Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri

Özge Apiş[*]

Özet

Teknolojinin gelişmesiyle birlikte, bilgisayar suçları olarak da ifade edilen bilişim suçları, ceza hukukunu oldukça meşgul eden bir alan haline gelmiştir. Zira bilişim sistemine girmek veya orada kalmak başlı başına kanun koyucunun yasakladığı bir fiil olarak ortaya çıkmaktayken, bazı suç tiplerinin de bilişim sistemlerinin kullanılması suretiyle işlenmesi yine kanun koyucu tarafından cezalandırılabilir nitelikte fiiller olarak öngörülmüştür.

Çalışmada öncelikle 5237 sayılı Türk Ceza Kanunu'nun (TCK) 243. maddesinde düzenlenmiş olan "*Bilişim Sistemine Girme*" suçu karşılaştırmalı hukuk kapsamında ele alınacaktır. Bu kapsamda bilişim sistemi kavramına açıklık getirilmeye çalışılacak ve TCK bağlamında suçun oluşabilmesi için suçun konusunun arz ettiği özellikler ele alınacaktır.

Çalışmada bir diğer amaç, 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi kapsamında düzenlenen "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*" koruma tedbiri ile TCK'nun 243. maddesinde düzenlenmiş olan "*Bilişim Sistemine Girme*" suçu arasındaki ilişkiye Yargıtay kararları ışığında değinmektir.

***Anahtar Kelimeler*:** Bilgisayar, bilişim sistemi, bilişim suçları, dijital delil.

Abstract

Along with the development of technology, computer crimes, also referred to as data processing system crimes, have become a field of criminal law. Accessing or remaining within all or part of data processing system has been regulated as a crime by the legislator similarly to the crimes that are committed by means of the use of the data processing systems.

---

[*] Dr. Öğr.Üyesi, Niğde Ömer Halisdemir Üniversitesi, İİBF, Kamu Yönetimi Bölümü.
Makalenin gönderilme tarihi: 05.02.2018; *Kabul tarihi:* 24.04.2018.

In this article, the crime of "Access to Data Processing System" which is legislated in article 243 of Law No. 5237 is discussed within the scope of comparative law. Therefore, firstly it's aimed to enlighten the subject of the crime, especially the terms; "computer", "computer crimes", "data", "cybercrimes", "data processing system" etc. The other topic that is discussed in this study is, the protection measure called "searching computers, computer programs and computer files" regulated in article 134 of Law No. 5271 in connection with the crime of "Access to Data Processing System". Also Supreme Court's decisions about this crime are analyzed.

***Key words*:** Computer, data processing system, data processing system crimes, digital/electronic proof.

Giriş

Verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerine sahip olan ve bu fonksiyonları çok yönlü olarak otomatik işlemlere tabi tutma olanağı veren bir sistem olarak tanımlanan bilişim sistemi, teknoloji alanında yaşanan gelişmeler neticesinde modern hayatın vazgeçilmez bir parçası haline gelmiştir.

Bilişim sistemlerinin, günlük hayatı kolaylaştırması şeklindeki yadsınamaz faydasının yanı sıra bu sistemlerin suçta araç olarak kullanılması, ceza hukukunun müdahalesini gerektiren bir sorun olarak ortaya çıkmıştır. İşte bu nedenle, gerek ulusal mevzuatta ve gerek ise uluslararası hukuk düzenlemelerinde bilişim sistemlerinin suçun konusu olması ya da suçun işlenmesinde araç olarak kullanılması suç olarak yaptırım altına alınmıştır. Bu doğrultuda kanun koyucu, 5237 sayılı TCK'da bilişim alanında suçlara ayrıca yer vermiştir.

Bilişim suçları, "*sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar*", "*bilişim sisteminin kullanılması zorunlu olmamakla birlikte, sistemin suçta kullanılmasının nitelikli hal olarak düzenlendiği suçlar*" ve "*kanunda bu sistemin kullanılması zorunlu olmamakla birlikte, söz konusu sistemin suçta vasıta olarak kullanıldığı suçlar*" şeklinde ayrımlara tabi tutulmuştur.

