BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE BİLGİSAYAR KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA

SEARCH, DUPLICATION AND SEIZURE OF COMPUTERS, COMPUTER PROGRAMS AND LOGS ACCORDING TO TURKISH CRIMINAL PROCEDURE CODE ART. 134 (tCPC Art. 134)

Dilek Özge UĞRAŞ*

Özet: Günümüzde teknolojik araçlarda yaşanan hızlı değişim ve gelişim etkisini tartışmasız hukuk alanında da göstermekte, kanun koyucuları kanunların teknolojinin beraberinde getirdiği gelişmeler ve farklı uyuşmazlık konuları hakkında mevcut düzenlemelerin yeterli olmadığı noktada bu gelişmelerle uyumlu yeni normlar düzenlemeye ya da mevcut normlarda değişiklikler yapmaya sevk etmektedir.

Bu hukuki düzenlemelerden birini de Ceza Muhakemesi Kanunu'nun m. 134 hükmünde yer alan norm oluşturmaktadır. Bu hükümle, geleneksel suçlarda söz konusu olan delillerin yanı sıra özellikle bilişim sistemleri aracılığıyla veya bu sistemlere karşı işlenen suçlarda söz konusu olabilecek delillerin elde edilmesine ilişkin olarak arama ve istisnai olarak elkoyma koruma tedbiri düzenlenmiştir.

Bu çalışmada anılan koruma tedbirinin şartları ve uygulanma usulü yakından incelenecek, bu kapsamda sorunlu olan hususlara değinilmeye gayret edilecektir.

Anahtar Kelimeler: Bilgisayar, Bilgisayar Programları, Bilgisayar Kütükleri, Arama, Elkoyma

Abstract: The rapid change and development in technological tools today shows its influence undisputedly also on the field of law, and encourages legislators to organize new norms or make amendments, which are compatible with these developments, when existing regulations are not sufficient regarding to developments brought by technology and different dispute issues.

One of the most significant regulations constitutes Art. 134 of Turkish Criminal Procedure Code, which regulates the conditions of any search in computers, computer programs and logs and as an

* Arş. Gör., Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku, ozge.erdem@asbu.edu.tr., ORCID: 0000-0002-2226-7369, Makalenin Gönderim Tarihi: 16.07.2020, Kabul Tarihi: 16.07.2020

extraordinary measure, seizure of these mediums in scope of a criminal investigation.

Hereby, in this article, the legal conditions of above-mentioned procedural measures and their practical application will be closely examined and efforts will be made to address the problematic issues in this context.

Keywords: Computer, Computer Programs, Computer Logs, Search, Seizure

I. GİRİŞ

Teknolojik imkânların klasik suçların işlenmesinde yeni yöntemler geliştirilmesine olanak tanımasının yanı sıra teknolojik araçların, yeni suçların doğrudan ve bunlara özgü araçları olarak kullanılması da söz konusu olabilmektedir. Nitekim Türk Ceza Kanunu'nda düzenlenen bilişim suçları, teknolojik vasıtaların suçun doğrudan aracı olduğu ve yalnız bu araçlar kullanılarak gerçekleştirilebilen özel suç tipleri ihtiva etmektedir. Bu özgün suçlarda olduğu gibi, klasik suçların da bilişim sistemleri kullanılarak işlenmesi halinde, suçtan geriye kalan delillerinin bizatihi bu sistemler dahilinde bulunması, ulusal ve uluslararası kanun koyucuları bu delillerin elde edilmesinde özel yollar izlenmesine yönelik düzenlemeler yapmaya sevk etmektedir. Nitekim tarafı olduğumuz Sanal Ortamda İşlenen Suçlar Sözleşmesi[1] bilişim sistemleri aracılığıyla işlenen suçların uluslararası ölçüde olması, taraf devletler arasında bu tür suçlara karşı ortak mücadele ihtiyacından ve hatta zorunluluğundan doğmuştur. Türk Hukukunda da bilişim sistemleri kullanılarak işlenen suçların delillerinin elde edilmesine yönelik özel düzenleme, 5271 sayılı Ceza Muhakemesi Kanunu m. 134 hükmüyle bilgisayarlarda, bilgisayar programları ve bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri olarak uygulanmaya başlamıştır.

İşte bu çalışmada anılan koruma tedbirinin şartları ve uygulanma usulü doktrin ve yargı kararları doğrultusunda, karşılaştırmalı hukuktaki uygulama ve doktrin de göz önünde bulundurularak, yakından incelenecek; hükme ilişkin olarak doktrinde ifade edilen ve uygulamada karşılaşılan sorunlara değinilmeye çalışılacaktır.

---

[1] Budapeşte 2001, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (Erişim Tarihi: 25.05.2020); sözleşme 02.05.2014 tarihli 29966 sayılı Resmî Gazete'de yayınlanan 22.04.2014 tarihli 6533 sayılı Kanun ile onaylanmıştır.

II. GENEL OLARAK

A. Delillerin Sınıflandırılması ve Dijital Deliller

Ceza muhakemesi hukukunda deliller, yargıcın muhakeme sonucunda maddi olayı çözmesine ve bunu sabit görmesine ya da görmemesine hizmet eden araçlardır.[2] Medeni muhakemenin aksine ceza muhakemesinde delil serbestisi sistemi benimsenmiş olup, kural olarak her şeyin delil olabilmesi mümkündür; belirli olaylar belirli delillerle ispat edilmek zorunda değildir.[3] Ceza hukukunu ilgilendiren olaylarda medeni muhakemeden farklı olarak bireylerin muhtemel uyuşmazlıklar hakkında önceden ispat vasıtalarını, işlenecek suçun delillerini hazırlanması söz konusu değildir.[4]

Doktrinde maddi olayın ispatına yarayan vasıtalar olarak deliller farklı sınıflandırmalara tâbi tutulmuştur.[5] Delilleri maddi olayı temsil kabiliyetine göre doğrudan ve dolaylı deliller[6]; kaynaklarına göre kişilerden (beyan delilleri) veya şeylerden kaynaklanan deliller (belgeler, keşfe konu olan ve beş duyu organıyla algılanabilen belirtiler)[7] olarak ayırmak mümkündür. Genel olarak kanunun sistematiği içerisinde delilleri beyan, belge ve belirti delilleri olarak sınıflandırmak mümkündür. Beyan delilleri, şüpheli, sanık ve tanık beyanları olarak üçe ayrılmaktadır.[8] Belge delilleri; somut olayı tespit eden, insan yapısı araçlardır.[9] Doktrinde bir görüşe göre belge delilleri yazılı, şekil tespit eden ve ses tespit eden belge delilleri olarak üçe ayrılmaktadır.[10] Daha isabetli görünen diğer bir görüşe göre ses ve görüntü tespit eden nes-

---

2 Nevzat Toroslu/Metin Feyzioğlu, Ceza Muhakemesi Hukuku, Ankara 2015, s. 171.

3 Nur Centel/Hamide Zafer, Ceza Muhakemesi Hukuku, İstanbul 2015, s. 219; ceza muhakemesinde yalnızca duruşmanın akışının ispatıyla ilgili olarak kanuni delil sistemi benimsenmiştir (CMK m. 222); buna göre duruşmanın kanunda öngörülen usul ve esaslara uygun olarak yapıldığının ispatı ancak duruşma tutanağıyla mümkündür ve bu tutanağa karşı yalnızca sahtecilik iddiası yöneltilebilir (Centel/Zafer, s. 219).

4 Centel/Zafer, s. 219.

5 Bu ayrımlar hakkında detaylı bilgi için bkz. Toroslu/Feyzioğlu, s. 177, 178.

6 Yener Ünver/Hakan Hakeri, Ceza Muhakemesi Hukuku, Ankara 2014, s. 601.

7 Urs Kindhäuser, Strafprozessrecht, Baden-Baden 2016, § 21 Rn.1.

8 Ünver/Hakeri, s. 602 vd.

9 Ünver/Hakeri, s. 616.

10 Ünver/Hakeri, s. 616; Toroslu/Feyzioğlu, s. 178.

neler belge değil, belirti delili niteliğindedir.[11] Belirtiler, keşif[12] veya bilirkişi incelemesiyle[13] ortaya çıkabilecek ve olaydan geriye kalan iz ve eserlerdir.[14] Belge delillerinin konusu bir düşüncenin aktarılması olup zihinsel olarak algılanması söz konusuyken, belirti delilleri beş duyu organıyla (işitme, görme, dokunma, koklama, tatma) algılanabilir niteliktedir.[15] Failin iradesi dışında olaydan geriye kalan iz ve eserler (tükürük, ayak izleri gibi) "*tabii belirti*" olarak, failin iradesiyle veya bir insan tarafından belirli bir amaçla hazırlanmış olan nesneler (düğme, tabanca, bıçak gibi) "*suni belirti*" olarak değerlendirilmektedir.[16] Belirti delilleri, kural olarak dolaylı deliller olup, maddi olayın ispatında tek başlarına yeterli değildirler, çoğu zaman diğer delillerle desteklenmeleri gerekmektedir.[17] Nitekim kanun koyucu CMK m. 214, 215 hükümlerinde *belgenin okunmasından* söz etmekle[18] belge delillerinin, belirti delillerinden farklı olarak beş duyu organıyla algılanamayan fakat zihinsel olarak idrak edilen deliller olma yönünü ortaya koymuştur. Yine Anayasa Mahkemesi[19] ve Yargıtay da bu tür delillerin tek başlarına ispat güçlerinin zayıf olduğunu ve diğer delillerle desteklenmesi gerektiğini belirtmiştir.[20]

Bilişim sistemleri kullanılarak işlenen suçlar ardında dijital deliller olarak nitelendirilebilecek deliller bırakmaktadır.[21] Geleneksel delillerden farklılık arz eden bu delillerin niteliği ve kavramın kapsamının

---

11 Ali Kemal Yıldız, Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu, CHD 2006/2, s. 258; Werner Beulke, Strafprozessrecht, München u.A. 2010, § 10 Rn. 204; Kindhäuser § 21 Rn. 105; Centel/Zafer, s. 269; Claus Roxin/Bernd Schünemann, Strafverfahrensrecht, München 2017, § 28 Rn. 9; BGH NJW 1960, 1582 (1582); BGH NJW 1977, 1545 (1545)

12 Centel/Zafer, s. 222; Ünver/Hakeri, s. 617.

13 Centel/Zafer, s. 273.

14 Centel/Zafer, s. 222.

15 Kindhäuser § 21 Rn. 105.

16 Centel/Zafer, s. 272.

17 Toroslu/Feyzioğlu, s. 198; Centel/Zafer, s. 272.

18 Centel/Zafer, s. 269.

19 AYM T: 18.08.171 E: 1971/41 K: 1971/67 "Yukarıdan beri açıklananlarla varılan sonuç şudur : Başkaca inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının ve gizli ajan raporlarının, bir yurttaşa yapılan "Türkiye Cumhuriyeti Anayasasını teğyir ve tebdile ve bu yasa ile kurulmuş Türkiye Büyük Millet Meclisini İskata veya görevini yapmaktan men'e cebren teşebbüs gayesiyle gizlice ittifak kurmak" gibi çok ağır bir isnada yasama dokunulmazlığının kaldırılması yönünden ciddilik kazandırabilmesi bir hukuk Devletinde düşünülemez…" .

20 Centel/Zafer, s. 269.

21 Devrim Aydın, Ceza Muhakemesinde Deliller, Ankara 2014, s. 86.

ortaya konması gerekmektedir. Dijital/elektronik delilleri, *"bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve veriler"*[22] olarak tanımlamak mümkündür. Bir diğer deyişle, elektronik delillerden anlaşılması gereken sayısal formatta üretilen, dönüştürülebilen ve kaydedilebilen enformasyon teknolojisi (*Informationstechnik-IT)* sistemleri yardımıyla algılanabilir hale gelen her türlü dijital bilgidir.[23] Bu bilgi ve veriler esas itibariyle 0 ve 1'lerden oluşan notasyonlardan meydana gelmekte olup duyu organlarıyla algılanabilir nitelikte değildir; duyu organlarıyla algınabilir hale gelmeleri çeşitli yazılımlarla aktarılmaları halinde mümkün olmaktadır.[24] Ceza muhakemesi sürecinde bu delillerin elde edilmesi, analiz edilmesi ve sunulması adli bilişim adı verilen teknik inceleme yöntemiyle gerçekleşmektedir.[25] Bu anlamda adli bilişimin, delillerin değerlendirilmesi faaliyetinin yargı makamınca yürütüldüğü ceza soruşturması ve kovuşturması bakımından bilirkişilik faaliyeti yürüttüğü ifade edilmekte[26], bilirkişilik faaliyetiyle içeriklerine ulaşılan dijital veriler doktrinde belirti delili olarak nitelendirilmektedir.[27]

Alman hukukunda Türk hukukundan farklı olarak CMK m. 134 hükmünde olduğu gibi dijital delillerin elde edilmesine ilişkin özel bir düzenleme bulunmamaktadır. Bu delillerin elde edilmesi Alman Ceza Muhakemesi Kanunu'nun (StPO) arama ve elkoymaya ilişkin genel hü-

---

22 Muharrem Özen/Gürkan Özocak, Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134), ABD 2015/1, s. 59.

23 Laura Iva Savić, Die digitale Dimension des Stafprozessrechts, Berlin 2020, s. 43.

24 Claudia Warken, Elektronische Beweismittel im Strafprozessrecht-eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, NZWiST 2017, 329 (329).

25 Özen/Özocak, s. 45.

