşma ayrı bir makale konusu olacak kadar geniş bir konudur. Bu nedenle adli yardımlaşma konusu çalışmamızda ASSS kapsamında ele alınacak ve sayısal delillerin elde edilmesi bakımından etkili bir yöntem olarak kabul edilmeyen bu yöntemin nasıl daha etkili hale getirilebileceği üzerinde durulacaktır.

130 Karşılıklı adli yardımlaşmaya dair genel ilkeler hakkında detaylı bilgi için bkz. Önok, s. 1251 vd.

cevap yükümlülüğünü gerektiren acil durumlarda 7 gün 24 saat çalışan irtibat noktaları[131] ve irtibat görevlileri ile taraflar arasındaki adli ağlar ve polis teşkilatları arası iş birliğinden yararlanılır.[132]

İnternet kullanımının giderek artması ve dünyanın farklı yerlerinde faaliyet gösteren şirketler tarafından depolanan kullanıcılara ait muazzam miktardaki sayısal veri karşılıklı adli yardımlaşma taleplerinin sayısının son yıllarda çarpıcı bir şekilde artmasına neden olmuştur.[133] Bu talep artışı öyle bir noktaya gelmiştir ki, kullanıcılara ait verilerin büyük çoğunluğunu ellerinde bulunduran ABD merkezli şirketlerden sayısal delil elde edilmesine ilişkin adli yardım talepleri, ABD'de karşılıklı adli yardımlaşma sürecinin işleyişini zora sokarak bu taleplere yanıt verme sürelerini oldukça yavaşlatmıştır.[134] Öyle ki adli yardımlaşma taleplerindeki bu artış sayısal delillerin elde edilmesi bakımından karşılıklı adli yardımlaşmayı etkili bir yöntem olmaktan çıkartacak seviyeye ulaşmıştır. Adli yardımlaşma taleplerinin 6 ila 24 aylık sürelerde cevaplanması pek çok adli yardım talebinden ve dolayısıyla ceza soruşturmasından vazgeçilmesine yol açmaktadır.[135] Artan talep sayısının yanında, temel hak ve hürriyetleri güvence altına almak için tasarlanan adli yardımlaşma prosedürleri sürecin yavaş işlemesine neden olmakta ve adli yardımlaşma sürecini daha maliyetli hale getirmektedir.[136] Bu nedenlerle adli yardımlaşma bulut ortamında saklanan delillerin elde edilmesinde her zaman işe yarayacak, gerçekçi bir çözüm yolu değildir.[137]

Bulut ortamında saklanan sayısal deliller kolaylıkla yok edilerek kararlılabileceğinden[138] adli yardımlaşma sürecinin en hızlı şekilde işletilmesi gerekir. Bunun için de adli yardımlaşmayı hızlandıracak yeni

131 ASSS'nin 35. maddesinde "24/7 Ağı" olarak adlandırılan bu irtibat noktalarının kurulması için özel bir hükme yer verilmiştir.
132 Cybercrime Convention Committee (T-CY), T-CY assesment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime (Adopted by the T-CY at its 12th Plenary), 3 Aralık 2014, s. 124.
133 U.S. Department of Justice (DOJ), Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019, s. 3.
134 DOJ, s. 10.
135 T-CY, Final Report, para. 17, s. 9
136 Boncinelli, s. 38.
137 T-CY, Final Report, para. 19, s. 9.
138 Değirmenci, "Bilgisayarlarda", s. 151.

yöntemlerin keşfedilmesi şarttır.[139] Avrupa Konseyi Siber Suç Sözleşmesi Komitesi (T-CY) bünyesinde kurulan Bulut Delil Grubu (CEG), ASSS'nin karşılıklı adli yardımlaşmaya ilişkin hükümleri hakkındaki değerlendirme raporunda adli yardımlaşma sürecine ilişkin tespit ve değerlendirmelerde bulunarak bu sürecin hızlandırılması için tavsiyelerde bulunulmuştur. Raporda CEG tarafından ulaşılan bazı önemli sonuçlar[140] ile bu sonuçlar doğrultusunda adli yardımlaşma sürecinin hızlandırılmasına ilişkin yapılan tavsiyeler[141] şunlardır:

- Sayısal delillerinin elde edilmesinde karşılıklı adli yardımlaşma sürecinin olması gerektiği gibi hızlı ve etkili bir şekilde işletilememesinin önündeki en büyük engellerden biri ASSS ve diğer anlaşmaların sunduğu imkanların taraf devletlerce tam olarak kullanılamamasıdır. Bu yüzden ASSS'nin başta koruma tedbirlerine ilişkin hükümleri olmak üzere tüm hükümleri taraf devletlerce uygulanmalıdır. (1 Numaralı Tavsiye)

- Adli yardımlaşma sürecinin işleyişine ilişkin taraf devletlerin ellerinde yeterli veri ve istatistik yoktur. Bu durum adli yardımlaşma sürecinin etkinliğinin izlenmesini imkânsız hale getirmektedir. Taraf devletler kendi bünyelerinde oluşturacağı çeşitli mekanizmalarla gerekli verilerin toplanması ve istatistiksel çalışmaların yapılmasını sağlayabilir. (2 Numaralı Tavsiye)
- Taraflar, bilişim suçlarıyla mücadele ve sayısal delillerin elde edilmesinde karşılıklı adli yardımlaşma, polis teşkilatları arası iş birliği ve diğer uluslararası iş birliği yöntemlerini geliştirebilmek için daha iyi eğitimler vermeli, bu eğitimler özellikle hâkim ve savcılara yönelik olmalı, yargı makamları arasında doğrudan iş birliği teşvik edilmeli ve yapılacak eğitimler Avrupa Konseyi tarafından desteklenmelidir. (4 Numaralı Tavsiye)
- Raporda, adli yardımlaşma süreçlerinin yavaş işlemesinin polis teşkilatları arasındaki iş birliğinin daha fazla tercih edilmesine yol açtığı bilgisine yer verilmektedir.[142] O halde, taraf devletler arasında yapılacak anlaşmalarla polisten polise iş birliği karşılık-

139 Önok, ss. 1235-1236.
140 CEG tarafından ulaşılan sonuçlar için bkz. T-CY, Assessment Report, ss.123-125.
141 Raporda sunulan tavsiyeler için bkz. T-CY, Assessment Report, ss. 125-127.
142 6 numaralı sonuç (Concl 6) için bkz. T-CY, Assessment Report, s. 123.

lı adli yardımlaşmaya alternatif olarak kullanılabilir. 7 numaralı tavsiyede de uluslararası iş birliği için taraf devletlerin karşılıklı adli yardımlaşma ve polisten polise iş birliği gibi her türlü kanalı kullanması gerektiği ifade edilmektedir.