Bilişim sisteminin kullanılması zorunlu olmamakla birlikte, sistemin kullanılmasının nitelikli hal olarak düzenlendiği suçlar (Hırsızlık (TCK m. 142/2-e) ve Dolandırıcılık (TCK m. 158/1-f) gibi), ve yine sistemin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasıta olabileceği suçlar, (Haberleşmenin Gizliliğini İhlal (TCK m. 132), Haberleşmenin Engellenmesi (m. 124), Eğitim ve Öğretimin Engellenmesi (TCK m. 112), Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetlerinin Engellenmesi (TCK m. 113), Hakaret ve Sövme (TCK m. 125),

Müstehcenlik (TCK m. 226), Kumar Oynanması İçin Yer ve İmkân Sağlanması (TCK m. 228), Suç İşlemeye Tahrik (TCK m. 214), Cinsel Taciz (TCK m. 105) bilişim sistemlerinin suçta araç olarak kullanıldığı suçlardır.[1]

Bu çalışma içerisinde değinilecek olan 5237 sayılı TCK'nun II. Kitabı'nın "*Topluma Karşı Suçlar*" başlıklı III. Kısmı'nın "*Bilişim Alanında Suçlar*" başlıklı 10. bölümünün 243. maddesinde dört fıkra halinde düzenlenmiş olan "*Bilişim Sistemine Girme Suçu*"nu ise, sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları) olarak ifade etmek mümkündür.

İleride ayrıntılı bir şekilde değineceğimiz üzere, bilgisayarlar bilişim sistemi özelliği göstermekle birlikte, bilgisayar kavramı bilişim sistemi kavramına göre daha dar bir kapsamı ifade etmektedir. Bu anlamda bilgisayar, bilişim sistemine girme suçunun konusu olabileceği gibi, koşulları oluşmuşsa bilgisayarda delil aranması, gerekli hallerde kopyalama yahut elkoyma işlemlerinin uygulanması da hukuka uygunluk sebebi olarak ortaya çıkacaktır. Zira bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma, ceza muhakemesinde bir koruma tedbiri olarak ortaya çıkmaktadır.

Bu nedenle çalışmamızda, bilişim alanındaki birtakım teknik kavramların izahının yapılması gerekliliği, sadece 5237 sayılı TCK bakımından değil, 5271 sayılı CMK bakımından da önem arz etmektedir. Diğer yandan, 5271 sayılı CMK'nun 134. maddesinde düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinin, sadece bilgisayarlar bakımından mı uygulanacağı yoksa "*bilgisayar*" ibaresinin "*bilişim sistemi*" olarak mı yorumlanması gerektiği sorusu, söz konusu teknik kavramların açıklanmasına bağlı olarak yanıt bulacaktır.

Bu nedenle çalışmamızın ilk bölümünde, 5237 sayılı TCK'nun 243. maddesinde düzenlenmiş olan "*Bilişim Sistemine Girme*" suçu, ceza hukuku genel teorisi kapsamında ele alınacak, tartışmalı hususlar hakkında görüşlerimiz ifade edilecektir.

İkinci bölümde ise, "*dijital/elektronik delil*" kavramına değinilerek, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinin uygulanma şartları ayrı ayrı ve tartışmalı hususlar hakkında görüşlerimize yer verilmek suretiyle ortaya konulmaya çalışılacaktır.

---

[1] Mahmutoğlu, Fatih Selami, Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, İÜHFM, C. 71, S. 1, 2013, s. 855, 856.

I. Bilişim Sistemine Girme Suçu (TCK m. 243)

I.1. Genel Açıklamalar ve Karşılaştırmalı Hukuk

765 sayılı Türk Ceza Kanunu'na, 06.06.1991 tarihli ve 3756 sayılı Kanun ile "*Bilişim Alanında Suçlar*" adıyla 525/a, 525/b, 525/c ve 525/d maddelerinin eklenmesiyle yasal boyut kazanan bilişim suçları,[2] 5237 sayılı TCK'nun 243 vd. maddelerinde düzenlenmiştir.