26 Nurullah Kunter/Feridun Yenisey/Ayşe Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, İstanbul 2010, s. 1103, 1105; Gürkan Yaşar Duran, Ceza Muhakemesi Kanunu'nda (CMK) "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", *BÜHFD,* C. 14, S. 173-174, Y. 2019, s. 203; gerçekten de bilgisayar, bilgisayar kütüklerinde ve bilgisayar programlarında arama ve elkoyma tedbirleri koruma tedbiri niteliğinde olmakla birlikte, delillerin ortaya konulması adli otopsi işleminde olduğu gibi zorunlu bir bilirkişilik gerektirmektedir (Kunter/Yenisey/Nuhoğlu, s. 1400; Duran, s. 204, 205). Adli otopside toplanması ve incelenmesi gereken deliller adli tıbbın uzmanlık alanına giren biyolojik ya da tıbbi delillerken, CMK m. 134 bakımından adli bilişimin uzmanlık alanına giren dijital delillerin elde edilmesi, tespiti ve analizi söz konusu olmaktadır (Duran, s. 204, 205).

27 Rolf Hannich/Bruns, Karlsruher Kommentar zur Strafprozessordnung, München 2019, StPo § 110 Rn. 2, 4; Aydın, s. 87; Duran, s. 207.

kümleri olan §§ 94, 102, 103 ve bu verilerin incelenmesine ilişkin § 110 paragrafları gereğince yapılmaktadır.[28] Alman hukukunda bilgisayarların mekanik donanımları (hardware) ve yazılım sistemleri (software) de § 94 StPO kapsamında elkoymaya konu eşya olarak değerlendirilmektedir.[29] Arama sonunda bulunan cihazlara geçici olarak § 110 StPO gereğince incelenmek üzere el konulması mümkündür; bu cihazların incelenmesi kâğıtların incelenmesine ilişkin § 110 StPO hükmü gereğince yapılmaktadır, hükümdeki "*kâğıt*" teriminin geniş yorumlanması gerekmektedir.[30] Bu terimden anlaşılması gereken yazıyla, çizimle, defter tutulmasıyla ve veri tabanları üzerinde işlenerek husule gelen her türlü düşünce açıklamasıdır; düşünce açıklamasının bir madde olarak "kâğıt" üzerinde gerçekleşmiş olması gerekli değildir; insanın kendini ifade edişine hizmet eden her türlü diğer materyaller de bu kapsamda değerlendirilmelidir.[31] Bu şekilde düşünce açıklamasını ihtiva eden cihazlar, bilirkişi incelemesine konu belirti delili niteliğindedir.[32]

B. Bilgisayar, Bilgisayar Kütükleri ve Bilgisayar Programları

CMK m. 134 hükmünde düzenlenen tedbirlerin konusu bilgisayarlar, bilgisayar kütükleri ve bilgisayar programları olarak belirlenmiştir. Temel olarak mekanik donanım (hardware) ve yazılım (software) denilen iki ana unsurun bir araya gelmesiyle oluşan[33] cihaz olan bilgisayar sözlükte, "*çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin*" olarak tanımlanmaktadır.[34] Bilgisayar programla-

---

28 Wolfgang Joecks/Markus Jäger/Karsten Randt/Joecks, Steuerstrafrecht, München 2015, AO § 399 Rn. 17, 62 vd.; Ingeborg Zerbes/Mohammad El-Ghazi, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, 425 (426); BVerfG NJW 2009, 2431 (2434) Rn. 61; BVerfG NJW 2005, 1917 (1920, 1921); BVerfG NStZ 2002, 377.

29 Tido Park, Durchsuchung und Beschlagnahme, München 2018, § 4 Rn. 804; Joecks/Jäger/Randt/Joecks AO § 399 Rn. 62.

30 Jürgen-Peter Graf/Hegmann, BeckOK StPO mit RiStBV und MiStra, München 2020, StPO § 110 Rn. 1-3.

31 KK-StPO/Bruns StPO § 110 Rn. 2; BeckOK StPO/Hegmann StPO § 110 Rn. 3; Dieter Dölling/Gunnar Duttge/Dieter Rössner/Hartmann, Gesamtes Strafrecht Handkommentar, Baden-Baden 2017, StPO §110 Rn. 3.

32 KK-StPO/Bruns StPO § 110 Rn. 2, 4.

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

34 Türk Dil Kurumu, Türkçe Sözlük, Ankara 2005, s. 268.

rı, bilgisayarın, belli işlemleri yerine getirebilmesi için belirli bir düzen ve kurallarla oluşturulmuş komutlardır.[35] Bilgisayar dosyaları olarak da ifade edilebilecek olan bilgisayar kütükleri ise, bir bilgisayar programı aracılığıyla kullanılabilen, sabit ya da taşınabilir nitelikte,[36] verilerin saklandığı, genellikle dayanıklı ve uzun ömürlü bir çeşit depolama aracı olarak tanımlanmaktadır.[37] CMK m. 134 hükmünde her ne kadar "bilgisayarlarda aramadan" söz edilmekteyse de, aramaya konu olan bir nesne olarak bilgisayarın kendisi değil veri tabanıdır.[38] Nitekim doktrinde de isabetli olarak hükümde sayılan tüm kavramları kapsayıcı ve TCK'da yer alan bilişim suçlarında kullanılan terminolojiyle de uyumlu olarak "*bilişim sistemi*" teriminin kullanılması önerilmiştir.[39] Bilişim sistemi kavramı, Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Sistemleri Hakkında Kanun Tasarısı m. 2/1/d hükmünde "*… Bilgisayar, çevre bilimleri, iletişim altyapısı ve programlarından oluşan veri işleme, saklama ve iletmeye yönelik sistemi…ifade eder*" denilerek bilgisayarları, bilgisayar kütüklerini ve bilgisayar programlarını da kapsar şekilde tanımlanmıştır. Bir sistemin, anılan özelliklere sahip bilişim sistemi niteliğinde olup olmadığının tespitinde, uzman bilirkişinin görüşü esas alınmalıdır.[40] Bilişim sisteminin arama konusunu oluşturabilmesi için şüpheliye ait olması, onun mülkiyetinde bulunması gerekmemektedir; kanunda "şüphelinin kullandığı" denilerek üçüncü kişilere ait cihazlar üzerinde de arama yapılabilmesine imkân tanınmıştır.[41] Ancak somut delillere dayalı kuvvetli şüphenin bulunduğu araçlarda arama yapılmalıdır, sırf şüpheli tarafından kullanılmış olabileceği düşüncesiyle şüphelinin bulunduğu ortamdaki tüm cihazların aranması[42] ölçülülük ilkesi bakımından tereddütlere yol açacaktır.

---

35 Batuhan Aktaş, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme", *YÜHFD*, C. 14, S. 2, Y. 2017, s. 219.

36 Murat Volkan Dülger, Bilişim Sistemleri Üzerinde Arama, Kopyalama ve Elkoyma Tedbiri, Ceza Muhakemesi Hukukunda Güncel Konular (Edt. Nur Centel), İstanbul 2015, s. 230.

37 Yaşar/Dursun, s. 18.

38 Joecks/Jäger/Randt/Joecks AO § 399 Rn. 62.

39 Dülger, Bilişim Sistemleri, s. 320.

40 Özge Apiş, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Tedbiri", *Yasama Dergisi*/37, Y. 2018, s. 55.

41 Centel/Zafer, s. 424.

42 Yavuz Erdoğan, Türk Hukuk Sisteminde Bilgisayar Araması ve Bulunan Delillere

Günümüzde bilgisayar olarak adlandırılmamakla birlikte, bir bilgisayarın hemen hemen bütün özelliklerini taşıyan akıllı telefonlar ve tabletler de bu hüküm kapsamında değerlendirilmelidir.[43] Nitekim Yargıtay da bu tür cihazlarda yapılacak inceleme işlemleri hakkında CMK m. 134 hükmünün uygulanma alanı bulacağını belirtmiştir.[44] Doktrinde bir görüşe göre, bu cihazların farklı özelliklerinden yola çıkılarak uygulanacak tedbir belirlenmelidir; buna göre cep telefonunda yapılan arama ya da elkoymanın cihazın telefon özelliği ile ilgili olması, konuşma veya mesaj kayıtlarının incelenecek olması halinde tedbir genel aramaya ilişkin CMK m. 119 gereğince; yapılan işlemin cihazın bilgisayar özelliğiyle ilgili olması, örneğin arama motoru, trafik kaydı, e-posta kayıtları gibi verilerin incelenmesi söz konusuysa CMK m. 134 hükmü gereğince gerçekleştirilecektir.[45] Bu görüşe katılmak mümkün değildir; zira kişiler arasında telefon üzerinden gerçekleştirilen mesaj kayıtlarıyla internet üzerinden gerçekleştirilen e-posta kayıtları arasında birinin gsm servis sağlayıcısı üzerinden diğerinin ise internet servis sağlayıcısı üzerinden gerçekleşmesi dışında hiçbir fark bulunmamaktadır. Kaldı ki günümüzde kişiler arası aynı mesajlaşma programının hem cep telefonunda hem de bilgisayarda yüklenmiş şekilde bulunması ve aynı kayıtlara her iki ayrı cihaz üzerinden de ulaşılabilmesi mümkündür; bu halde anılan görüş çerçevesinde düşünüldüğünde ilgili mesajların cep telefonu üzerinden incelenmesi halinde genel arama tedbirine göre, bunların bilgisayar üzerinden incelenmesi halinde ise CMK m. 134 hükmünde yer alan özel düzenlemeye göre işlem yapılacaktır. Böyle bir uygulama farklılığının tercih edilmesi ise ikna edici görünmemektedir.

Elkonulması, Bilgi Sistemleri ve Bilişim Yönetimi (Edt. Fahrettin Özdemirci/Zeynep Akdoğan), Ankara 2017, s. 178.

43 Özen/Özocak, s. 69; Duran, s. 209; Aktaş, s. 219.

44 Yargıtay 17. CD. T: 15.02.2017 E: 2015/27517 K: 2017/1716; "…Cumhuriyet savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda K ismiyle kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkumiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hakim kararı alınması gerektiği bu kararın alınmaması nedeniyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı…".

45 Özen/Özocak, s. 69, 70.

Burada değinilmesi gereken bir diğer husus da elektronik postalar (e-posta/e-mail) hakkında hangi tedbirin uygulanma alanı bulacağıdır. Elektronik posta sistemlerini mail user agent (MUA) ve webmail sistemleri olarak ikiye ayırmak mümkündür. Bu sistemlerden ilkinde, belirli bir cihazda yüklü olan e-posta programları aracılığıyla posta alışverişi gerçekleştirilmekte, postanın cihaza yüklenmesi söz konusu olmaktadır; cihaz üzerinden internet bağlantısı bulunmadığında dahi daha önce indirilmiş olan bu postalara ulaşmak mümkün olduğu gibi, çevrimdışı olarak elektronik posta yazmak ve bunu taslak halinde kaydetmek de mümkündür.[46] Bu sistemde aracı yazılım yoluyla elektronik postalar, üye olunan elektronik posta servisinin serverından alıcının cihazına aracı yazılım vasıtasıyla indirilmektedir.[47] Kısaca burada elektronik postalarla ilgili süreç bunların yazılması, göndericinin serverına yollanması (burada postanın kayda alınması), buradan alıcının serverına ulaştırılması, alıcının serverından alıcıya ulaştırılması ve alıcının posta kutusunda erişime sunulmasından meydana gelmektedir.[48]

Bir diğer sistem olan webmailde ise doğrudan herhangi bir cihazda bulunan yazılıma bağlı olunmadan elektronik posta serverına internet tarayıcısı üzerinden ulaşılarak e-postalara buradan erişilmesi söz konusudur; webmail sisteminde diğerinden farklı olarak elektronik postalar cihaza indirilmemekte, kullanıcı doğrudan internet tarayıcısı üzerinden servera bağlanarak e-postalarına ulaşmakta, internet bağlantısı olmaksızın bunlara ulaşamamaktadır.[49] Yine webmail sisteminde diğerinden farklı olarak doğrudan server üzerinden postanın gönderilmesi söz konusu olduğundan gönderilen postanın yazılım üzerinden, göndericinin serverında ara kayıt şeklinde kaydedilmesi söz konusu olmamakta, posta doğrudan server üzerinden gönderilmektedir.[50] Alman hukukunda doktrin ve yargı uygulamasında postanın henüz servera ve serverdan alıcıya transfer sürecinde olması halinde iletişimin denetlenmesine ve izlenmesine ilişkin tedbirin uy-

46 Park § 4 Rn. 808; bu tür sistemlere akıllı telefonlarda ve bilgisayarlarda yüklü bulunan elektronik posta programları (örneğin Outlook, Apple Mail) örnek gösterilebilir.
47 Park § 4 Rn. 808.
48 Park § 4 Rn. 808.
49 Park § 4 Rn. 808.
50 Park § 4 Rn. 808.