- Adli yardımlaşma talepleri, genellikle ya eksik ya çok geniş olmakta ya da çifte cezalandırılabilirlik (dual criminality) şartı olarak adlandırılan, adli yardımlaşma talebine konu fiilin her iki ülke hukukuna göre de suç teşkil etmesi gerekliliğini taşımamaktadır. Bu nedenle talepte bulunulan devletin iç hukukun bilinmesi, bu konuda görevli personele daha fazla eğitim verilmesi ve adli yardımlaşma taleplerinde kullanılacak çok dilli şablonların hazırlanması sürecin hızlandırılması adına faydalı olacaktır.[143] Adli yardımlaşma taleplerinde bulunması gereken tüm bilgilere eksiksiz olarak yer verilmelidir. (12 Numaralı Tavsiye)
- CEG tarafından ulaşılan sonuçlardan bir diğeri, talep edilen verilerin kaybolma veya değiştirilme tehlikesinin olduğu hallerde taraf devletlerin ASSS m. 31/3'te öngörülen hızlı cevaplandırma yükümlülüğüne uymamasına ilişkindir.[144]
- Bazı acil durumlarda hizmet sağlayıcılar kendilerine yapılan taleplere doğrudan yanıt verebilmektedir. Bu hallerde adli yardımlaşmaya başvurmak yerine yabancı hizmet sağlayıcılarla doğrudan temasa geçilerek talepte bulunulması daha hızlı yanıt alınabilmesini sağlayacaktır.[145]
- Taraf devletlerin en çok talep ettiği veri türü kullanıcıya ait abone bilgileridir. Adli yardımlaşma taleplerini yanıtlamakla sorumlu makamlara ağır bir yük getiren bu taleplerin cevaplanması için farklı bir prosedürün izlenmesi karşılıklı adli yardımlaşmayı daha verimli hale getirecektir. Yapılacak yasal değişiklikler ve karşılıklı anlaşmalarla abonelik bilgilerinin hızlı bir şekilde talep eden devlete verilmesine imkân sağlanmalıdır. (19 Numaralı Tavsiye)
- Karşılıklı iki veya çok taraflı anlaşmalarla özellikle karmaşık davalardaki koordinasyonu kolaylaştırmak için müşterek soruştur-

143 8 numaralı sonuç (Concl 8) için bkz. T-CY, Assessment Report, s. 124.
144 13 numaralı sonuç (Concl 13) için bkz. T-CY, Assessment Report, s. 124.
145 15 numaralı sonuç (Concl 15) için bkz. T-CY, Assessment Report, ss. 124-125.

ma ekiplerinin (Joint Investigative Team-JIT) kurulması sayısal delillerin elde edilmesini kolaylaştıracaktır. (23 Numaralı Tavsiye)

Yukarıda sayılan tavsiyelerin yanı sıra adli yardımlaşma sürecinde görevli makamlara teknoloji okuryazarı personellerin görevlendirilmesi (3 Numaralı Tavsiye), 7/24 irtibat noktalarının adli yardımlaşma sürecindeki rolünün güçlendirilmesi, karşılıklı adli yardımlaşma prosedürlerinin aşamalarının azaltılması ve sürecin hızlandırılmasına katkı sağlayan uygulamaların T-CY ile paylaşılması (6 Numaralı Tavsiye), ölüm tehlikesi ve benzeri acil durumlarla ilgili talepler için acil durum prosedürlerinin oluşturulması (8 Numaralı Tavsiye), adli yardımlaşma taleplerin elektronik ortamda iletilmesine imkan sağlanması (11 Numaralı Tavsiye), adli yardımlaşma talebinde eksiklik olmaması adına yetkili makamların gerektiğinde talepte bulunulan tarafın yetkililerine danışmaya teşvik edilmesi (14 Numaralı Tavsiye), adli yardımlaşma taleplerinin ret nedenlerine ilişkin şeffaflığın sağlanması (15 Numaralı Tavsiye), Avrupa Konseyi'nin taraf devletlerin kendi iç hukuklarındaki uygulama ve yasal düzenlemelere ilişkin çevrimiçi bilgilendirme platformu oluşturulmasına yönelik çalışmalar yapması (18 Numaralı Tavsiye), adli yardımlaşma taleplerinde adli makamlar arasında doğrudan iş birliğinin geliştirilmesi (21 Numaralı Tavsiye) ve devletlerarası diyaloğun geliştirilmesi raporda yer alan diğer tavsiyelerdir.

4. Kullanıcı Adı ve Şifrenin Girilmesi Suretiyle

Buluttaki verilerin elde edilmesinin diğer yolu kullanıcı adı ve şifresinin girilmesi suretiyle bulutta depolanan verilere erişimdir. Bulut bilişim hizmetlerine ve bulutta depolanan verilere yasal olarak erişebilmek için kişiye tahsis edilen kullanıcı adı ve şifrenin bilinmesi gerekir. Sunucuya yasal olarak erişim ancak bu şekilde mümkündür. Ancak bu erişimin hukuka uygunluğundan söz edebilmek için kullanıcı hesap bilgilerinin meşru yollardan elde edilmesi gerekir. Hesap bilgilerinin şifre kırıcı çeşitli yazılım ve programlarla elde edilmiş olması şüphesiz ki bulut hesabına erişim hakkı vermez.[146] Herhangi bir hukuki prosedür izlenmeden elde edilen bu veriler hukuka aykırı delil

[146] Değirmenci, "Bulut Bilişim", s. 110; Dereboylular, s. 173.

statüsündedir.[147] Ancak hesap bilgilerinin CMK m. 134 kapsamında alınan arama kararına istinaden, yani hukuki bir prosedür izlenerek imajı alınan sabit bir bellek üzerinde çeşitli yazılım ve programların kullanılması suretiyle öğrenilmesi ve bulutta depolanan verilerin bu yöntemle elde edilmesi CMK m. 134/2 hükmü dikkate alındığında hukuka uygun olacaktır.[148] Bu yöntemin bulut veri depolama merkezlerine fiziken erişimin mümkün olduğu özel bulut veya veri depolama merkezleri yurt içinde bulunan ve kullanıcıya ait verinin bu merkezlerden hangisinde depolandığının bilindiği genel bulut dağıtım modellerinde kullanılabileceğine dikkat etmek gerekir. Çünkü aksi takdirde verinin depolandığı sabit belleğe fiziken erişilemeyeceğinden imaj alınması da mümkün olmayacaktır. Dolayısıyla ortada CMK m. 134/2 kapsamında elde edilen kullanıcı bilgilerinin girilmesi suretiyle erişim sağlanabilecek, kullanıcıya ait, imajı alınmış bir depolama alanı olmadığından herhangi bir sayısal delil elde edilmesi de imkansızdır.

Kullanıcı adı ve şifresi farklı şekillerde elde edilebilir. Günümüzde birçok hizmet online ortama taşındığından bu hizmetlerin her birine erişim için bir kullanıcı adı, e-posta adresi veya T.C. kimlik numarası gibi kişinin ayırt edilmesini sağlayacak bir kimlik bilgisi ve yetkisiz girişlerin önlenmesi için bir şifre gerekmektedir. Ancak bu hizmetlerin her biri farklı kombinasyonlarda kimlik bilgisi ve şifre belirlenmesini gerektirdiğinden bu bilgilerin tamamının akılda tutulması neredeyse imkânsız hale gelmiştir. Bu yüzden Internet Explorer, Google Chrome, Mozilla Firefox, Yandex gibi web tarayıcılarının hepsi kullanıcı adı ve şifresinin kaydedilmesine imkân vermekte, böylelikle kullanıcılar hesap bilgilerini her seferinde girmek zorunda kalmadan bu hizmetlere kolaylıkla erişebilmektedirler. Ayrıca bazı internet sitelerinde yer alan

147 Değirmenci, Sayısal Delil, s. 242; Bulutta bulunan verilere hukuka aykırı erişim neticesinde ortaya çıkabilecek suçlar hakkında yapılan değerlendirmeler için bkz. Değirmenci, "Bulut Bilişim", s. 108.

148 Alman hukukunda hukuka uygun bir arama kararına dayanarak bulut hesaplarına ait şifrenin kırılmasının orantılı bir zorlama olarak kabul edildiği ve bu yüzden hukuka aykırı sayılmadığına ilişkin bkz. Uğraş, s. 114; CMK m. 134/2 hükmü bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi halinde bilişim cihazlarına el konulmasına müsaade etmekte ve şifrenin çözülmesinden sonra bu cihazların gecikme olmaksızın iade edileceğini ifade etmektedir. Kanaatimizce bilişim cihazının şifresinin çözülmesiyle kullanıcı hesabına ilişkin şifrenin çözülmesi arasında bir fark yaratılmamalıdır.

"beni hatırla/kullanıcı adı ve şifremi hatırla" kutucuğunun işaretlenmesi halinde de hesap bilgilerinin girilmesine gerek kalmamaktadır. Bu hallerde kişinin bulut ve sosyal medya hesapları gibi hizmetlere erişmesini sağlayan hesap bilgileri kullanılan web tarayıcının sistemde kayıtlı olduğu klasöre, yani dahili hafızaya kaydedilmektedir.[149] Dolayısıyla bilgisayarda kayıtlı bir veri haline gelen bu bilgilerin CMK m. 134 kapsamında yapılan arama neticesinde elde edilmesi ve bu bilgiler vasıtasıyla bulutta veya sosyal medya hesaplarında arama yapılması gündeme gelebilir. Adli kolluk görevlilerinin arama yapılan cihaz açık olduğu takdirde cihazın dahili hafızasındaki verilerin yanı sıra şüpheliye ait e-posta veya bulut hesaplarındaki verilere de erişim sağlaması yaygın bir uygulamadır.[150] Öğretide bu bilgilere bilgisayarda yapılacak arama sonucunda ulaşılabileceği ve bulutta arama yapılabileceği ileri sürülmektedir.[151] Kanaatimizce bu görüşe şüpheyle yaklaşmak gerekir. Nasıl ki bir ev araması sırasında ele geçirilen anahtarın ait olduğu araç, işyeri veya başka bir konutta aynı arama kararına istinaden arama yapılamıyorsa, bilgisayarda arama neticesinde elde edilen şifre ve kullanıcı adıyla erişim sağlanabilen bulut veya sosyal medya hesapları üzerinde de arama yapılamaması gerekir. Çünkü artık aramanın konusu değişmiştir. Daha önce ifade ettiğimiz üzere bu şekilde elde edilen kullanıcı bilgileri aracılığıyla bulutta arama yapılması için bu hesaplar üzerinde arama yapılmasına ilişkin yeni bir kararın alınması gerekir.

Bulut veya sosyal medya hesaplarına ait kullanıcı adı ve şifre bilgileri, hakkında arama yapılacak şahsın rızasıyla da elde edilebilir. Bilindiği üzere CMK'da rızaya dayalı/muvafakatli aramaya yer verilmediğinden yetkili merciin kararı olmaksızın yapılan arama hukuka

---

149 "Chrome'un şifrelerinizi kaydetme şekli, bunları depolayarak cihazlarınızda kullanmak isteyip istememenize göre değişir. Chrome'da oturumunuz açıkken şifrelerinizi Google Hesabınıza kaydedebilirsiniz. Kaydettiğiniz şifrelere daha sonra tüm cihazlarınızda Chrome uygulamasında ve Android cihazlarınızdaki bazı uygulamalarda kullanılabilir. Aksi takdirde, şifrelerinizi yalnızca yerel olarak bilgisayarınızda saklayabilirsiniz". https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=tr#:~:text=%C5%9Eifreler%20senkronize%20edildiklerinde%2C%20t%C3%BCm%20cihazlar%C4%B1n%C4%B1zda,yaln%C4%B1zca%20bilgisayar%C4%B1n%C4%B1zdaki%20Chrome%20uygulamas%C4%B1na%20kaydedilir. (Erişim Tarihi: 18.07.2022).

150 T-CY, Final Report, para. 45, s. 16.

151 Göksoy, s. 132.

aykırılık teşkil eder. Nasıl ki arama kararı olmadan rızaya dayalı arama yapılması koruma tedbirlerinin kanunla düzenlenmesi gerekliliğine aykırıysa,[152] kullanıcı adı ve şifresinin rızayla verilmesi üzerine yapılan arama da hukuka aykırı olacaktır. Ancak ASSS m. 32/b'de[153] *"kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer Tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu Taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişilebilir veya bunları temin edebilir."* hükmü yer almaktadır. Bu hükme göre, bulut bilişim hizmetinin sağlandığı sunucu veya veri depolama merkezinin bulunduğu yer ASSS'ye taraf ülkelerden birinin topraklarında bulunuyorsa, bu veriyi açıklama yetkisine sahip kişi yani kullanıcının rızasıyla ASSS'ye taraf diğer ülkeler bulutta saklı bu verilere ulaşabilecektir. Söz konusu hüküm herkesin erişimine açık olmayan veriler için geçerlidir. Herkesin erişimine açık kaynaklarda depolanan veriler bulundukları konumdan bağımsız olarak ASSS m. 32/a hükmü kapsamında elde edilebilir.[154] Görüldüğü üzere ASSS m. 32/b hükmüne göre, kişinin hukuka uygun surette alınan rızasına dayalı olarak bulutta depolanan ve kamuya açık olmayan verilere erişilebilirken[155] mevzuatımızda böyle bir düzenlemeye yer verilmemiştir. Öğretide ASSS'deki

---

152 Aranan kişinin, arama koruma tedbirinin işlem tanıkları olmadan icrasına rıza göstermesine ilişkin benzer değerlendirme için bkz. Fahri Gökçen Taner/Yaprak Öntan, "CMK'nın 119/4 Maddesi Uyarınca Adli Aramada Bulundurulması Gereken Tanıklar Konusunda İçtihatta Dönüşüm", *AÜHFD*, C. 65, S. 4, Y. 2016, ss. 2465-2466.

153 ASSS'deki bu hüküm, oldukça istisnai haller bakımından geçerli olan bir çözüm yolu sunar. Örneğin, üzerinde taşıdığı bilgisayar, tablet ve akıllı telefonunda açık bulunan posta kutusunda uyuşturucu kaçakçılığı yaptığına ilişkin deliller bulunan bir şüpheli, yakalandığında kolluk kuvvetlerinin bu hesaba erişmesine izin verirse ve kolluk kuvvetleri de bu verilerin ASSS'ye taraf devletlerden birinin topraklarında depolandığından eminse ASSS m. 32/b kapsamında bulutta depolanan bu deliller elde edebilir. T-CY, Final Report, para. 44, s. 16.

154 Değirmenci, Sayısal Delil, s. 242. Örneğin, Türkiye'de yaşayan bulut kullanıcısının verileri Almanya'daki bir sunucuda saklanıyorsa, kullanıcının izniyle buradaki verilere erişilebilir. Değirmenci, "Bulut Bilişim", s. 110.