gulama alanı bulacağı hususunda görüş birliği bulunmaktadır.[51] Postanın MUA sisteminde, serverda ara kayıt halinde olduğu duruma ilişkin olarak BGH[52], elektronik posta sağlayıcısında (e-mail provider) bu iletilere el konulmasının kıyasen, postada el konulmasına ilişkin hükümlere (§§ 99 StPO) göre yapılması gerektiğini belirtmiştir. Alman Federal Anayasa Mahkemesi, bu halde iletişimin gizliliğine ilişkin Anayasa'nın 10. maddesinde düzenlenen menfaatin etkilendiğini kabul etmekle birlikte, meselenin elkoymaya ilişkin genel hükümlere (§§ 94 vd. StPO) göre değerlendirilmesi gerektiğini belirtmiştir.[53] Bu halde mahkemeye göre her ne kadar Telekomünikasyon Kanununun 3. maddesinde tanımlandığı anlamda dinamik bir süreç söz konusu olmayıp iletiler elektronik posta sağlayıcısında statik bir şekilde bekliyor olsa da, Anayasa m. 10 hükmü yalın olarak Telekomünikasyon Kanunu'nda esas alınan telekomünikasyon terimini esas almamakta, iletişim, komünikasyon akışına üçüncü kişilerin dahil olmasından dolayı hak sahiplerini ve bunların korunmaya değer menfaatlerini esas almaktadır.[54] Yine aramaya ilişkin genel hüküm olan § 94 StPO ve postada elkoymaya ilişkin § 99; iletişimin denetlenmesine ilişkin § 100a ve iletişim bilgilerinin elde edilmesine ilşkin § 100g StPO hükümlerinin düzenlendikleri yerin sistematiğinden Anayasanın 10. maddesinde düzenlenen temel hakka müdahaleye izin veren hükümlerin yalnızca §§ 99, 100a, 100g StPO hükümlerinden kaynaklandığı sonucuna varılması doğru değildir.[55] Mahkemeye göre bu halde iletişimin gizliliğine ilişkin menfaat söz konusu olmakla birlikte §§ 94 vd. StPO hükümleri esas olarak yeterli hukuki gerekçeyi sunmaktadır, § 94 hükmü kapsamına fiziki nitelikte olmayan varlıklar da dahildir, bu anlamda tedbir aramaya ilişkin kurallara uygun olarak muhatabının bilgisi dahilinde, açık şekilde gerçekleştirilmelidir.[56] Federal Anayasa Mahkemesinin bu kararı elektronik postaların ele geçirilmesinde arama ve elkoymaya ilişkin genel kuralların yeterli görülmesinin koruma alanını zayıflatacağı yönünden eleştirilmiş, § 100a StPO hükmünde düzenlenen tedbire uygun şekilde nitelikli şartların arandığı gizli bir tedbir olarak yerine getirilmesinin daha isabetli olacağı belirtilmiştir.[57]

---

51 Joecks/Jäger/Randt/*Joecks* AO § 399 Rn. 71; Park § 4 Rn. 810.
52 BGH NJW 2009, 1828 (1828).
53 BVerfG NJW 2009, 2431 (2436) Rn. 55 vd.
54 BVerfG NJW 2009, 2431 (2436) Rn. 47.
55 BVerfG NJW 2009, 2431 (2436) Rn. 57.
56 BVerfG NJW 2009, 2431 (2436) Rn. 55 vd.
57 Werner Beulke/Sabine Swoboda, Strafprozessrecht, Heidelberg 2018, § 12 Rn. 253b.

Elektronik posta iletilerine alıcı ya da gönderinin bilişim sisteminde bulunması halinde, elektronik posta sağlayıcısının hâkimiyet alanında bulunmadığı için iletişimin gizliliği söz konusu olmayacaktır. Bu halde elkoymaya ilişkin genel hükümler uygulanma alanı bulacaktır, zira bu halde artık iletişim ve haberleşme hürriyetini düzenleyen Anayasanın 10. maddesinden kaynaklanan özgürlüklere değil fakat özel hayatın gizliliğine ve kişinin maddi ve manevi varlığını geliştirme hürriyetini düzenleyen m. 2 ve 13 hükümlerinden kaynaklanan özgürlük alanına müdahalenin söz konusudur ve bu müdahalenin de elkoymaya ilişkin genel hükümler gereğince yapılması gerekmektedir.[58] Bir diğer deyişle; postanın yazılması ve göndericinin serverına ulaşması, göndericinin serverından alıcının serverına ulaşması, alıcının serverından postanın alıcının erişimine sunulmak üzere aracı yazılıma ulaştırılması aşamalarında iletişimin denetlenmesine ilişkin tedbirler söz konusuyken, diğer aşamalarda elkoymaya ilişkin genel hükümler uygulanma alanı bulacaktır.[59] Webmail servislerinin söz konusu olduğu hallerde aynı şekilde serverda kayıtlı olan elektronik postalar hakkında da elkoymaya ilişkin genel hükümler geçerli olacaktır.[60]

III. BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİNİN DİĞER ARAMA VE ELKOYMA TEDBİRLERİYLE İLİŞKİSİ

Bilişim sistemlerinde arama koruma tedbirinin genel arama tedbiri ile ilişkisi konusunda doktrinde farklı görüşler ileri sürülmüştür. Bir görüşe göre, CMK m. 134 hükmünde düzenlenen tedbir arama ceza muhakemesi koruma tedbirinin bilgisayar kütük ve programlarında icrasıyla ilgili özel bir hükümdür,[61] burada kural arama tedbiri olup, elkoyma tedbiri ikincil ve istisnai olarak düzenlenmiştir.[62] Bu görüşe göre, CMK m. 134 hükmünde düzenlenen arama tedbiri hakkında CMK m. 141-144 hükümlerinde, CMK m. 134 hükmünde sayılan arama işlemleri özel olarak düzenlenmediğinden tazminat istemi söz konusu

58 Park § 4 Rn. 810; Beulke/Swoboda, § 12 Rn. 253b.
59 Park § 4 Rn. 811, 815.
60 Park § 4 Rn. 816.
61 Ünver/Hakeri, s. 428.
62 Yener Ünver, Durchsuchung des Computers im Rahmen des Art. 134 tStPO, Strafrecht und moderne Technologien-Ceza Hukuku ve Modern Teknolojiler (Hrsg. Gunnar Duttge/Yener Ünver), Ankara 2018, s. 215.

olamamaktadır, bu halde bilişim sistemlerinde hukuka aykırı olarak arama gerçekleştirilmesi halinde İdari Yargılama Usulü Kanunu gereğince idare mahkemeleri önünde tam yargı davası açılarak tazminat istenebilecektir.[63] Hukuka aykırı bir elkoyma işleminden kaynaklanan tazminat istemlerinde ise, özel norm olarak CMK m. 141-144 gereğince ceza mahkemesi önünde tazminat davası açılması mümkündür.[64] Ancak bu görüş bir yandan CMK m. 134 hükmünde yer alan düzenlemenin genel arama karşısında özel bir düzenleme olduğunu belirtmekte ancak hukuka aykırı olarak gerçekleştirilen aramalar hakkında CMK hükümlerinin uygulanmayacağını ifade etmektedir. Diğer yandan bu görüş kapsamında arama tedbirinde başvurulmamakla birlikte, elkoyma tedbirinde koruma tedbirlerinden kaynaklanan tazminat istemlerinde CMK'da yer alan hükümlerin uygulanma alanı bulacaktır. CMK m. 141[65] hükmünde ayrıca CMK m. 134 hükmünde yer alan koruma

63 Ünver, s. 199, 200.

64 Ünver, s. 200.

65 CMK m. 141 hükmünde koruma tedbirleri nedeniyle tazminat istemine konu olabilecek durum olarak "arama tedbirinin ölçüsüz şekilde gerçekleştirilmesi" sayılmıştır, hükmün lafzından ilk olarak tedbirin uygulanmasında ölçülülük ilkesine aykırılık halinde tazminat isteminin söz konusu olabileceği, hukuka aykırı arama kararlarından kaynaklı olarak bu hükme başvurulamayacağı anlaşılmaktadır. Ancak Yargıtay bu hususa ilişkin olarak hukuka aykırı aramalar hakkında da bu hükme dayanılarak tazminat talebinin söz konusu olabileceğini belirtmiştir. Nitekim Yargıtay 12 CD 24.12.2013-9105/30731 sayılı kararına göre: "Fıkra düzenlemesinden genel olarak, tazminat isteminin haksız arama kararı veya hukuka aykırı arama kararına değil, arama kararının ölçüsüz şekilde yerine getirilmesine dayanması gerektiği anlaşılmakta ve Dairemiz uygulamaları da bu yönde ise de açıkça hukuka aykırı olarak verilen bir arama kararı için tazminat isteminde bulunup, bulunulamayacağının da değerlendirilmesi gerekmektedir… Tazminat talebinin dayanağını oluşturan arama kararı bu açıdan değerlendirildiğinde, somut delile dayanmayan, içinde makul şüpheyi barındırmayan, sadece bir telefon ihbarı üzerine davacının evinde arama yapıldığı anlaşılmakta olup, talep açısından ayrıca maddenin öngördüğü "makul şüphe" kavramı üzerinde de durulmalıdır…Hâkimin hangi delil unsurlarına dayanarak ihtilaflı arama emrini çıkardığı açık bir şekilde ortaya konmamış, sadece emniyet müdürlüğünün Cumhuriyet savcısına gönderdiği yazıda yer alan oldukça genel, kısa ve öz açıklamalarla yetinilmiştir. Bu noktada AİHM, ceza mahkemelerinin ilgili şahısların evlerinde arama yapılmasını gerektirecek somut deliller olmadığı yönündeki tespitlerini kayda geçmektedir… Cumhuriyet Savcılığınca işin gereği araştırılmaya başlanmadan, ortada makul şüphe olduğuna dair bir delil ve başka kişi veya olaylar hakkında yapılan bir soruşturma da bulunmadığı ve yapılan aramanın AİHM kararlarındaki ölçütlere ve ilkelere uygun olmadığı dolayısıyla hukuka aykırı olduğu anlaşılmakla davacı lehine makul bir miktar manevi tazminata hükmedilmesi gere-

tedbirinin sayılmış olmaması, tazminata ilişkin bu hükmün uygulanamaması için, CMK m. 134 hükmünde düzenlenen tedbirin genel arama karşısında özel bir düzenleme olarak kabul edilmesi halinde ikna edici bir gerekçe teşkil etmemektedir. Daha isabetli görünen diğer bir görüşe göre CMK m. 134 hükmünde düzenlenen tedbir, genel arama ve elkoyma tedbirlerinin özel bir görünümünü oluşturmaktadır[66] ve bu nedenle bu tedbirlerin hukuka aykırı olarak uygulanmasından kaynaklanan zararların tazmininde CMK m. 141-144 hükümleri uygulanma alanı bulacaktır.[67]

Doktrinde bir görüşe göre kişinin özel hayat beklentisinin azaldığı ya da ortadan kalktığı hallerde, bilgisayarlarda arama yapılabilmesi genel arama tedbirine ilişkin kurallarla gerçekleştirilebilecektir.[68] Somut olaylar bakımından makul bir insan tarafından, özel hayatın alenilik kazanmadığının anlaşılabilir olması halinde, özel hayat beklentisinin varlığından söz edilecektir.[69] Örneğin kişinin bilgisayarını başka bir kişiye sattığı ve içerisindeki verileri silmediği durumda bu verilere ilişkin özel hayat beklentisinin azaldığından söz edilecektir, ancak kişinin bu verileri bilgisayarın çöp kutusu bölümüne aktarmış olması halinde özel hayatının korunmasına ilişkin beklentisinin devam ettiği kabul edilmelidir.[70] Kişinin özel hayat beklentisinin azaldığı ya da ortadan kalktığı hallerde üçüncü kişiler tarafından bu verilerin elde edilmesi halinde, verilerin hukuka aykırı olarak elde edildiğinden söz edilemeyecektir.[71] Buna göre örneğin, bilgisayarını tamir için teslim eden bir kişinin cihazında, teknik servis elemanının çocuk pornografisi niteliğinde veriler tespit etmesi ve bu konuda adli makamlara ihbarda bulunması halinde, teknik servis elemanı tarafından elde edilen verilerin hukuka uygun olarak kabul edilmiş olacağı, zira kişinin özel hayatının gizliliğine ilişkin makul bir beklentisinin

kirken, yazılı gerekçelerle davanın reddine karar verilmesi, kanuna aykırı…dır." (Aktaran: Centel/Zafer, s. 470 dn. 346).

66 Centel/Zafer, Apiş, s. 68; s. 424; Yargıtay 16. CD. T: 21.04.2016 E: 2015/4672 K: 2016/2330 (Aktaran: Duran, s. 191 dn. 69).

67 Duran, s. 234.

68 Duran, s.184, 186.

69 Feridun Yenisey/Ayşe Nuhoğlu, Ceza Muhakemesi Hukuku, Ankara 2017, s. 422.

70 Yenisey/Nuhoğlu, s. 422, 423.

71 Yenisey/Nuhoğlu, s. 423.

bulunmadığı ifade edilmiştir.[72] Ancak özel hayat beklentisine ilişkin mesele, açıklandığı gibi, üçüncü kişiler tarafından verilerin elde edilmesi halinde bunların hukuka uygun yollardan elde edilip edilmediği tartışmasıyla ilgili olup, arama koruma tedbiri bakımından bir etkisi bulunmamaktadır. Kaldı ki, burada üçüncü kişiler tarafından yapılan inceleme, koruma tedbirlerini yürütmekle yetkili organlar tarafından yapılan "arama koruma tedbiri" niteliğinde olmayıp, değerlendirmeye konu olan husus üçüncü kişilerin özel hayatın gizliliğini ihlal edip etmediği ve bu surette verilere erişiminin hukuka aykırı olup olmadığıdır. Buradan yola çıkılarak genel arama tedbirine ilişkin koşulların adli makamların bilişim sistemlerinde arama işlemini gerçekleştirmesi için yeterli olacağı sonucuna ulaşmak isabetli görünmemektedir. Öte yandan kanunda özel hayat beklentisine göre bir ayrım yapılmamış olması karşısında, bu şekilde koruma tedbirinin uygulanma alanının genişletilmesi kanunilik ilkesine de aykırılık teşkil edecektir.