155 Öğretide veri sahibinin rızasıyla bir devletin başka bir devletin topraklarında yargı yetkisi kullanmasının devletlerin egemenliği ilkesine aykırı olduğu ileri sürülse de Önok'a göre, ASSS'ye taraf olmayı seçen bir devletin bu işlemin yapılmasına rıza gösterdiği söylenebilir. Önok, s. 1259; Geçerli bir rızanın varlığı halinde Amerikan Hukukunda da herhangi bir arama kararına gerek kalmaksızın bilgisayarlarda arama yapılabilmektedir. Bilişim sistemlerinde rızayla arama ve Amerikan Hukukunda arama kararı gerektirmeyen diğer haller hakkında ayrıntılı bilgi için bkz. Değirmenci, "Riley v. California Kararı", s. 63 vd.

bu düzenlemeye uygun olarak şüpheli veya sanığın rızasıyla kullanıcı hesap bilgilerinin temin edilebileceği ve bulutta arama yapılabileceği, bu durumun rızaya dayalı arama olarak değil, arama esnasında şüphelinin olumlu katkısı olarak değerlendirilmesi gerektiği ileri sürülmektedir.[156] İdeal hukuk dikkate alındığında usulüne göre yürürlüğe koyarak bağlayıcılığını[157] kabul ettiğimiz uluslararası bir sözleşme ile iç hukuktaki düzenlemelerin aynı doğrultuda olması gerekir. Ancak CMK m. 134 ve m. 135 hükümleri bilişim suçlarının karmaşık ve teknik yapısı dikkate alınarak hazırlanan ASSS'de öngörülen koruma tedbirlerine göre oldukça eksiktir.[158] Bu konuda Anayasa m. 90/5'te düzenlenen milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi halinde milletlerarası antlaşmalara üstünlük tanınmasına ilişkin kuralın uygulanması ve bulut veya sosyal medya hesaplarında rızaya dayalı arama yapılmasının mümkün olduğu ileri sürülebilir.[159] Ancak kanaatimizce Anayasa m. 90/5 hükmünün temel hak ve hürriyetler lehine yorumlanması ve şüpheli ve sanık bakımından iç hukuktaki düzenlemeler uluslararası sözleşmelere göre daha çok güvence sağlıyorsa iç hukuk hükümlerinin uygulanması gerekir. Mevzuatımız yetkili merciin kararı olmadan sadece şüpheli ve sanığın rızasına dayalı olarak arama[160] ve iletişimin denetlenmesi[161] koruma

156 Değirmenci, Sayısal Delil, s. 243, 244; Kullanıcı adı ve şifresinin şüpheli ve mağdur tarafından rızayla verilebileceğine ilişkin bir diğer görüş için bkz. Göksoy, s. 132.

157 Kaymaz, s. 45.

158 CMK'nın ASSS karşısındaki durumu için bkz. Cahit Aliusta/Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, C. 4, S. 35-42, No. 2, Y. 2018, s. 40.

159 ASSS'nin iç hukukun bir parçası olduğu için uygulanabilir nitelikte olduğuna ancak bunun için Anayasa m. 13 hükmü gereğince kanuni düzenleme yapılması gerektiğine dair görüş için bkz. Dereboylular, s. 195.

160 Özbek/Doğan/Bacaksız, ss. 309-310; "… sanığın iş yerinde bulunan bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılması, bilgisayar kayıtlarından kopya çıkarılması, bu kayıtların çözülerek metin hâline getirilmesi için sanık tarafından gösterilen rızanın yeterli olmayacağı ve mutlaka 'Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' başlıklı CMK'nın 134. maddesine göre hâkim kararı alınması gerektiği, hâkim kararı olmaksızın bilgisayar ve hard disklerde yapılan arama sonucunda elde edilen delillerin hukuka aykırı yöntemlerle elde edilen delil niteliğinde olduğunun…" Yargıtay CGK, E. 2017/7-961, K. 2019/622, T. 22.10.2019 (www.kazanci.com); Danıştay İdari Dava Daireleri Kurulu E. 2007/2257, K. 2012/1117, T. 14.09.2012 tarihli kararıyla, Danıştay 10. Dairesinin Adli ve Önleme Aramaları Yönetmeliğindeki ilgilinin rızasıyla arama yapılmasına izin veren ibarenin iptaline ilişkin kararını onamıştır.

161 Özbek/Doğan/Bacaksız, s. 377; Mağdurun rızası varsa iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi mümkündür. Ancak

tedbirlerine başvurulmasına imkân sağlamadığından kanaatimizce, ASSS doğrultusunda iç hukukta gerekli düzenleme ve değişiklikler yapılmadıkça şüpheli ve sanığa ait bulut veya sosyal medya hesaplarında rızaya dayalı arama yapılamaz.[162]

C. Bulutta Depolanan Verilere Erişim İçin Alternatif Bir Yöntem: Veri Yerelleştirme/İkameti

Bulutta depolanan sayısal delil niteliğindeki veriler, buraya kadar yapılan açıklamalardan anlaşılacağı üzere, bir bilişim cihazının dahili hafızasındaki verilere erişilmesinde olduğu gibi CMK m. 134 kapsamında alınacak arama kararına istinaden kolaylıkla elde edilememektedir. Özellikle şüphelinin/sanığın kullandığı bulut hizmet sağlayıcısına ait veri depolama merkezlerinin yurt dışında olduğu hallerde, adli yardımlaşma sürecinin işleyişindeki aksaklıklar nedeniyle elde edilmek istenen deliller ya elde edilememekte ya da geç elde edilmektedir. Verilerin bulut hizmet sağlayıcısına ait veri merkezleri arasında sürekli hareket halinde olduğu hallerde ise, verilerin nerede olduğu tam olarak tespit edilemediğinden adli makamlar bulutta depolanan verilerin elde edilmesi için hangi yönteme başvurması gerektiğini dahi tespit edememektedir. Bulutta depolanan verilerin elde edilmesi sürecinde yaşanan bu zorluklar, devletleri vatandaşlarına ait verilerin ülke topraklarındaki yerleşik sunucularda depolanması yoluna başvurmaya sevk etmiştir.[163] Veri yerelleştirme (data localization),[164] veri ikameti (data residency)[165] veya veri milliyetçiliği (data nationalism)[166]

CMK m. 135 şüpheli ve sanık hakkında başvurulabilen bir koruma tedbiri olduğundan, mağdurun rızasıyla iletişimin denetlenmesinde CMK m. 160 vd. hükümlerine başvurulur. Özbek, "Türk Hukukunda", s. 193.

162 Aynı yönde görüş için bkz. Hamza Aytaç Doğanay, Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri, Legem Yayıncılık, Ankara, 2020, ss. 18-19; Şüphelinin rızasına dayalı olarak arama yapılamayacağı ve bunun kendini suçlayıcı beyanda bulunmama hakkı bakımından değerlendirilmesi için bkz. Dereboylular, ss. 172-173.