Doktrinde bir görüşe göre konutta veya işyerinde CMK m. 134 hükmünde yer alan tedbirin konusunu oluşturan araçların bulunabilmesi için gerçekleştirilecek arama, CMK m. 134 gereğince gerçekleştirilecek aramanın zorunlu bir unsuru olarak görülmelidir.[73] Bu bakımından bilgisayarların veya diğer araçların bulunabilmesi amacıyla konutta veya işyerinde yapılacak aramalarda CMK m. 116 vd. hükümleri gereğince ayrıca arama kararı verilmesine gerek bulunmamaktadır.[74] Ancak CMK m. 134 gereğince konutta veya işyerinde yapılan aramada yalnızca bilgisayar ya da diğer araçlar aranabilecek, bu kapsamın dışına çıkılarak şüpheliye ait diğer evrak veya çeşitli belgeler aranamayacaktır; bu kapsamında dışına çıkılması halinde elde edilen deliller hukuka aykırı nitelikte olacaktır.[75] Bu görüşe göre, şüphelinin kullandığı bilgisayarı saklamak için üçüncü bir kişiye vermesi durumunda, CMK m. 134 hükmüne dayanılarak yapılan arama kapsamında üçüncü kişilerin konutunda arama yapılabilmesi

---

72 Tara McGraw Swaminatha, The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defences, Yale Journal of Law and Technology, C. 7 S. 1, Y. 2005, s. 54-60.

73 Yaşar/Dursun, s. 22.

74 Yaşar/Dursun, s. 22.

75 Yaşar/Dursun, s. 22.

de mümkün olacaktır.[76] Daha isabetli görünen bir diğer görüşe göre, CMK m. 134 hükmünde düzenlenen tedbirlerin konusu şüphelinin kullandığı bilişim sistemleri olup; şüpheli veya üçüncü bir kişinin konutu ya da işyerinde bu hüküm kapsamında arama yapılması mümkün değildir.[77] Genel arama ve CMK m. 134 hükmünde düzenlenen arama arasındaki ilişki, hakkında tutuklama kararı verilmiş olan kişilerin tutuklanmasının yakalamayı da içinde barındırdığı hallerde olduğu gibi araç- amaç tedbir ilişkisine benzetilmemelidir. Hakkında tutuklama kararı verilmiş olan bir kişinin bu kararın yerine getirilmesi amacıyla yakalanması, tedbirlerden birinin diğerinin unsurunu oluşturduğu bu hal, Yakalama, Gözaltına Alma ve İfade Alman Yönetmeliği m. 5/d hükmünde kolluğun doğrudan yakalama işlemini gerçekleştirebileceği bir durum olarak ayrıca düzenlenmiştir. Genel arama ve CMK m. 134 gereğince yapılacak arama işlemleri arasında ise böyle bir bağ bulunmamaktadır. Bu nedenle CMK m. 134 hükmü gereğince şüphelinin kullandığı bilişim sistemlerinin incelenmesi söz konusu olduğunda, bu cihazların konutta veya işyerlerinde arama yapılarak bulunması gerektiğinde ayrıca CMK m. 116 vd. hükümleri gereğince genel aramaya ilişkin şartların yerine getirilmesi gerekmektedir.[78] Aranan cihazların bulunması halinde genel arama işlemi sona erecektir, bu noktada bilişim sistemlerinde arama işlemlerinin gerçekleştirilmesi sırasında genel aramada bulunması gereken kişilerin hazır bulunup bulunamayacağı sorusu ortaya çıkmaktadır. Daha önce değinildiği gibi CMK m. 134 hükmü, genel arama karşısında özel hüküm niteliğindedir, bu nedenle arama sırasında hazır bulunması gereken kişilere ilişkin CMK m. 120 hükmü kıyasen uygulanmalıdır.

Yine CMK m. 134 hükmü kapsamdaki cihazların aranmasının avukat bürolarında ya da askeri mahalde gerçekleştirilecek olması halinde CMK m. 119/5, 130 hükümlerinde öngörülen şartların ayrıca yerine getirilmiş olması gerekmektedir.[79]

---

76 Duran, s. 193.
77 Duran, s. 193.
78 Duran, s. 193, 194.
79 Duran, s. 194-196, 198.

IV. ARAMA VE ELKOYMA TEDBİRLERİNİN UYGULANMA ALANI VE ŞARTLARI

A. Tedbirlerin Uygulanma Alanı

1. Kişi Bakımından Uygulanma Alanı

CMK m. 134 hükmünde sayılan tedbirlerin muhatabının şüpheli olduğu belirtilmiştir; şüpheli dışındaki kişilerin kullandığı bilişim sistemlerinde arama yapılıp yapılamayacağı hususunda ise doktrinde farklı görüşler bulunmaktadır. Bir görüşe göre CMK'da düzenlenmese de mağdurun rızası bulunması halinde mahkeme kararı gerekmeksizin arama yapılabilecektir.[80] Ancak mağdurun rızasının bulunması halinde mahkeme kararının aranmayacağına ilişkin Adli ve Önleme Aramaları Yönetmeliği m. 8/f hükmünde yer alan *"ilgilinin rızası ile"* ibaresi Danıştay kararıyla iptal edilmiştir.[81] Bu nedenle suç şüphesi altında bulunmayan mağdur veya tanık gibi üçüncü kişilerin kullandığı bilişim sistemlerinde arama yapılmasının dayanağı bulunmamaktadır.[82]

Bu noktada ayrıca özellikle bulut bilişim sistemlerinde söz konusu olan, verinin harici, üçüncü kişiye ait olan sistemlerde depolanması halinde bilişim sistemlerinde arama, kopyalama ve elkoymaya ilişkin kuralların uygulanıp uygulanamayacağı üzerinde durulmalıdır. Bu husus Sanal Ortamda İşlenen Suçlar Sözleşmesi m. 19/2 hükmünde de düzenlenmiş olup, Alman hukukunda sözleşmeyle uyum sağlanması amacıyla kâğıtların incelenmesine ilişkin StPO § 110 hükmünde 2007 yılında yapılan değişiklikle, arama işleminin konusunu oluşturan veri taşıyıcısından, başka bir yerde bulunan veri taşıyıcısına uzaktan erişimin bulunması ve verilerin kaybolma tehlikesinin bulunması halinde, uzakta bulunan veri taşıyıcısına erişilerek verilerin temin edilebileceği ve bunların incelenmek üzere muhafaza altına alınabileceği düzenlenmiştir.[83]

---

80 Erdoğan, s. 182.

81 Danıştay Onuncu Dairesinin T: 13.03.2007 E: 2005/6392 K:2007/948 sayılı Kararı; bu karar Danıştay İdari Dava Daireleri Kurulu T:14.09.2012 E: 2007/2257 K: 2012/1117 sayılı kararı ile onanmıştır (Bkz. Adli ve Önleme Aramaları Yönetmeliği dn. 1).

82 İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", *Fasikül Dergisi*, S. 9, Y. 2010, s. 28; Ünver, s. 210.

83 KK-StPO/Bruns StPO § 110 Rn. 8.

Türk hukukunda uzaktan erişime konu olan bu sistemlerde tedbirin uygulanması Adli ve Önleme Aramaları Yönetmeliği m. 17/3 hükmünde "*Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır*" denilerek düzenlenmiştir. Ancak koruma tedbirlerinin kapsamının yönetmelikle genişletilmesinin, kanunilik ilkesi bakımından tereddütleri de beraberinde getirdiği ifade edilmelidir.[84] CMK m. 134 hükmünün ise bulut sistemlerinde arama yapılabilmesi için kanuni dayanak oluşturmadığı, zira burada failin kullanmadığı -verilerin depolandığı- bir bilgisayarda arama işleminin gerçekleştirilmesinin söz konusu olduğu, CMK m. 134 hükmüne göre yapılan aramada ancak failin kullandığı bilgisayarlarda fiziki olarak mevcut bulunan verilerin aranabileceği, uzaktan erişim yoluyla elde edilen delillerin bu nedenle hukuka aykırı delil niteliğinde olacağı doktrinde belirtilmiştir.[85] Yine bu sistemde verilerin fiziki olarak depolandığı yerin failin kullandığı cihazlar dışında olması, verilerin başka bir ülkede depolanmış olabilmesi ve hatta sürekli göç halinde bulunabilmesi, bu halde bulut bilişim sağlayıcısının dahi verilerin hangi zamanda nerede bulunduğuna dair bilgiye sahip olmama ihtimalinin bulunması, yargı yetkisi bakımından sorunları da beraberinde getirmektedir.[86] Öte yandan verilerin yargı yetkisi içinde depolanmış olması halinde dahi, veri dağıtım teknolojilerinin bir kullanıcının verilerini bulut bilişim ortamındaki bir dizi veri depolama aygıtına bölerek depolamış olmasının mümkün olduğu ifade edilmiştir.[87]

Bulut bilişim, enformasyon tekniği altyapılarının internet üzerinden kullanıcıların hizmetine sunulduğu platformlara ilişkin kapsayıcı

84 Erdoğan, s. 181.

85 Özde Dereboylular, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği", *CHD*, S. 39, Y. 2019, s. 183, 184.

86 Dereboylular, s. 170, 171.

87 Dereboylular, s. 172; nitekim Rusya'da bu tür sorunların önüne geçmek amacıyla 241 sayılı Federal Kanun'la Rus vatandaşlarının verilerinin Rusya Federasyonu dışında depolanmasının yasaklandığı belirtilmiştir (Dereboylu, s. 174); Irina Diz, Anwendbarkeit und Reichweite der Befugnisse gem. §§ 110 III, 100j StPO im hinblick auf "Cloud Computing" und "Cloud Storage", Strafrecht und moderne Technologien-Ceza Hukuku ve Modern Teknolojiler (Hrsg. Gunnar Duttge/Yener Ünver), Ankara 2018, s. 187.

bir kavram olarak kullanılmaktadır.[88] Harici bir alanda verilerin depolanmasının söz konusu olduğu sistemlerde kullanıcı internet aracılığıyla bir server üzerinden ya da bir hizmet paketi kapsamında (webspace) harici depolama alanına ulaşmaktadır.[89] Bu tür sistemlere daha önce değinilen elektronik postaların serverda kaydedildiği webmail uygulamaları, dropbox, Google drive, Skydrive gibi uygulamalar örnek gösterilebilir.[90]

Alman hukukunda da bulut bilişim sistemlerinde yer alan veriler söz konusu olduğunda nasıl bir yöntem izleneceği konusunda farklı görüşler ileri sürülmüştür. Esas itibariyle doktrinde bilgisayar kütüklerinin ülke içerisinde bulunduğu durumlara ilişkin görüş birliği mevcut olup, bu tür verilere aramaya ilişkin genel hükümler gereğince ulaşılması ve bu verilerin StPO § 110 III hükmü gereğince incelenebilmesi ve muhafaza altına alınabilmesi mümkündür; bu halde tedbirden üçüncü kişilerin etkilenmesi söz konusu olduğu için StPO § 110 III/2 nin atfı ile StPO § 98 II gereğince mahkeme kararı gerekli olup, StPO § 33 II, III gereğince kütüğün sahibi konumunda bulunan üçüncü kişilere mahkemede dinlenme hakkı tanınmalıdır.[91] Bu verilerin şifre koruması altında bulunması halinde şifrelerin bilişim uzmanlarınca hukuka uygun bir arama emrine dayalı olarak kırılması mümkün olup, burada arama tedbirinde söz konusu olan, hukuka uygun, orantılı bir zorlamadan söz edilecektir.[92] Buna karşın verilerin yurtdışında bulunduğu hallerde hâkim görüşe göre, bunlara kamuya açık olarak erişim mümkün olduğunda Sanal Ortamda İşlenen Suçlar Sözleşlemesi m. 32/a gereğince ya da uluslararası hukukta geçerli olan teamül kuralları gereğince erişilebilmesi mümkündür.[93] Ancak erişimin şifre kullanılması gibi çeşitli yollarla kısıtlanmış olması halinde, Sözleşmenin 32/b hükmü gereğince bunlara erişim ancak hak sahibinin rızası veya ilgili devletin hukuki yardımıyla mümkündür; hak sahibinin rızası-

88 KK-StPO/Bruns StPO § 110 Rn. 8.
89 KK-StPO/Bruns StPO § 110 Rn. 8.
90 Magda Wicker, Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, 765 (765).
91 Park § 4 Rn. 824; BeckOK StPO/Hegmann StPO § 110 Rn. 13; KK-StPO/Bruns StPO § 110 Rn. 8.
92 KK-StPO/Bruns StPO § 110 Rn. 8; Diz, s. 186; BeckOK StPO/Hegmann StPO § 110 Rn. 13.
93 KK-StPO/Bruns StPO § 110 Rn. 8a.

nın bulunmaması durumunda ancak uluslararası adli yardımlaşma[94] yoluna başvurulabilecektir.[95] Öte yandan bu usullere uyulmadan elde edilen delillerin, devletlerin egemenlik hakkı ihlal edilerek hukuka aykırı yollarla elde edilmiş olduğunun ve hükme esas alınamayacağının kabulü, hukuka aykırı şekilde bu verilerin elde edilmesinin kasıtlı olarak gerçekleştirildiği, ilgili devletin verilere ulaşılmasını ya da bunların kullanılmasını açıkça reddetmesine rağmen, buna uygun davranılmadığı istisnai hallerde söz konusu olacaktır.[96] Verilerin yer aldığı kütüklerin ülke içerisinde bulunup bulunmadığı ya da nerede bulunduğu tespit edilebilir nitelikte değilse ve soruşturma makamlarının tüm çabalarına rağmen verilerin yurtdışında mı yurtiçinde mi olduğu konusunda bilgi edinilememişse, bu noktada en azından hizmet sağlayıcısının yurtiçinde depolama alanı bulunma imkânı elenmemeli[97] ve verilerin yurtdışında bulunduğunun açıkça saptanamadığı hallerde bunların incelenebileceği ve hükme esas alınabileceği kabul edilmelidir.[98] Ayrıca, gecikmesinde sakınca olan hallerde resmi olarak talepte bulunulmadan önce, verilerin kaybolmasını önlemek amacıyla Sözleşmenin m. 29, 32 hükümleri gereğince Avrupa Birliği ülkeleri arasında verilerin bulunduğu ülke tarafından, bunların geçici olarak muhafaza altına alınmasının talep edilmesine olanak tanınmıştır.[99] Sözleşmenin 25. maddesi gereğince böyle bir talep şekle bağlı olmayıp telefax veya elektronik posta yoluyla da gerçekleştirilebilir.[100]

Verilerin yurtdışında bulunması halinde bunların elde edilmesine ilişkin bir diğer görüşe göreyse, burada uzaktan erişim sağlanan

---

94 Detaylı bilgi için bkz. Durmuş Tezcan/Mustafa Ruhan Erdem/Rıfat Murat Önok, Uluslararası Ceza Hukuku, Ankara 2021, s. 171 vd.).