163 Boncinelli, s. 28; Devletler iç hukukun uygulanmasını sağlamak, yabancı devletlerin gözetiminden kaçınmak, vatandaşlarının gizliliğini ve güvenliğini sağlamak, ekonomik kalkınmayı güvence altına almak gibi nedenlerle veri yerelleştirme yoluna başvurmaktadır. Veri yerelleştirme nedenleri hakkında detaylı bilgi için bkz. Anupam Chander/Uyên P. Lê, *Data Nationalism, Emory Law Journal*, Vol. 64, Issue 3, s. 713 vd.

164 Schwartz, s. 1694.

165 Boncinelli, s. 28.

166 Chander/Lê, s. 677 vd.

olarak adlandırılan bu alternatif yöntemde, veriler tek bir ülke veya belirli bir coğrafi bölge sınırları içerisindeki veri depolama merkezlerinde bulunmakta ve bu verilere dışarıdan erişim sağlanamamaktadır. Örneğin, Amazon Web Hizmetlerinin (AWS) dünya üzerinde 31 coğrafi bölgede 99 farklı erişilebilirlik alanı vardır.[167] Belirli bir coğrafi bölgeden sunulan bulut hizmetine aynı hizmet sağlayıcıya ait başka bir coğrafi bölgeden erişim sağlanamaz.[168] Mesela, AWS ve Microsoft'un Avrupa Birliği bölgesinden sunulan bulut hizmetlerine ABD'den erişilememektedir.[169]

Veri yerelleştirmenin yukarıda bahsettiğimiz şekli veri yerelleştirmenin teknik boyutudur.[170] Teknik yerelleştirmede kullanıcıya ait veriler hizmet sağlayıcı tarafından belirli bir coğrafi bölgede tutularak kullanıcıya ait verilerin farklı coğrafi bölgelerdeki veri depolama merkezleri arasında hareket halinde olmasının ve verilerin farklı sunucularda parça parça depolanmasının[171] önüne geçilir. Verilerin hizmet sağlayıcılar tarafından teknik imkanlarla yerelleştirilmesi, verilerin depolandığı yerin bilinmemesi (loss of location)[172] sorununu ortadan kaldıracağından bulutta depolanan veriyi elde etmek isteyen adli makamlar, verinin yurt içinde veya yurt dışında bulunmasına göre başvurması gereken yöntemi kolaylıkla tayin edebilecektir. Ancak teknik yerelleştirme bulutta depolanan sayısal delillerin elde edilmesini belirli bir ölçüde kolaylaştırır. Çünkü bu yöntem verilerin kullanıcının bulunduğu ülkede depolanmasını sağlamaz. Bulut hizmet sağlayıcılar, verilerin kullanıcıların kendi seçeceği coğrafi bölgelerde depolan-

---

167 https://aws.amazon.com/tr/about-aws/global-infrastructure/?nc2=h_ql_le_int_gi (Erişim Tarihi: 28.02.2023).

168 ABD yetkili makamlarının yurt dışında bulunan veri merkezlerinde arama yapıp yapamayacağına ilişkin Microsoft İrlanda davasının arkasında yatan asıl neden, yukarıda izah ettiğimiz veri yerelleştirme modelinin tam olarak kurulamaması, Microsoft'un Dublin'deki veri merkezinde bulunan verilere Microsoft'un Redmond Washington'daki merkezinden teknik olarak erişim sağlanabilmesidir. Schwartz, ss. 1696-1697; Amerikan Anayasa Mahkemesi Microsoft İrlanda davasında ABD'de çıkarılan arama kararına istinaden yurt dışında arama yapılamayacağı ve iç hukukta arama yapma yetkisi veren yasayla yurt dışında soruşturma yürütmek gibi bir amacın güdülmediği sonuçlarına ulaşmıştır. Microsoft İrlanda davası hakkında bkz. Dereboylular, ss. 188-190.

169 Schwartz, s. 1697.

170 Schwartz, s. 1696.

171 Dereboylular, s. 173.

172 Dereboylular, s. 173.

masına imkân sağlamaktadır.[173] Dolayısıyla kullanıcı özellikle yurt dışındaki bir coğrafi bölgeyi tercih ederek sayısal delil niteliğindeki verilerinin ele geçirilmesini güçleştirebilir. Kaldı ki bulut hizmet sağlayıcılarının sunmuş olduğu erişilebilirlik alanları belirli coğrafi bölgelerle sınır olduğundan kullanıcı istese de verilerini kendi ülkesinde depolayamayabilir. Örneğin, AWS'nin hizmet sunduğu 26 coğrafi bölge içerisinde Türkiye bulunmadığından verilerin teknik olarak yerelleştirilmesi bulutta depolanan sayısal delillerin elde edilmesi bakımından bir kolaylık sağlamayacaktır.

Verileri yerelleştirmenin bir diğer yolu olan verilerin yasal olarak yerelleştirilmesi, bir başka ifadeyle yasal yerelleştirme ise kullanıcılara ait verilerin ülke sınırları içerisinde depolanmasını sağlayan[174] veya verilerin yurt dışına çıkarılmasını özel olarak engelleyen yasal düzenlemelere başvurmak suretiyle veri ikametinin sağlanmasıdır. Yasal yerelleştirmenin sağlanması için devletler verilerin yurt dışına çıkarılmasını engelleyen, verilerin yurt dışına çıkarılması için sahibinin rızasını arayan, verilerin yurt içinde depolanmasını veya verilerin kopyalarının yurt içinde saklanmasını zorunlu kılan ya da veri ihracatı için vergi uygulanması gibi çok farklı yasal düzenlemelere başvurmaktadırlar.[175]

Yasal yerelleştirmede yapılan yasal düzenlemelerle bulut hizmet sağlayıcılara, kullanıcılara ait verileri ülke içerisinde tutma yükümlülüğü getirilmektedir. Ülke içerisindeki faaliyetlerine devam etmek isteyen bulut hizmet sağlayıcılar faaliyet gösterdikleri ülkenin kanunlarına uymak zorunda kalmaktadır. Kamuoyunda *"Sosyal Medya Yasası"* olarak bilinen 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un 6. maddesiyle, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna eklenen ek m. 4'ün 5. fıkrası Türkiye'den günlük erişimi bir

173 "Amazon S3 klasörünüzü oluştururken bir AWS Bölgesi belirtirsiniz.", "Verilerinizi, coğrafi yedeklilik ve olağanüstü durum kurtarma amacıyla diğer operasyonlarınızdan uzak bir Bölgede depolamayı da seçebilirsiniz". https://aws.amazon.com/tr/s3/faqs/ (Erişim Tarihi: 28.02.2023).

174 Schwartz, s. 1696.

175 Chander/Lê, s. 680.

milyondan fazla olan yurt içi ve yurt dışı kaynaklı sosyal ağ sağlayıcılara, Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alma mükellefiyeti getirmektedir. Söz konusu düzenlemeyle atılan bu adım verilerin yasal olarak yerelleştirmesini sağlamaya yöneliktir.

Yine ek m. 4/1 ile günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcılara Türkiye'de temsilci bulundurma yükümlülüğü getirilme nedenlerinden biri de adli makamlarca gönderilen tebligat, bildirim veya taleplerin gereğinin yerine getirilmesini sağlamaktır. Daha önce ifade ettiğimiz üzere, bulut bilişim hizmet modellerinden biri olan SaaS aracılığıyla sunulan sosyal ağ hizmetlerine ilişkin bu düzenleme de bulutta depolanan sayısal delil niteliğindeki verilerin elde edilmesine yöneliktir. Bu hüküm adli makamların bulut formundaki sosyal medya hesaplarında depolanan verilerin elde edilmesine ilişkin taleplerini, sosyal ağ sağlayıcının Türkiye temsilcisine iletmesine ve bulut hizmet sağlayıcıyla yapılacak iş birliğiyle bu delillerin elde edilebilmesine imkân sağlamaktadır. Söz konusu düzenleme göstermektedir ki, Türkiye de pek çok ülke gibi vatandaşlarına ait verilerin yurt içinde depolanmasını sağlamak için yasal yerelleştirme yolunda ilk adımları atmıştır. Bulutta depolanan verilerin elde edilmesindeki güçlükler ve devletlerin toplum ve bireyleri suça karşı koruma yükümlülükleri dikkate alındığında, en azından karşılıklı adli yardımlaşma sürecinin etkinliği ve ivediliği ile uluslararası iş birliğinin işlevselliği sağlanana kadar devletlerin bu alternatif yönteme başvurması kanaatimizce kabul edilebilir.[176]

SONUÇ

Başta akıllı telefonlar olmak üzere günümüzde kullanılan bilişim cihazlarının çoğu veri depolama, işleme gibi özelliklerin yanı sıra internet erişimi ve iletişim gibi farklı fonksiyonları da yerine getirmektedir. Bilişim cihazlarından delil elde etmenin teknik boyutu (adli bilişim) kadar hukuki boyutu da önemlidir. Adli bilişim yöntemleri ne kadar ilerlemiş olursa olsun, usulüne göre bir karar alınmadığı ve bu karar hukuka uygun olarak icra edilmediği takdirde elde edilen delil

176 Veri yerelleştirmenin yaratacağı olası sorunlar için bkz. Chander, ss. 680-681; Dereboylular, s. 174.

bir anlam ifade etmeyecektir. Dolayısıyla bu delillerin kanuna aykırılığını önlemek için CMK m. 134 veya m. 135'te düzenlenen koruma tedbirlerinden hangisine başvurulması gerektiği sorununun açıklığa kavuşturulması gerekir.

CMK m. 134'te düzenlenen koruma tedbiri sadece bilgisayar, bilgisayar kütükleri ve programlarında arama, kopyalama ve elkoymaya müsaade etmektedir. Akıllı telefon, tablet, akıllı saat gibi bilişim cihazları da birer bilgisayardır. Veri işleme, saklama ve iletme özelliğine sahip tüm cihazların bu kapsamda değerlendirilmesi gerekir. Bilgisayarın fiziki varlığına yönelik bu koruma tedbiriyle arama yapılan bilgisayarın hafızasında kayıtlı olan durağan veriler elde edilir. CMK m. 135'te düzenlen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi koruma tedbirine ise akış halindeki verilerin elde edilmesi için başvurulabilir. CMK m. 135 ile kişiler arasındaki canlı iletişim dinlenerek kayda alınmakta, yani akış halindeki veriler elde edilebilmektedir. Bu tedbirin CMK m. 134'ten en önemli farklı gizlilik ihtiva etmesi, yani kullanıcının dinlendiğinden haberinin olmamasıdır.

Elektronik posta ve anlık mesajlaşma uygulamalarıyla internet üzerinden gerçekleştirilen iletişimin tespiti de CMK m. 135 kapsamına girmektedir. Kanaatimizce anlık mesajlaşma uygulamalarıyla gerçekleştirilen iletişimin de elektronik posta üzerinden gerçekleştirilen iletişim gibi düşünülmesi gerekir. Bu bağlamda veri, e-posta veya anlık mesajlaşma uygulamalarına erişimin sağlandığı bilişim cihazlarına kaydedilmediği sürece CMK m. 135 kapsamında elde edilebilir. E-postalarda olduğu gibi veri ara sunucudan çağrılarak bilgisayara kaydedilmişse artık durağan bir veri haline dönüştüğünden bu delilin CMK m. 134'te düzenlenen koruma tedbirine başvurularak elde edilmesi gerekir. Verinin akış halinde mi, durağan mı olduğunun tespitinde bu uygulamaların sahip olduğu özellikler ve uygulamaya erişim sağlanan ortam (web tarayıcı veya program üzerinden) dikkate alınarak bir sonuca ulaşılmalı ve bu bağlamda ilgili koruma tedbirine başvurulmalıdır. Geçmişte yapılan haberleşme içerikleri, yani depolanmış iletişim canlı ve eşzamanlı iletişimin tespitine ilişkin olmadığından CMK m. 135 kapsamında denetlenemez. Ayrıca bu gönderiler mektup gibi fiziği varlığa sahip olmadıklarından CMK m. 129 kapsamında da elde edilemeyecektir. Geçmişte yapılan depolanmış iletişimin içeriğine, bu gönderi ancak bir veri olarak ilgili bilişim cihazına

kaydedilerek durağan veri haline gelmişse CMK m. 134 kapsamında erişilebilir.

Dünyanın herhangi bir yerinde bulunan bilişim cihazlarında veri depolamaya veya bu cihazlara uzaktan erişilerek kullanılmasına imkân veren bulut bilişim hizmetlerinde kayıtlı verilerin, hukuka uygun olarak nasıl elde edilebileceği sayısal delillerin elde edilmesinde karşılaşılan bir diğer önemli bir sorundur. Buluttaki veriler, bulut hizmet sağlayıcılara ait veri depolama merkezlerinin yurt içinde veya yurt dışında bulunmasına göre farklı yöntemlerle elde edilebilir. CMK m. 134'te öngörülen koruma tedbirine başvurularak bulutta arama yapılabilmesi için bulut hizmet sağlayıcısına ait veri depolama merkezlerine fiziken erişilebilmesi gerekir. Çünkü CMK m. 134 hükmü bilgisayar kütüklerine fiziken erişimin mümkün olduğu hallerde arama yapılmasına müsaade etmektedir. Bu nedenle bulut hizmet sağlayıcıya ait veri depolama merkezlerinin yurt içinde bulunduğu hallerde CMK m. 134 kapsamında bulutta arama yapılabilir. Bulut hizmet sağlayıcılara ait veri depolama merkezlerinin yurt dışında bulunduğu durumlarda ise CMK m. 134 kapsamında arama yapılması başka bir ülkenin yargı yetkisine tecavüz teşkil edeceğinden yurt dışında bulunan verilerin elde edilebilmesi için adli yardımlaşmaya başvurulması gerekir. Ancak adli yardımlaşma sürecinin işleyişindeki aksaklıklar sebebiyle bu yöntemin bulutta depolanan verilerin elde edilmesi bakımından hızlı ve etkin bir çözüm yolu olduğu söylenemez. Adli yardımlaşma sürecinin hızlandırılması için devletlerin karşılıklı iş birliğini artırması, ASSS'nin sunduğu imkanlardan yararlanması, yardım talebinde bulunulacak ülkenin iç hukukunu daha iyi öğrenmesi ve müşterek soruşturma ekiplerinin kurulması gibi klasik karşılıklı adli yardımlaşma sürecini daha işlevsel hale getirecek bazı yenilikçi adımlar atması gerekir.