95 KK-StPO/Bruns StPO § 110 Rn. 8a; Park § 4 Rn. 826.

96 KK-StPO/Bruns StPO § 110 Rn. 8a; Christopher Knauer/Hans Kudlich/Hartmut Schneider/Hauschild, Münchener Kommentar zur StPO, Band I, München 2014, StPO § 110 Rn. 19; BGH NJW 2007, 2269 (2271, 2272).

97 Bu şekildeki düşünce biçiminin arkasında özellikle Amerikan İstihbarat Birimlerinin ülkedeki verilere erişimine ilişkin skandalların ortaya çıkmasından sonra birçok bulut hizmeti sağlayıcısının açıkça Alman hukukunda geçerli olan kişisel verilerin korunmasına ilişkin hükümler uyarınca Almanya içerisinde de depolanacağını duyurmaları ve halihazırda birçok büyük şirketin Almanya'da host-serverlar kullanmalarının bulunduğu belirtilmiştir (KK-StPO/Bruns StPO § 110 Rn. 8a).

98 KK-StPO/Bruns StPO § 110 Rn. 8a.

99 BeckOK StPO/Hegmann StPO § 110 Rn. 15; MüKoStPO/Hauschild StPO § 110 Rn. 18.

100 MüKoStPO/Hauschild StPO § 110 Rn. 18.

kütüklerin hizmet sağlayıcısı tarafından kullanıcıya kiralandığı, kullanıcının fiilen bu kütüklere erişimin bulunmasının yeterli olduğu, nitekim kanunda bunların mülkiyetine sahip olmasının aranmadığı belirtilmiştir.[101] Burada önemli olan yurtiçinden bu kütüklere erişimin sağlanabiliyor olmasıdır; hizmet sağlayıcısının veri depolarının bulunduğu yerde fiziki olarak arama yapılmadığı sürece arama ve inceleme işlemleri bunlara ilişkin genel hükümler olan StPO §§ 102, 110 III gereğince iç hukuk kurallarına göre yapılacaktır; yine bu şekilde arama ve incelemenin yapılabilmesi için verilere yurtiçinden erişilebilir olması ve soruşturmanın yurtiçinde gerçekleştiriliyor olması gerekli ve yeterlidir.[102] Egemenlik ilkesine uygun hareket edilmesi ve devletlerarası yardımlaşma için öngörülen usullerin izlenmesi, arama işleminin bu üçüncü kişi nezdinde fiili olarak yurtdışında gerçekleştirilmesi halinde söz konusu olacaktır.[103]

CMK m. 134 hükmünde yer alan düzenlemede şüphelinin kullandığı bilgisayar kütüklerinden söz edildiği için, Alman StPO'da yer alan düzenlemeye benzer şekilde, şüphelinin kullanımında olan cihazlardan bunlara erişimin bulunması ve verilerin yurtiçinde depolanmış olması halinde CMK m. 134 hükmüne dayanılarak arama, kopyalama ve elkoyma işlemlerinin yapılabileceği kabul edilmelidir. Öte yandan verilerin yurtdışında depolanmış olması halinde CMK m. 134 hükmünün bunlara erişim için hukuki dayanak oluşturmadığı konusundaki eleştiri hatalı görünmektedir. Zira burada mesele başka bir devletin egemenlik alanına müdahale edilmesi olacağından buna yalnızca iç hukukta yapılabilecek bir düzenlemeyle hukuki dayanak kazandırılması en başından mümkün değildir. Bu alanda karşılaşılan sorunların çözümü Sanal Ortamda İşlenen Suçlar Sözleşmesi ile de adres alındığı gibi, uluslararası iş birlikleri ve düzenlemelerle çözülebilecek niteliktedir.

2. Ceza Muhakemesi Evresi Bakımından Uygulanma Alanı

Kanun koyucu, tedbirlerin ancak bir suç dolayısıyla yapılan soruşturmada uygulanabileceğini belirtmiştir. Soruşturma, yetkili makamlarca suç şüphesinin öğrenilmesiyle başlayacak olup (CMK m. 2/1-e), bilişim sistemlerinde arama, kopyalama veya elkoyma tedbirlerine

101 Wicker, s. 766, 767.
102 Wicker, s. 768, 769.
103 Wicker, s. 768.

soruşturmanın başlamasından önce, soruşturmanın başlatılıp başlatılmayacağına karar vermek üzere deliller toplanması amacıyla başvurulamayacaktır. Yine söz konusu soruşturmanın ceza soruşturması olması gerekir, idari ya da disiplin soruşturması nedeniyle bilişim sistemlerinde arama, kopyalama veya elkoyma tedbirlerine başvurulabilmesi mümkün değildir.[104]

Kanun koyucu, tedbirin uygulanma alanı bakımından soruşturma konusu suç yönünden herhangi bir kısıtlamaya yer vermemiştir. Kanun tasarısında yer alan iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren suçlar nedeniyle yapılan soruşturmada bu tedbirlere başvurma şartına, kanunda yer verilmemiştir.[105] Yine diğer bazı koruma tedbirlerinin uygulanması için aranan soruşturma konusu suçun kanunda öngörülmüş olan katalog suçlardan biri olması şartı bu tedbir bakımından aranmamıştır. Doktrinde tedbirin uygulama alanının genel tutulması ve belirli suçlara özgü olarak kısıtlanmamış olması; tedbirle temel haklar üzerindeki gerçekleştirilen müdahalenin ağırlığına işaret edilerek eleştirilmiştir.[106]

Doktrinde bir görüşe göre madde metninde açıkça tedbirin soruşturma aşamasında ve şüphelinin kullandığı bilişim sistemlerine yönelik olarak düzenlenmiş olmasından dolayı, tedbirin kovuşturma aşamasında uygulanması mümkün değildir;[107] kaldı ki duruşmaların aleni olması ilkesinin söz konusu olduğu kovuşturma aşamasında bu tedbire başvurulması halinde, şüphelinin tedbirin uygulanması kararından haberi olacağından delilleri ortadan kaldırmasının her zaman mümkün olabileceği belirtilmiştir.[108] Hükmün lafzından yola çıkarak tedbirin yalnızca soruşturma aşamasında uygulanmasının mümkün olduğunu kabul eden bir diğer görüşe göreyse, tedbirin uygulanma alanının soruşturma evresiyle kısıtlanması hatalıdır; nitekim her ne kadar kovuşturma evresinde alenilik ilkesi hâkim olsa da sanığın tutuklu olması veya herhangi başka bir nedenle ilgili veri taşıyıcılarına ulaşamaması ve delilleri ortadan kaldırma olanağının bulunmaması

104 Cengiz Tanrıkulu, Ceza Muhakemesi Hukukunda Bilişim Sistemerinde Arama ve Elkoyma, Ankara 2014, s. 395; Rezan Epözdemir, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri", *Terazi Hukuk Dergisi*, C. 13, S. 142, Y. 2018, s. 91; Yaşar/Dursun, s. 8.

105 Tanrıkulu, s. 388.

106 Aktaş, s. 235; Centel/Zafer, s. 426.

107 Kunter/Yenisey/Nuhoğlu, s. 1098; Aydın, s. 108; Epözdemir, s. 91.

108 Centel/Zafer, s.

da mümkündür; yine verilerin silinmiş olması halinde de bunların kısmi olarak da olsa geri getirilebilmesi mümkündür.[109] Bu nedenle kanun hükmünde kovuşturma evresinde de tedbirin uygulanmasını mümkün kılacak şekilde değişiklik yapılmalıdır.[110] Tedbirin kovuşturma evresinde de uygulanabilir olduğunu savunan yazarlar ise, bu uygulamaya başvurulabilmesinin gerekçesini, kovuşturma evresinde mahkemenin re'sen araştırma yetkisine sahip olmasında (CMK m. 207) görmektedir.[111] Hükmün lafzından yola çıkarak bu tedbirlerin yalnızca soruşturma aşamasında uygulanmasının mümkün olduğunu belirten görüşler daha isabetli görünmektedir. Nitekim her ne kadar kovuşturma evresinde de delillerin toplanması, mahkemenin bu konuda re'sen yetkili olması söz konusu olsa da CMK m. 134 hükmünde açıkça kıyasa yer bırakılmaksızın bu tedbirlerin soruşturma aşamasında söz konusu olacağı, şüpheli hakkında uygulanacağı belirtilmiştir. Buna karşın doktrinde, uygulamada ihtiyaçların tedbirlere kovuşturma aşamasında da başvurulması yönünde olduğu belirtilmiştir.[112] Yine Yargıtay da bir olayda daha dijital delillerin yeterli ölçüde toplanmadığı ve ilk derece mahkemesi tarafından daha fazla dijital delilin elde edilmesi ve daha ayrıntılı kovuşturma yapılması gerektiği belirtilerek bozma kararı[113]; diğer bir olayda mağdurun cep telefonuna gönderilen mesajın hangi bilgisayardan gönderildiğinin tespit edilmemesi soruşturmada önemli bir eksik olarak değerlendirilerek, bu tespitin kovuşturma aşamasında girilmesi için bozma kararı vermiştir.[114]

B. Uygulanma Şartları

1. Somut Delillere Dayanan Kuvvetli Şüphe Sebeplerinin Varlığı

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine başvurulabilmesi için kanun koyucu, somut delillere dayanan kuv-

---

109 Ünver, s. 217.
110 Ünver, s. 217.
111 Baştürk, s. 25; Yaşar/Dursun, s. 10.
112 Tanrıkulu, s. 399.
113 Yargıtay 1. CD T: 14.11.2011 E: 3891 K: 3230 sayılı kararı (Aktaran: Tanrıkulu, s. 399).
114 Yargıtay 4. CD T: 09.05.2006 E: 16417 K:10607 sayılı kararı (Aktaran: Tanrıkulu, s. 399).

vetli şüphe sebeplerinin varlığını aramaktadır. Doktrindeki eleştiriler doğrultusunda[115] şüphe derecesine ilişkin bu düzenleme, hükme 21/2/2014 tarihli 6526 sayılı Kanun'un 11. maddesiyle eklenmiştir.

Somut delillerden anlaşılması gereken kuvvetli şüphenin oluşmasına imkân tanıyan, yalnızca sübjektif tahminleri esas almayan fakat maddi olguları yansıtan delillerdir.[116] Somut delillerin ilişkili olması gereken, bilişim sistemlerinde arama sonucu suç soruşturmasına ilişkin delillerin elde edileceğini gösteren olgulardır. Arama kararında kuvvetli suç şüphesinin dayanağını oluşturan bu somut delillerin neler olduğu açıkça ortaya konulmalıdır. Öte yandan doktrinde kuvvetli şüphenin, suçun işlendiğine ilişkin şüphe derecesini yansıttığı belirtilmiştir.[117] Ancak hükmün lafzında *"bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı…halinde şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına…"* yer alan ifadesinden, şüphe derecesinin arama işlemine yönelik olarak belirlendiği anlaşılmaktadır. Nitekim CMK m. 135 hükmünde, bilişim sistemlerinde aramadan farklı olarak iletişimin tespiti, dinlenmesi ve kayda alınması tedbirlerinin uygulanabilmesi açıkça *"suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığına"* bağlı tutulmuş, somut delillere dayanan kuvvetli şüphe açıkça suç işlendiğine ilişkin şüphenin[118] derecesi olarak belirlenmiştir. Yine aramaya ilişkin genel hüküm olan CMK m. 116 hükmünde *"…suç delillerinin elde edilebileceği hususunda makul şüphe varsa…aranabilir"* denilerek aranan şüphe derecesi, diğer koruma tedbirlerinden farklı olarak suçun işlendiğine yönelik olarak değil, açıkça suç delillerinin elde edilmesine ilişkin olarak belirlenmiştir. Bilişim

115 Hükümde 2014 yılında yapılan değişiklikten önce doktrinde düzenleme, koruma tedbirlerine başvurulması için gerekli olan belirli bir şüphe derecesine ulaşılmış olmasının CMK m. 134 hükmünde aranmaması yönünden eleştirilmekte, olaylara dayanmayan bir şüphe üzerine soruşturmaya başlanmasının kanuni değil keyfi bir davranış olduğu belirtilmekteydi

116 Ünver, s. 198.

117 Özen/Özocak, s. 62; Apiş, s. 72; Ünver, s. 206; Centel/Zafer, s. 401; "belirtelim ki şüpheli veya sanığın üstünde, eşyasında, konutunda, işyerinde veya ona ait diğer yerlerde aranan şeyin arandığı yerde olduğunu gösteren somut delillere dayalı kuvvetli şüphe, aynı zamanda şüpheli veya sanığın suçu işlediğine dair somut delillere dayalı kuvvetli şüphe demektir."

118 Benzer şekilde CMK m. 100, 128, 133, 139, 140 hükümlerinde açıkça suçun işlendiğine dair kuvvetli şüpheden söz edilmiştir.

sistemlerinde yapılacak olan aramanın özel hayata ve kişinin maddi ve manevi varlığını geliştirme hürriyetlerine genel arama tedbirine kıyasla daha ağır bir müdahale teşkil edecek olması, kanun koyucuyu isabetli olarak bu tedbirin uygulanması bakımından genel arama tedbirinde delillerin mevcudiyetine yönelik aranan şüphe derecesinden daha yüksek bir şüphe derecesinin aranmasına sevk etmiştir. Belirtildiği gibi hükmün lafzından anlaşılan, aranan kuvvetli şüphe derecesinin delillerin bilişim sisteminde bulunduğuna ilişkin olmasıdır; kanun koyucu suçun işlendiğine dair nitelikli bir şüphe derecesinin bulunmasını aramamıştır. Bu iki şüphe derecesinin farkını şu şekilde açıklamak mümkündür; örneğin mağdurun, şüphelinin kendisinin rızası dışında cep telefonuyla fotoğraflarını çektiğini iddia ettiği ve bu yönde tanık beyanının bulunduğu bir soruşturmada, mağdurun ve tanığın beyanları somut deliller teşkil edecek, soruşturma organlarında bu beyanlara dayalı olarak suçun delili niteliğindeki fotoğrafların şüphelinin cep telefonunda bulunduğuna ilişkin kuvvetli şüphe oluşabilecektir.

Ancak henüz soruşturmanın bu aşamasında Cumhuriyet savcısında suçun işlendiğine dair mahkûm olma olasılığının çok yüksek göründüğü kuvvetli şüphenin[119] oluşmamış olması ve bu şüphe derecesine ilgili delillerin elde edilmesiyle ulaşılabilecek olması mümkündür. Benzer şekilde, soruşturma makamında suçun işlendiğine ilişkin soruşturma kapsamında elde edilen deliller sonucunda kuvvetli şüphe oluşmuş olabilir, ancak bu suçun delillerinin şüphelinin kullandığı bilişim sistemlerinde bulunduğuna ilişkin aynı şüphe derecesini oluşturacak deliller mevcut bulunmayabilir. Bunu bir örnek üzerinden açıklamak gerekirse, şüpheli hakkında Sermaye Piyasa Kanunu'nun 106. maddesinde düzenlenen bilgi suistimali suçundan dolayı yürütülen bir soruşturmada, şüphelinin içeriden öğrenen kişi niteliğinde olması ve yatırım hesabında ani bir kazancın gözlenmesi halinde, kazancın elde edildiği işlemin bilgi suistimalinden kaynaklandığına ilişkin diğer delillerle desteklenen kuvvetli şüphe oluşabilir; ancak bu işlemi şüphelinin bilişim sistemlerini kullanarak mı gerçekleştirdiği yoksa aracı kuruma emrin başka yollarla mı iletildiği konusunda aynı derecede kuvvetli şüpheye ulaşılamamış olabilir. Nitekim bilgi suistimali

119 Dülger, Bilişim Sistemleri, s. 318; Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2020, s. 583, 584.

suçuna vücut veren hareket olarak işlem emrinin verilmesi, kişinin bilişim sistemlerini kullanarak internet üzerinden emri iletmesi yoluyla olabileceği gibi, aracı kurum yetkilisine telefon açarak bu emri vermesi de mümkündür.[120] Elbette ki suç delillerinin belirli bir yerde mevcut olduğuna ilişkin şüphenin bulunması, o suçun işlendiğine yönelik şüphenin de varlığına işaret etmektedir. Delillerin belli bir yerde bulunduğuna ilişkin belirli bir kanaat oluştuğunda, delillerin ait olduğu suçun işlendiğine ilişkin de kanaat oluşmuş olacaktır. Ancak CMK m. 134 hükmünün lafzından her iki hususa ilişkin şüphe derecesinin birbirinden farklı olabileceği sonucuna ulaşılmaktadır. Buna karşın, kişilerin özgürlük alanlarına son derece ağır bir müdahale teşkil eden bu tedbirlerin uygulanmasında delillerin arama yapılan yerde bulunacağına dair kuvvetli şüphenin yanı sıra suçun işlendiğine dair kuvvetli şüphenin de bulunması gerektiği ileri sürülebilir. Ancak bu şekilde düşünüldüğünde, bir yandan başka surette delil elde etme imkânının bulunmaması şartı aranırken diğer yandan soruşturma konusu suçun işlendiğine dair kuvvetli şüphenin nasıl oluşmuş olabileceği tereddütü ortaya çıkmaktadır; zira kuvvetli şüpheden anlaşılması gerekenin şüphelinin mahkûm edilmesi konusunda yüksek bir olasılık bulunduğu[121] kabul edildiğinde artık bu yoğunlukta delile ulaşıldığına göre bu tedbire başvurma gereği de bulunmayacak, tedbire başvurulması orantılılık ilkesine aykırılık teşkil edecektir.[122] Nitekim haklı olarak doktrinde başka surette delil elde edilmesi imkânının bulunmaması şartının gerçekleşmiş sayılabilmesi için, soruşturmanın başında veya soruşturma sürecinde başka bir tedbire başvurulmasının olayın aydınlatılmasını olanaksız kılacak olması gerektiği belirtilmiştir.[123] Şu halde bu iki şart birlikte değerlendirildiğinde anlaşılması gereken, suç delillerinin ancak bilişim sistemlerinde yapılacak aramayla elde edilebileceği hususunda kuvvetli şüphenin bulunması ve bu delillere ulaşmanın ise ancak bu tedbirlere başvurulmasıyla mümkün olmasıdır.

---

120 Nitekim bugün birçok banka online olarak borsada işlem emri verilmesi imkânı sağlamanın yanı sıra yatırım işlem hatları üzerinden telefonla işlem emri oluşturulması hizmeti sunmaktadır.

121 Dülger, Bilişim Sistemleri, s. 318.

122 Benzer tereddütler CMK m. 135 hükmünde düzenlenen iletişim tespiti, dinlenmesi ve kayda alınması koruma tedbiri yönünden de geçerlidir, bkz. Bahri Öztürk/Behiye Eker Kazancı/Sesim Soyer Güleç, Ceza Muhakemesi Hukukunda Koruma Tedbirleri, Ankara 2019, s. 270.

123 Öztürk/Eker Kazancı/Soyer Güleç, s. 273.

2. Başka Surette Delil Elde Etme İmkânının Bulunmaması

Başka surette delil elde etme imkânının bulunmaması, Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik m. 4/c hükmünde; *"Soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olması"* şeklinde tanımlanmıştır. Doktrinde bu şarttan anlaşılması gerekenin tüm tedbirlerinin denenmesi neticesinde bir delilin elde edilememesi değil fakat somut olayı aydınlatabilecek delillerin elde edilmesi için ilgili tedbire başvurma zorunluluğunun bulunması olduğu belirtilmiştir.[124] Bu tedbire son çare (ultima ratio) olarak başvurulmalıdır.[125]

Başka surette delil elde etme imkânının bulunmamasına ilişkin düzenlemeyi, soruşturma konusu suç ile ilgili olarak diğer koruma tedbirleri yoluyla hiçbir delilinin elde edilemediği ve suça ilişkin delillerin ancak bilişim sistemlerinde yapılacak arama ile mümkün olabileceği şeklinde anlamamak gerekir. Nitekim suç ile ilgili hiçbir delilin, Cumhuriyet savcısında suçun işlendiği yönünde izlenimin oluşmasına neden olacak hiçbir olgunun[126] bulunmadığı durumda soruşturmanın başlatılması için gerekli olan "basit şüphenin" oluştuğundan da söz edilemeyecektir. Dolayısıyla burada başka türlü delil elde etme imkânının bulunmamasından anlaşılması gereken, soruşturma konusu suçun delili niteliğindeki belli verilere ancak bilişim sistemlerinde yapılacak aramayla ulaşılabilecek olmasıdır.

Bu duruma örnek olarak Cumhuriyet savcısının TCK m. 243 hükmünde düzenlenen bilişim sistemine girme suçunun işlendiğine yönelik olarak ihbar aldığı ve soruşturmanın başlatılması için yeterli şüphenin oluştuğu durumda bu suçun işlendiğine dair delillerin elde

---

124 Aktaş, s. 235; bir diğer görüşe göre CMK'da düzenlenen koruma tedbirleri arasında temel haklara yapılan müdahalenin ağırlığına göre kronolojik bir sıralama bulunmaktadır; bu kronoloji izlenerek uygulanan tedbirler vasıtasıyla elde edilmesi mümkün olan ve olayları ispata yeter deliller mevcut ise o halde başka surette delil elde etme imkânının bulunmadığından söz edilemeyecektir (Tanrıkulu, s. 390).

125 Yaşar/Dursun, s. 12; Baştürk, s. 27.

126 Centel/Zafer, s. 80.

edilebilmesi için şüphelinin bilişim sisteminin incelenmesinin gerekmesi gösterilebilir. Zira burada ihbarın mağdur tarafından yapılmış olması halinde mağdurun beyanı da delil niteliğindedir ve soruşturma konusu suça ilişkin beyan delili niteliğinde delil bulunmaktadır, ancak suçun işlendiğine dair şüphelinin kullandığı bilişim sistemlerinin incelenmesi yoluyla elde edilebilecek delillerin başka surette elde edilmesi imkânı bulunmamaktadır.

Doktrinde bu şartın aranmasının özellikle bilişim suçları ve bilişim sistemleri aracılığıyla işlenmiş suçlar hakkında yapılacak olan soruşturmalarda son derece hatalı olduğu belirtilmiştir.[127] Bu görüşe göre, bu halde yapılması gereken ilk iş, sistemin yapısı ve veri bütünlüğü bozulmadan içindeki bağlantıların ve verilerin tespit edilmesi olacaktır. Zira bu suçlara ilişkin olarak yürütülen soruşturmada genellikle başka surette delil elde etme imkânı bulunmamakta, başka şekillerle delillerin elde edilmesi sağlanmaya çalışıldığında ve son çare olarak bu tedbire başvurulduğunda artık çok geç olabilmekte; faile ve delillere ulaşma imkânı son derece güçleşebilmektedir.[128] Bu görüş, her suç soruşturmasında ilk olarak bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine başvurulması halinde kişisel verilerin güvenliğinin ve özel hayatın korunması imkânının kalmaması tehlikesinin ise kuvvetli şüphe sebeplerinin bulunması şartının gerçek anlamda uygulanmasıyla aşılabileceğini belirtilmiştir.[129] Ancak başka surette delil elde etme imkânının bulunmaması şartından; diğer koruma tedbirlerinin denenmesi fakat sonuç alınamaması değil, fakat belirli bir delilin ancak bilişim sistemlerinde yapılacak arama tedbiriyle elde edilebileceği anlaşıldığında ayrıca bilişim sistemleri aracılığıyla gerçekleştirilen veya bu sistemlere karşı işlenen suçların, delillerin elde edilmesine ilişkin bu nitelikli şarttan hariç tutulmasına da ihtiyaç kalmayacaktır.

3. Hâkim veya Gecikmesinde Sakınca Bulunan Hallerde Cumhuriyet Savcısının Kararı

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine ilişkin CMK m. 134 hükmünün ilk halinde, şüphelinin kullandığı bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine başvurulabil-

127 Dülger, Bilişim Suçları, s. 585.
128 Dülger, Bilişim Suçları, s. 585.
129 Dülger, Bilişim Suçları, s. 585.

mesi Cumhuriyet savcısının istemi üzerine hâkim kararıyla mümkündü. Hükümde 25/07/2018 tarihli 7145 sayılı Kanun'un 16. maddesiyle yapılan değişiklik sonrasında bu tedbirlere gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla da başvurulabilmesi düzenlenmiş[130], Anayasa m. 20 hükmünde uygun olarak Cumhuriyet savcısı tarafından verilen kararların yirmi dört saat içerisinde hâkim onayına sunulacağı ve hâkimin en geç yirmi dört saat içerisinde karar vereceği hükümde belirtilmiştir. Sürenin dolması veya hâkim tarafından aksi yönde karar verilmesi halinde ise çıkarılan kopyalar ve çözümü yapılan metinler derhal imha edilecektir (CMK m. 134/1).

Adli aramalar bakımından gecikmesinde sakınca bulunan halin tanımı kanunda yapılmamıştır, Adli ve Önleme Aramaları Yönetmeliği m. 4 hükmünde *"Gecikmesinde sakınca bulunan hâl: a) Adlî aramalar bakımından; derhâl işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin tespit edilememesi ihtimâlinin ortaya çıkması ve gerektiğinde hâkimden karar almak için vakit bulunmaması hâlini …ifade eder."* denilerek tanımlanmıştır.

Doktrinde düzenlemenin lafzının gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı kararıyla başvurulabilecek tedbirlerin CMK m. 134/1 hükmünde sayılan "arama, kopyalama ve metin haline getirme" işlemleriyle sınırlı olduğu izlenimini yarattığı, nitekim elkoymanın hükmün ikinci fıkrasında düzenlendiği ve Cumhuriyet savcısı tarafından verilebilecek kararların açıkça birinci fıkrada belirtilen arama ve kopyalama işlemlerine ilişkin olarak düzenlendiği, ikinci fıkrada benzer bir düzenleme yapılmamasının bazı tereddütleri doğurduğu belirtilmiştir.[131] Bu durum karşısında, düzenlemeyi iki şekilde yorumlamak mümkündür; öncelikle düzenlemeyle Cumhuriyet savcısı kararıyla elkoyma işleminin yapılamayacağı, bunun için hâkim kararının gerekli olduğu düşünülebilir.[132] İkinci olarak elkoyma tedbiri bakımın-

---

130 Kanunda yapılan bu değişiklik ile 668 sayılı Kanun Hükmünde Kararname ile getirilen gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısın kararı ile bu tedbirlere başvurulması imkânı olağanüstü hâl süresi ile sınırlı olmaktan çıkarılarak kalıcı hale getirilmiştir.

131 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. 146, Y. 2018, s. 151, 152.