ASSS m. 19/2 hükmü taraf devletlere kendi sınırları içerisinde bulunan bilgisayar sistemleri üzerinde uzaktan arama yapılmasına ilişkin gerekli yasal düzenlemeleri yapma yetkisi tanısa da bu konuda mevzuatımızda herhangi bir düzenlemeye gidilmemiştir. Adli ve Önleme Aramaları Yönetmeliği m. 17/3'te yer alan *"bilgisayar ağları ve diğer uzak bilgisayar kütükleri"*nde CMK m. 134 kapsamında arama yapılabileceğine ilişkin hüküm ise temel hak ve hürriyetlerin kanunla kısıtlanması gerekliliği karşısında bir anlam ifade etmemektedir. Do-

layısıyla ASSS m. 19/2 hükmünce tanınan yetki kullanılarak gerekli yasal düzenlemeler yapılmadıkça yurt içinde bulunsa bile herhangi bir bilişim sistemi üzerinde uzaktan veya online arama yapılması mümkün değildir.

Bulutta ve sosyal medyada bulunan delillerin elde edilmesi bakımından başvurulabilecek bir diğer yöntem, bu hesaplara ait kullanıcı adı ve şifrenin girilmesi suretiyle ilgili hesaba erişimdir. Kullanıcıya ait hesap bilgileri CMK m. 134 kapsamında alınan arama kararına istinaden imajı alınan bir depolama birimi üzerinde yapılan inceleme sonucunda doğrudan elde edilebileceği gibi çeşitli yazılım ve programların kullanılması suretiyle de elde edilebilir. Ancak elde edilen bu bilgilere dayanarak yeni bir arama kararı alınmadan söz konusu hesaplar üzerinde arama yapılamaz. Söz konusu bilgilerin herhangi bir hukuki prosedür izlenmeden şifre kırıcı programlarla elde edilerek ilgili hesaplara erişim ise şüphesiz ki hukuka aykırı bir yöntem olacaktır.

ASSS m. 32/b'de ASSS'ye taraf devletlerin herhangi birinin ülkesinde depolanan verilerin bu bilgileri ifşa etme yetkisine sahip kişilerin rızasıyla temin edilebileceği düzenlenmiştir. Bu hükme göre, bulut bilişim hizmetinin sağlandığı sunucu eğer ASSS'ye taraf ülkelerden birinin topraklarında bulunuyorsa, bu veriyi açıklama yetkisine sahip kişi yani kullanıcının rızasıyla ASSS'ye taraf diğer ülkeler bulutta depolanan bu verilere ulaşabilecektir. ASSS'deki durum bu olmakla birlikte, iç hukukumuzda rızaya dayalı arama müessesi düzenlenmediğinden kanaatimizce bu yolla delil elde edilebilmesi mümkün değildir. Şüpheli ve sanık bakımından mevzuatımızdaki düzenlemeler ASSS'ye göre daha güvenceli olduğundan bu konuda AY m. 90/5 hükmüne başvurulamaz.

Bulutta depolanan verilerin elde edilmesinde yaşanan güçlükler devletleri, vatandaşlarına ait verilerin ülke topraklarında depolanması yoluna başvurmaya sevk etmiştir. Veri yerelleştirme, veri ikameti veya veri milliyetçiliği olarak adlandırılan bu alternatif yöntemde veriler, devletlerin yaptığı hukuki düzenlemelerle yasal olarak yerelleştirilebileceği gibi bulut hizmet sağlayıcıları da verileri belirli bir ülke veya coğrafi bölge sınırları içerisindeki veri depolama merkezlerinde tutarak teknik olarak veri ikametini sağlayabilmektedir. Mevzuatımızda

bu doğrultuda yapılan bazı değişikliklerle verilerin yurt içindeki sunucularda tutulması ve hizmet sağlayıcıların Türkiye'de temsilci bulundurması gibi bazı yükümlülükler getirilerek verilerin yasal olarak yerelleştirilmesi sağlanmaya çalışılmaktadır.

Kaynakça

Kitaplar

Aslan Ahmet, Cumhuriyet Savcısı ve Soruşturma, Adalet Yayınevi, Ankara, 2018.

BTK, Bulut Bilişim, Ankara, 2013, https://www.btk.gov.tr/uploads/pages/slug/bulut-bilisim.pdf (Erişim Tarihi: 28.02.2023).

Centel Nur/Zafer Hamide, Ceza Muhakemesi Hukuku, Beta Basım Yayım, İstanbul, 2020.

Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: challenges (Discussion paper prepared by the T-CY Cloud Evidence Group), 26 Mayıs 2015. (Discussion Paper)

Cybercrime Convention Committee (T-CY), Criminal justice Access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (Final report of the T-CY Cloud Evidence Group), 26 Eylül 2016. (Final Report)

Cybercrime Convention Committee (T-CY), T-CY asssesment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime (Adopted by the T-CY at its 12th Plenary), 3 Aralık 2014. (Assessment Report)

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

Doğanay Hamza Aytaç, Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri, Legem Yayıncılık, Ankara, 2020.

Dülger Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2020.

Göksoy Resul, Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması, Seçkin Yayıncılık, Ankara, 2019.

Henkoğlu Türkay, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, İstanbul, 2014.

Kaymaz Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Seçkin Yayıncılık, Ankara, 2015.

Mell Peter/Grance Timothy, The NIST Definition of Cloud Computing, NIST Special Publication, 2011.

NIST, Cloud Computing Standards Roadmap, NIST Special Publication, Temmuz 2013.

Orta Mesut, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), Yetkin Yayınları, Ankara, 2015.

Özbek Veli Özer/Doğan Koray/Bacaksız Pınar, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2021.

Özen Muharrem/Baştürk İhsan, Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara, 2011.

Öztürk Bahri /Eker Kazancı Behiye/ Soyer Güleç Sesim, Ceza Muhakemesi Hukukunda Koruma Tedbirleri, Seçkin Yayıncılık, Ankara, 2022.

Parlar Ali/Çetin Ahmet, Ceza Muhakemesinde Soruşturma Evresi ve Uygulaması, Aristo Yayınları, İstanbul, 2017.

Saydam Mehmet, Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Oniki Levha Yayınları, İstanbul, 2011.

Siber Suç Uzmanları Komitesi, Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı (Çev. İnternet ve Hukuku Platformu), Ankara 2008.

Şahin Cumhur, Ceza Muhakemesi Kanunu Gazi Şerhi, Seçkin Yayıncılık, Ankara, 2005.

Şahin Cumhur/Göktürk Neslihan, Ceza Muhakemesi Hukuku- I, Seçkin Yayıncılık, Ankara, 2021.

Şen Ersan, Türk Hukuku'nda Telefon Dinleme Gizli Soruşturmacı X Muhbir, Seçkin Yayıncılık, Ankara, 2013. (X Muhbir)

Şentürk Akaner Candide, Bir Koruma Tedbiri Olarak Online Arama ve Türk Hukukunda Uygulanabilirliği, Seçkin Yayıncılık, Ankara, 2022.

TBMM, Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu, Haziran 2012, https://acikerisim.tbmm.gov.tr/xmlui/handle/11543/2781 (Erişim Tarihi: 28.02.2023).