132 Değirmenci, s. 152.

dan da birinci fıkrada anılan makamların yetkili olduğu düşünülebilir, ancak bu halde Cumhuriyet savcısı kararıyla elkoyma gerçekleştirilmesi halinde, hâkim kararı için sürenin dolması veya aksine karar verilmesi halinde metinlerin ve kopyaların imha edileceği açıkça düzenlendiği gibi elkoyma işleminde de elkonulan eşyanın iade edilmesine Anayasa m. 20 hükmüne uygun olarak kanunda ayrıca yer verilmesi gerekmektedir.[133] Birinci fıkra hükmünde açıkça elkoyma tedbirine de yer verilmesiyle bu tereddütlerin ortadan kaldırılması mümkündür.

C. Elkoyma Tedbiri Yönünden Aranan Diğer Şartlar

CMK m. 134 hükmünde aramaya konu cihazlara elkonulması işlemi istisnai olarak uygulanabilecek bir işlem olarak öngörülmüş; sistemlere şifrenin çözülememesinden dolayı girilememesi, gizlenmiş bilgilere ulaşılamaması veya işlemin uzun sürecek olması şartlarından birinin gerçekleşmiş olmasına bağlı kılınmıştır. İşlemin uzun sürecek olması nedeniyle elkoyma tedbirine başvurulabilmesi olanağı kanuna 25.7.2018 tarihli 7145 sayılı Kanun'un 16. maddesiyle yapılan değişiklikle eklenmiştir. Doktrinde değişikliğin uygulamadan gelen talepler doğrultusunda yapıldığı, nitekim yerinde yapılacak arama veya kopyalama işlemlerinin çoğu zaman teknik yetersizlik ya da kolluğun sınırlı zamanı nedeniyle gerçekleştirilemediği ve bu halde kanunda düzenlenmeyen bir neden olmasına rağmen uygulamadan kaynaklanan ihtiyaç nedeniyle esasında hukuka aykırı olarak cihazlara el konulduğu belirtilmiştir.[134] Elkoyma tedbirine başvurulabilmesi, hükümde sayılan amaçlarla sınırlı olarak gerçekleştirilebilecek, şifrenin çözülmesi, delillerin kopyalanmasının ardından elkonulan cihazlar derhal iade edilecektir (CMK m. 134/2). Kanun'da bu işlemin ne kadar sürebileceğine dair bir sınırlama öngörülmemiştir; ancak daha önce de belirtildiği gibi burada esas itibariyle adli bilişim uzmanlarınca gerçekleştirilecek bir bilirkişi incelemesi söz konusu olduğundan, bilirkişiliğe ilişkin hükümler kıyasen uygulanmalıdır; buna göre adli bilişim uzmanları tarafından yapılan inceleme üç ayı geçemeyecek, kendisini atayan merciin gerekçeli kararıyla bu süre üç ay daha uzatılabilecektir (CMK m. 66/1).[135]

---

133 Değirmenci, s. 152.
134 Değirmenci, s. 152.
135 Duran, s. 216.

V. TEDBİRLERİN UYGULANMA USULÜ

Bilişim sitemlerinde arama, kopyalama ve elkoyma tedbirlerinin uygulanması esnasında delil toplanması için olay yerinde adli bilişim uzmanının bulunması gerekmektedir; zira dijital nitelikteki bu tür delillerin bilişim sistemlerinde yanlış işlemler sonucu yok olması veya zarar görmesi olasılığı yüksek olup, delillerin sağlıklı bir şekilde elde edilebilmesi için işlemler mutlaka alanında uzman kişiler tarafından gerçekleştirilmelidir.[136] Nitekim olay yerinde adli bilişim uzmanının bulunması, Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik m. 10 vd. hükümlerinin de bir gereğidir.[137]

CMK m. 134 hükmünde kural, verilerin arama yapılan yerde kopyalanmasıdır; bu tedbir kural olarak şüphelinin kullandığı bilişim sistemlerinde arama yapılmasını, sistemdeki verilerin kopyasının çıkarılmasını ve kayıtların çözümü yapılarak metin haline getirilmesini içermektedir.[138] Şüphelinin kullandığı bilişim sistemi, olduğu yerde bırakılacak, kolluk güçleri veri taşıyıcısının veya sistemin aslını almayacaktır.[139] CMK m. 134/5 hükmünde verilerin elkonulmasına gerek kalmaksızın kopyasının alınması halinde kopyası alınan verilerin kâğıda yazdırılacağı, bu hususun tutanağa kaydedilerek ilgililer tarafından imza altına alınacağı düzenlenmiştir. Bu hüküm doktrinde hem gereksiz olduğu hem de yerine getirilmesinin somut olayda maddi olarak imkânsız olmasının mümkün olduğuna işaret edilerek eleştirilmiştir.[140]

CMK m. 134 hükmünde verilerin kopyalanmasından ve elkoyma sırasında sistemdeki bütün verilerin yedeklenmesinden söz edilmiş, ancak kanunda veya yönetmelikte bu işlemlerin nasıl yapılacağına ilişkin bir düzenlemeye yer verilmemiştir. Doktrinde isabetli olarak kopyalama ve yedekleme işlemlerinin verilerin imajı alınarak ve hash değeri oluşturularak şüpheli ve müdafi önünde gerçekleştirilmesi; adli bilişim uzmanlarınca daha sonra yapılacak incelemelerin oluşturulan yedekler üzerinde gerçekleştirilmesi gerektiği belirtilmiştir.[141] Bu şe-

136 Özen/Özocak, s. 65; Duran, s. 205.
137 Kunter/Yenisey/Nuhoğlu, s. 1105.
138 Dülger, Bilişim Sistemleri, s. 320.
139 Dülger, Bilişim Sistemleri, s. 320.
140 Özen/Özocak, s. 70.
141 Dülger, Bilişim Sistemleri, s. 323.

kilde, elde edilen verilerin bütünlüğü ve güvenilirliği sağlanarak, ileride söz konusu olabilecek verilerin değiştirildiğine yönelik iddiaların önüne geçilmiş olacaktır.[142]

CMK m. 134/3 hükmünde elkoyma işlemine başvurulması halinde, elkoyma sırasında sistemdeki bütün verilerin yedeklemesinin yapılacağı, f. 4 hükmünde bu şekilde alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline[143] verileceği düzenlenmiştir.[144] Doktrinde yedekleme işlemiyle kast edilenin, uygulamada imaj alma olarak ifade edilen, fiziksel kopyalama olduğu belirtilmiştir.[145] Fiziksel kopyalamada, bir depolama aygıtının üzerine veri yazılabilen tüm alanlarının, özel bir formatta ve hash değeri hesaplanarak bire bir kopyalanması söz konusu olmaktadır; kopyalamanın herhangi bir adli bilişim dosya formatına çevrilmeden doğrudan verilerin dosya formatında kopyalanması şeklinde gerçekleştirilmesi ise klon kopyalama olarak adlandırılmaktadır.[146] Yine bir veri depolama aygıtının tamamen ya da kısmen kopyalanması (mantıksal kopyalama) yoluna gidilmeksizin, depolama aygıtı içerisindeki bir veya birden fazla dosyanın kopyalanması söz konusu olduğunda bu işlem klasör ya da dosya kopyalama olarak adlandırılmaktadır.[147] Hash değeri, dosyaların parmak izi de denilebilen ve içeriğinde en ufak bir değişiklik yapıldığında değişen, imaj alma işlemi sonrasında elde edilen ve imajı alınan verilerin bir nevi mühürlenmesini sağlayan sayısal bir değerdir.[148] Herhangi bir dosya, belge veya programın orijinali ile farklılık bulunup bulunmadığının tespitinde hash değerine bakılacaktır. Eğer hash değeri, işlem öncesi ve sonrasında aynı ise datada herhangi bir değişiklik olmadığı; farklı ise datada değişiklik yapıldığı sonucuna varılmaktadır. Hash

142 Dülger, Bilişim Sistemleri, s. 323, 324.

143 Hükümde kullanılan vekil terimi hatalıdır; zira CMK m. 2/1/d gereğince vekil; katılan, suçtan zarar gören veya malen sorumlu kişiyi ceza muhakemesinde temsil eden avukatı ifade etmektedir. CMK m. 2/1/c gereğince şüpheli veya sanığın ceza muhakemesinde savunmasını yapan avukat hakkında ise müdafi terimi kullanılmaktadır.

144 CMK m. 134/4 hükmünde 6256 sayılı Kanun ile yapılan değişiklikle şüpheliye veya vekiline yedekten kopya verilmesi, talebe bağlı olmaktan çıkarılmıştır. Değişiklik öncesinde kopya verilmesi bu kişiler tarafından "istenmesi halinde" gerçekleşmekteydi.

145 Değirmenci, s. 149, 150.

146 Değirmenci, s. 149.

147 Değirmenci, s. 149.

148 Özen/Şenocak, s. 53; Dülger, Bilişim Sistemleri, s. 323.

değerinin elde edilmesi için diskin bütününün fiziksel kopyalama yoluyla kopyalanmasına gerek yoktur; mantıksal kopyalama ya da dosya kopyalama yolunda da kopyalanan dosyaların imajı alınarak hash değeri elde edilmesi mümkündür.[149]

Elkoyma işlemi yapılması gerektiğinde, doktrinde hash değeri oluşturularak yedekleme yapılmasının elkoyma işleminden sonra değil bizatihi elkoyma işlemi esnasında yapılması gerektiği belirtilmiştir.[150] Nitekim kanunda da açıkça yedekleme işleminin elkoyma işlemi sırasında yapılacağı belirtilmiştir (CMK m. 134/3). Bu anlamda, yedekleme işleminin arama yapılan yerde teknik nedenlerle gerçekleştirilememesi ve işlem yapılmak üzere cihazların merkeze götürülmesi gerektiğinde bunlar üzerinde seri numarası bulunan özel delil torbalarına konularak götürülmeli, yedekleme işlemi şüpheli ve müdafiin önünde gerçekleştirilerek, oluşturulan yedeğin kopyası bu kişilere verilmelidir. Nitekim doktrinde, uygulamada elkoyma işleminin koluk tarafından tedbire konu araçların şüpheli ve müdafiin önünde özel delil torbalarına konulup mühürlenerek, bu esnada gerçekleştirilen tüm işlemlerin tutanağa bağlanarak gerçekleştirildiği ifade edilmiştir. Merkeze götürülen bu araçlar üzerinde inceleme yapılacağı zaman ise duruma göre şüpheli ve/veya müdafiin incelemenin yapılacağı merkeze çağırıldığı ve bu işlem için hazırlanmış özel bir yere alınarak adli bilişim uzmanını inceleme yaparken buraya yerleştirilmiş kameralar sayesinde kendilerine ayrılan yerden canlı olarak monitörlerden izlediği belirtilmiştir.[151]

Alman hukukunda tedbirin muhatabı kişinin ya da müdafiin inceleme işlemleri sırasında hazır bulunma hakkına sahip olup olmadığı StPO § 110 III hükmünde 2004 yılında Birinci Yargıda Modernleşme Kanunu kapsamında yapılan değişiklikle, hazır bulunma hakkının alternatif bir düzenlemeye yer verilmeksizin kaldırılmasıyla tartışmalı hale gelmiştir. Alman Anayasa Mahkemesi[152] bu konuda, hazır bulunma hakkı kanunen açıkça düzenlenmemekle beraber, somut olayda müdahalenin ölçülülük ilkesine uygunluğunun sağlanmasının gerek-

149 Bundesamt für Sicherheit in der Informationstechnik, Leitfaden, IT-Forensik", Bonn 2011, s. 211.
150 Özen/Özocak, s. 68.
151 Dülger, Bilişim Sistemleri, s. 326.
152 BVerfG NJW 2005, 1917 (1922); NJW 2009, 2431 (2437).

tirmesi halinde bu kişilerin inceleme esnasında hazır bulunmalarına olanak tanınması gerektiğini belirtmiştir; bilhassa veri taşıyıcılarının üçüncü kişilerle ortak kullanımının söz konusu olduğu hallerde, şüpheli olmayan bu kişilerin de gerektiğinde ilgili verilerin soruşturma açısından önemine ilişkin olarak, anlaşılır ve kontrol edilebilir açıklamalarda bulunması ve incelenecek verilerin tasnifinin ve kapsamının daraltılmasının kolaylaştırılması mümkündür.[153] Bir görüşe göre eşya üzerinde ortak zilyetliğe sahip kişilerin iradesine karşı olarak müdafiin incelemeye katılma hakkı bulunmamaktadır.[154] Diğer bir görüşe göre müdafiin incelemeye katılma hakkı hiçbir surette bulunmamaktadır; incelemeye konu verilerin müvekkiline ait olması halinde de burada StPO § 147 hükmü gereğince dosyayı inceleme hakkı söz konusu olmamaktadır, zira bu hak mahkemenin önüne gelmiş deliller ve resmi olarak muhafaza altına alınmış olan deliller hakkında söz konusu olup inceleme işlemi nedeniyle geçici olarak muhafaza altına bulunan veriler mahkeme tarafından bunlar hakkında elkoyma kararı verilene kadar bu nitelikte değildir.[155] Elkoyma kararı ise ancak inceleme işleminden sonra söz konusu olmaktadır, inceleme işlemi aramanın bir aşaması olarak değerlendirilmekte ve verilerin delil olarak değerlendirilip değerlendirilemeyeceğine, mahkemeden elkoyma kararı talep edilmesine gerek olup olmadığına ya da geçici olarak muhafaza altına alınan eşyaların iade edilmesine karar verilmek üzere yapılmaktadır.[156] Daha isabetli görünen diğer bir görüşe göre, kanun hükmünde hazır bulunma hakkının kaldırılmış olması redaksiyon hatası olarak değerlendirilmelidir; bu değişiklikle birlikte artık tedbirin muhatabının inceleme sırasında hazır bulunma hakkına sahip olmaması ve incelemenin "karanlıkta" gerçekleştirilebileceğinin kabulü mümkün değildir.[157] Kaldı ki inceleme esnasında hazır bulunma hakkı kanunun sistematiğinden de çıkarılmaktadır; bu işlem esas itibariyle aramanın bir aşaması olup, arama işleminde hazır bulunma hakkı kanunda açık-

153 BeckOK/Hegmann StPO § 110 Rn. 11.
154 BeckOK/Hegmann StPO § 110 Rn. 10.
155 MüKoStPO/Hauschild StPO § 110 Rn. 12.
156 Park § 2 Rn. 239, 242.
157 Christopher Knauer/Christian Wolf, Zivilprozessuale und strafprozessuale Änderungen durch das Erste Justizmodernisierungsgesetz-Teil 2: Änderungen der StPO, NJW 2004, 2932 (2938).