Tezcan Durmuş vd., Dijital Ceza Muhakemesi Hukuku (Editörler: Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem), Seçkin Yayıncılık, Ankara, 2022.

Tonini Paolo, Manuale di procedura penale, Giuffrè, Milano, 2010.

Topaloğlu Murat/Özkişi Harun/Tekkanat Egemen, Bulut Bilişim, Seçkin Yayıncılık, Ankara, 2017.

Turan Metin, Bulut Bilişim, Seçkin Yayıncılık, Ankara 2019.

U.S. Department of Justice (DOJ), Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, April 2019.

Ünver Yener/Hakeri Hakan, Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara, 2020.

Yaşar Osman, Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu, Cilt I, Seçkin Yayıncılık, Ankara, 2018.

Yenidünya A. Caner/Değirmenci Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, 2003.

Yenisey Feridun/Nuhoğlu Ayşe, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2022.

Makaleler ve Kitap Bölümleri

Aliusta Cahit/Benzer Recep, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* C. 4, S. 35-42, No. 2, Y. 2018, ss. 35-42.

Aytekin İnceoğlu Asuman, "Türk Hukukunda Adli Amaçlı İletişimin Denetlenmesi", *Uğur Alacakaptan'a Armağan Cilt-1,* İstanbul 2008, ss. 103-126.

Boncinelli Vanni, "Modelli tecnici e discipline giuridica del c.d. cloud computing", Rivista italiana di informatica e diritto, 3, 1 (lug. 2021), ss. 27-45.

Chander Anupam/Lê Uyên P., "Data Nationalism", *Emory Law Journal,* Vol. 64, Issue 3, ss. 677-739.

Değirmenci Olgun, "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi", *Bilişim Hukuku Dergisi*, C. 2, S. 1, ss. 47-79.

Değirmenci Olgun, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği", *Terazi Hukuk Dergisi*, C. 9, S. 97, Eylül 2014, ss. 14-28.

Değirmenci Olgun, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m. 134), 7145 sayılı Kanun'la Yapılan Değişikliklerin Değerlendirilmesi", *Terazi Hukuk Dergisi*, C. 13, S. 13, Kasım 2018, ss. 146-155.

Değirmenci Olgun, "Bulut Bilişim ve Beraberinde Getireceği Hukuksal Sorunlar Üzerine Görüşler", *Terazi Hukuk Dergisi,* C. 12, S. 136, Y. Aralık 2017, ss. 106-110.

Değirmenci Olgun, "Sayısal (Dijital) Verilerde Yakalama Sonrası Arama: Amerikan Yüksek Mahkemesinin Riley v. California Kararı Sonrası Amerikan Hukukunun Değerlendirilmesi", *TAAD*, Y. 7, S. 24, Ocak 2016, ss. 59-88.

Dereboylular Özge, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği", *CHD*, S. 39, Y. 14, ss. 161-202.

Kerr Johndavid/Teng Kwok, "Cloud Computing: legal and privacy issues", *Journal of Legal Issues and Cases in Business*, Vol. 1, 2012, ss. 1-11.

Önok Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş Birliği", *MÜHF-HAD Prof. Dr. Nur CENTEL'e Armağan*, C. 19, S. 2, Y. 2013, ss. 1229-1269.

Özbek Veli Özer, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", *DEÜHFD,* C. 4, S. 1, Y. 2002, ss. 101-158.

Özbek Veli Özer, "Türk Hukukunda İletişimin Adli/İdari Amaçla Denetlenmesi ve Uygulamadaki Sorunlar", Ceza Muhakemesi Hukukunda Güncel Konular, İstanbul 2015, ss. 147-225. (Türk Hukukunda)

Özen Muharrem/Özocak Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi (CMK m. 134)", *Ankara Barosu Dergisi,* Y. 73, S. 2015/1, ss. 43-77.

Saliger Frank, "Alman Ceza Muhakemesi Hukuku'na göre Telekomünikasyonun Denetlenmesi" (Çev. Murat Ceyhan), *Ceza Muhakemesi Hukukunda Güncel Konular*, İstanbul 2015, ss. 131-145.

Schwartz Paul M., "Legal Access To The Global Cloud", *Columbia Law Review*, Vol. 118, No. 6, ss. 1681-1762.

Şahbaz İbrahim, "Koruma Tedbiri Olarak İletişim Denetlenmesi", Ceza Yargılaması Hukukunda Son Gelişmeler Sempozyumu, Ankara 2016, ss. 27-74.

Şahin Cumhur, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi – Yargıtay Kararları Çerçevesinde Bir Değerlendirme", *GÜHFD*, C. 11, S. 1-2, Y. 2007, ss. 1095-1112.

Şen Ersan, "Bilgisayar Aramasında ve İletişimin Denetlenmesinde Hukuka Aykırılık Soruları", https://www.hukukihaber.net/bilgisayar-aramasinda-ve-iletisimin-denetlenmesinde-hukuka-aykirilik-sorulari-makale,7344.html (Erişim Tarihi: 28.02.2023).

Taner Fahri Gökçen/ Öntan Yaprak, "CMK'nın 119/4 Maddesi Uyarınca Adli Aramada Bulundurulması Gereken Tanıklar Konusunda İçtihatta Dönüşüm", *AÜHFD*, C. 65, S. 4, Y. 2016, ss. 245-2469.

Uğraş Dilek Özge, "Bilgisayarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", *TBBD*, S. 154, Y. 2021, ss. 97-134.

Yang Bo-Wen vd.: "Cloud Computing Architecture for Social Computing – A Comparison Study of Facebook and Google", *2011* International Conference on Advances Social Networks Analysis and Mining, 2011, ss. 741-745.

Yaşar Yusuf/Dursun İsmail, "Bilgisayarlar, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", *MÜHF-HAD*, C. 19, S. 3, ss. 3-34.

Mahkeme Kararları

Danıştay İdari Dava Daireleri Kurulu E. 2007/2257, K. 2012/1117, T. 14.09.2012 (www.kazanci.com).

De Tommaso/İtalya, Başvuru Nu. 43395/09, 23.02.2017.

Yargıtay 16. C.D. E. 2015/3, K. 2017/3, T. 24.04.2017 (www.kazanci.com).

Yargıtay CGK, E. 2017/7-961, K. 2019/622, T. 22.10.2019 (www.kazanci.com).

İnternet Kaynakları

https://acikerisim.tbmm.gov.tr/xmlui/handle/11543/2781

https://aws.amazon.com/tr/about-aws/global-infrastructure/?nc2=h_ql_le_int_gi

https://aws.amazon.com/tr/s3/faqs/

https://faq.whatsapp.com/791574747982248/?helpref=uf_share

https://faq.whatsapp.com/800085810452992/?helpref=uf_share

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf

https://one.google.com/about

https://turkcellbulut.com/homepage

https://wearesocial.com/us/blog/2022/01/digital-2022-another-year-of-bumper-growth-2

https://www.btk.gov.tr/uploads/pages/slug/bulut-bilisim.pdf

https://www.hukukihaber.net/bilgisayar-aramasinda-ve-iletisimin-denetlenmesinde-hukuka-aykirilik-sorulari-makale,7344.html

https://www.kazanci.com

https://www.resmigazete.gov.tr/