ça düzenlenmiştir (StPO § 106).[158] Müdafiin hazır bulunma hakkının ise aramaya ilişkin bu genel hükmün yanı sıra, sistematik olarak ifade ve sorgu almada hazır bulunma hakkından çıkarılabileceği belirtilmiştir.[159] Nitekim müdafiin hazır bulunması aynı zamanda şüphelinin lehine olan delillerin gözden kaçırılması tehlikesinin önlenmesine de hizmet edecektir.[160]

CMK m. 134/2 hükmünde şifrenin çözülmesi ve gerekli kopyaların alınması halinde elkonulan cihazların gecikme olmaksızın iade edileceği düzenlenmiştir. Esas itibariyle, imaj alınarak yedekleme, cihazların içerisindeki verilere erişim şifre koruması altında bulunsa dahi gerçekleştirilebilir; bu şifrelerin ise daha sonra özel programlar aracılığıyla kırılması mümkündür.[161] Ancak şifrenin kırılmasından önce cihazların içerisindeki veriler hakkında görevlilerin bilgisi olmayacaktır, bu halde sırf yedekleme işleminin gerçekleştirilmesi ardından cihazların iade edilmesi halinde içerisinde çocuk pornografisi niteliğindeki görüntüler gibi bulundurulması suç teşkil eden verilerin de şüpheliye iadesi sağlanmış olacaktır. Bu halde esas itibariyle, eşyanın, verilere ulaşılarak ve bu nitelikteki veriler silinerek şüpheliye iade edilmesi daha isabetli olacaktır. Dolayısıyla kanun koyucunun şifrenin çözülmesi ve yedekleme işleminin yapılmasını iadenin yapılabilmesi için birlikte gerçekleşmesi gereken koşullar olarak öngörmesi son derece isabetli görünmektedir. Nitekim doktrinde de özellikle suçun konusu olan çocuk pornografisi yahut mağdurun kredi kartı bilgileri gibi verilerin, cihazın içinde yer aldığı durumlarda bunun geri verilmesinin suçun işlenmesine kanun tarafından cevaz verilmesi anlamına geleceği belirtilmiştir.[162] Bu gibi durumlarda TCK m. 54 hükmü gereğince eşya müsaderesi gündeme gelebilecekse de CMK m. 134 hükmünde özel bir düzenleme yapılması gerektiği haklı olarak belirtilmiştir.[163] Zira TCK m. 54 hükmü gereğince, suçun işlenmesinde kullanılan eşyanın müsadere edilmesi mümkün olmakla birlikte, TCK m. 134 hükmünde düzenlenen tedbirinin konusunu oluşturan cihazların iyiniyetli üçün-

158 Knauer/Wolf, s. 2938; Kristina Peters, Anwesenheitsrecht bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, NZWiST 2017, 465(470).
159 Knauer/Wolf, s. 2938; Park § 2 Rn. 259.
160 Park § 2 Rn. 259.
161 Değirmenci, s. 149.
162 Özen/Özocak, s. 70.
163 Özen/Özocak, s. 70.

cü kişilere[164] ait olması ve bu nedenle müsadere edilememesi mümkündür. Öte yandan eşyanın şüpheliye ait olması halinde de cihazın müsadere edilmesi yerine, bu tür veriler silinerek iade edilmesi daha orantılı olacaktır. Bu nedenle doktrinde ifade edilen CMK m. 134 hükmünde özel bir düzenlemeye yer verilmesi görüşü son derece isabetli görünmektedir.

VI. SONUÇ

Ceza Muhakemesi Kanunu m. 134 hükmünde düzenlenmiş olan koruma tedbirleri, nitelik itibariyle arama ve elkoyma tedbirlerinin özel bir görünümünü teşkil etmektedir. Bu tedbirlerin uygulanma alanı bilgisayar, bilgisayar kütükleri ve bilgisayar programları olarak belirlenmiş olmakla birlikte, Türk Ceza Kanunu'nda kullanılan terminolojiyle uyum sağlanması ve bunları kapsayıcı bir üst kavram niteliğinde olması nedeniyle bilişim sistemleri kavramının tercih edilmesi daha isabetli görünmektedir.

Kanun hükmünde açıkça tedbirlerin soruşturma aşamasında ve şüpheli hakkında uygulanabileceği düzenlenmiş olup, kovuşturma evresinde uygulanma imkânı bulunmamaktadır. Tedbirin uygulanabilmesi için bilişim sistemlerinin şüpheli tarafından kullanılması gerekli ve yeterlidir; ayrıca bunların şüpheliye ait olmasına gerek yoktur.

Şüphelinin kullanmadığı fakat suçun delillerinin yer aldığı, üçüncü kişilerin ya da mağdurun kullandığı cihazlarda arama yapılabilmesinin, bu kişilerin rızalarının bulunması halinde dahi yasal dayanağı bulunmamaktadır.

CMK m. 134 hükmünde düzenlenen tedbirlere başvurulabilmesi somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânın bulunmaması halinde mümkündür. Kuvvetli şüphe sebeplerinin aranması, hükümde 2014 yılında 6526 sayılı Kanun'la yapılan değişikle gerçekleşmiştir. Buna göre; suç delillerinin şüphelinin kullandığı bilişim sistemlerinde bulunduğu hususunda soruşturma mercilerinde olgulara dayanan, sübjektif varsayım ve tahmin niteliğinde olmayan şüphe derecesine ulaşılmış olmalıdır. Başka surette delil etme imkânın bulunmamasından anlaşılması ge-

164 İyiniyetli üçüncü kişi hakkında detaylı açıklamalar için bkz. Aysun Dalkılıç, Türk Ceza Hukukunda Müsaade, Ankara 2013, s. 72-75.

reken diğer bütün koruma tedbirlerinin denenmiş fakat sonuç alınamamış olması değil; belirli delillere ancak bu tedbirlere başvurulması yoluyla ulaşılabilecek olmasıdır. 6526 sayılı Kanun'la yapılan değişiklikle ayrıca elkoyma işlemi sırasında alınacak olan yedekten bir kopya çıkarılarak şüpheliye ya da müdafiine verilmesi isteğe bağlı olmaktan çıkarılarak zorunlu hale getirilmiştir.

Kanunda 2018 yılında 7145 sayılı Kanun'la yapılan değişiklikle ilk olarak 668 sayılı Kanun Hükmünde Kararname ile getirilen gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararı ile bu tedbirlere başvurulması olağanüstü hâl süresi ile sınırlı olmaktan çıkarılarak kalıcı hale getirilmiştir.

CMK m. 134 hükmünde aramaya konu cihazlara elkonulması işlemi istisnai olarak uygulanabilecek bir işlem olarak öngörülmüş; ancak sistemlere şifrenin çözülememesinden dolayı girilememesi, gizlenmiş bilgilere ulaşılamaması veya işlemin uzun sürecek olması şartlarından birinin gerçekleşmiş olmasına bağlı kılınmıştır. İşlemin uzun sürecek olması nedeniyle elkoyma tedbirine başvurulabilmesi olanağı, uygulamadan kaynaklanan ihtiyaçlar doğrultusunda 7145 sayılı Kanun'un 16. maddesiyle yapılan değişiklikle eklenmiştir.

Tedbirlerin uygulanması kapsamında elde edilen dijital verilerin güvenilirliğini korumak amacıyla verilerin kopyalanması ve yedeklenmesi sırasında imaj alınarak hash değeri oluşturulmalı, bu değer şüpheli veya müdafii ile paylaşılmalıdır.

Kaynakça

Kitaplar

Aydın Devrim, Ceza Muhakemesinde Deliller, Ankara 2014.

Beulke Werner, Strafprozessrecht, München u.A. 2010.

Beulke Werner/Swoboda Sabine, Strafprozessrecht, Heidelberg 2018.

Bundesamt für Sicherheit in der Informationstechnik, Leitfaden, IT-Forensik", Bonn 2011.

Centel Nur/Zafer Hamide, Ceza Muhakemesi Hukuku, İstanbul 2015.

Dalkılıç Aysun, Türk Ceza Hukukunda Müsaade, Ankara 2013.

Dölling Dieter/Duttge Gunnar/Rössner Dieter (Hrsg.), Gesamtes Strafrecht Handkommentar, Baden-Baden 2017.

Dülger Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2020. (Bilişim Suçları)

Graf Jürgen-Peter (Hrsg.), BeckOK StPO mit RiStBV und MiStra, München 2020. (BeckOK StPO)

Hannich Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, München 2019. (KK-StPO)

Joecks Wolfgang/Jäger Markus/Randt Karsten (Hrsg.), Steuerstrafrecht, München 2015.

Kindhäuser Urs, Strafprozessrecht, Baden-Baden 2016.

Knauer Christopher/Kudlich Hans/ Schneider Hartmut (Hrsg.), Münchener Kommentar zur StPO, Band I, München 2014. (MüKoStPO)

Kunter Nurullah/Yenisey Feridun/Nuhoğlu Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, İstanbul 2010.

Öztürk Bahri/Eker Kazancı Behiye/Soyer Güleç Sesim, Ceza Muhakemesi Hukukunda Koruma Tedbirleri, Ankara 2019.

Park Tido, Durchsuchung und Beschlagnahme, München 2018.

Roxin Claus/Schünemann Bernd, Strafverfahrensrecht, München 2017.

Savić Laura Iva, Die digitale Dimension des Stafprozessrechts, Berlin 2020.

Tanrıkulu Cengiz, Ceza Muhakemesi Hukukunda Bilişim Sistemerinde Arama ve Elkoyma, Ankara 2014.

Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat, Uluslararası Ceza Hukuku, Ankara 2021.

Toroslu Nevzat/Feyzioğlu Metin, Ceza Muhakemesi Hukuku, Ankara 2015.

Türk Dil Kurumu, Türkçe Sözlük, Ankara 2005.

Ünver Yener/Hakeri Hakan, Ceza Muhakemesi Hukuku, Ankara 2014.

Makaleler

Aktaş Batuhan, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme", *YÜHFD*, C. 14, S. 2, Y. 2017, ss. 211-239.

Apiş Özge, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Tedbiri", *Yasama Dergisi*/37, Y. 2018, ss. 49-86.

Baştürk İhsan, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", *Fasikül Dergisi*, S. 9, Y. 2010, ss. 23-32.

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. 146, Y. 2018, ss. 146-155.

Dereboylular Özde, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği", *CHD*, S. 39, Y. 2019, ss. 161-202.

Diz Irina, Anwendbarkeit und Reichweite der Befugnisse gem. §§ 110 III, 100j StPO im hinblick auf "Cloud Computing" und "Cloud Storage", Strafrecht und moderne Technologien-Ceza Hukuku ve Modern Teknolojiler (Hrsg. Gunnar Duttge/Yener Ünver), Ankara 2018, ss. 183-195.

Duran Gürkan Yaşar, "Ceza Muhakemesi Kanunu'nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", *BÜHFD*, C. 14, S. 173-174, Y. 2019, ss. 173-241.

Dülger Murat Volkan, Bilişim Sistemleri Üzerinde Arama, Kopyalama ve Elkoyma Tedbiri, Ceza Muhakemesi Hukukunda Güncel Konular (Edt. Nur Centel), İstanbul 2015, ss. 315-327. (Bilişim Sistemleri)

Epözdemir Rezan, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri", *Terazi Hukuk Dergisi*, C. 13, S. 142, Y. 2018, ss. 88-98.

Erdoğan Yavuz, Türk Hukuk Sisteminde Bilgisayar Araması ve Bulunan Delillere Elkonulması, Bilgi Sistemleri ve Bilişim Yönetimi (Edt. Fahrettin Özdemirci/Zeynep Akdoğan), Ankara 2017, ss. 173-190.

Knauer Christopher/Wolf Christian, Zivilprozessuale und strafprozessuale Änderungen durch das Erste Justizmodernisierungsgesetz-Teil 2: Änderungen der StPO, NJW 2004, ss. 2932-2938.

McGraw Swaminatha Tara., The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defences, Yale Journal of Law and Technology, C. 7 S. 1, Y. 2005, ss. 51-86.

Özen Muharrem/Özocak Gürkan, Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134), ABD 2015/1, ss. 43-76.

Peters Kristina, Anwesenheitsrecht bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, NZWiST 2017, ss. 465-473.

Ünver Yener, Durchsuchung des Computers im Rahmen des Art. 134 tStPO, Strafrecht und moderne Technologien-Ceza Hukuku ve Modern Teknolojiler (Hrsg. Gunnar Duttge/Yener Ünver), Ankara 2018, ss. 196-226.

Yıldız Ali Kemal, "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu", *CHD* 2006/2, ss. 253-264.

Warken Claudia, Elektronische Beweismittel im Strafprozessrecht-eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, NZWiST 2017, ss. 329-337.

Wicker Magda, Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, ss. 765-769.

Yaşar Yusuf/Dursun İsmail, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", *MÜHF-HAD*, C. 19, S. 3, Y. 2013, ss. 3-34.

Zerbes Ingeborg/El-Ghazi Mohammad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, ss. 425-433.

İnternet Kaynakları

https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf

Mahkeme Kararları

www.beck-online.beck.de

www.kazanci.com.tr