Bilişim alanında suçlar bölümünde, hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu (m. 243), bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m. 244/1–2), bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m. 244/4), banka veya kredi kartlarının kötüye kullanılması suçu (m. 245), yasak cihaz veya programlar (245/A) yer almaktadır.

5237 sayılı TCK'nun 243. maddesine göre, "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*

Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."

24/3/2016 Tarihli ve 6698 sayılı Kanun'un 30. maddesiyle "*bu fıkrada yer alan 've' ibaresi 'veya' şeklinde değiştirilmiştir*" şeklinde yapılan düzenlemeyle, 243. madde bakımından sisteme erişim yeterli görülmüş, suçun oluşabilmesi için sistemde bir süre kalmaya devam etme de aranmamıştır. Değişiklik öncesinde ise, suçun oluşabilmesi için hem sisteme girilmesi ve hem de orada kalmaya devam edilmesinin aranması doktrinde eleştirilmiştir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin (AKSSS) 2. maddesinde de bilişim sistemine hukuka aykırı erişim, suçun oluşması için yeterli sayılmış, failin ayrıca burada kalmaya devam etmesi aranmamıştır.[3]

Mukayeseli hukukta da genel eğilim bu yöndedir.

Nitekim Alman Ceza Kanunu'nun (ACK) "*Özel Hükümler*" başlıklı II. Kitabının "*Özel Hayat ve Özel Hayat Alanının İhlali*" adlı 15. bölümün 202a maddesinde "*Veri Casusluğu*" suçu düzenlenmiştir.

---

2 http://www.resmigazete.gov.tr/arsiv/20901.pdf, (Erişim Tarihi: 15.03.2018).

3 "*Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı gerekli önlemleri almalıdır. Taraf devlet bu suçun oluşması için erişimin güvenlik önlemleri ihlal edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlayabilir*."

Söz konusu maddeye göre, "*Her kim, yetkisi olmaksızın, kendisinin bilgisine sunulmuş olmayan ve hak sahibi olmayanların girişine karşı özel olarak korunmuş bulunan verileri bu korumayı aşarak kendisine veya bir başkasına giriş yapma olanağı sağlarsa, üç yıla kadar hapis cezası veya adli para cezasıyla cezalandırılır.*

Birinci fıkrada belirtilen veriden, sadece elektronik, manyetik veya sair doğrudan doğruya algılanamayacak bir şekilde kaydedilmiş veya aktarılmış olan veriler anlaşılır. "[4]

Fransız Ceza Kanunu'nun (FCK) "*Malvarlığına Karşı Suçlar*" başlıklı III. Kitabının "*Sair Malvarlığına Karşı Suçlar*" adlı II. Bölümünün "*Bilişim Sistemine Yetkisiz Erişim*" başlıklı III. Kısmında ve 323. maddesinde bilişim sistemlerine ilişkin düzenlemeler getirmiştir. Bunlardan madde 323-1, TCK'nun 243. maddesinde yer alan "*Bilişim Sistemine Girme*" suçuna benzer nitelikte düzenlemeler içermektedir. Zira adı geçen maddenin 1. fıkrasında Fransız Kanun Koyucu, bilişim sisteminin tamamı veya bir kısmına girilmesi (erişim) yahut orada kalınmasına iki yıl hapis ve 60,000 Euro para cezası öngörmüştür. Bu fiil nedeniyle sistemdeki verilerin silinmesi yahut değiştirilmesine veya sistemin çalışmasında tahrifata sebebiyet verilmesi hali ise 2. fıkrada üç yıl hapis ve 100,000 Euro para cezasıyla cezalandırılmıştır. Bu suçların, kişisel verilerin işlenmesine yönelik bir bilişim sistemine karşı işlenmesi halinde ise ceza, 5 yıla kadar hapis ve 150,000 Euro'ya kadar para cezası olacaktır.[5]

İsviçre Ceza Kanunu (İCK) da konuya ilişkin düzenlemeler içermektedir. Nitekim Kanun'un "*Özel Hükümler*" isimli II. Kitabının "*Malvarlığına Karşı Suçlar*" başlıklı II. Bölümünde ve 143 bis136 numaralı maddesinde kanun koyucu, "*Bilişim Sistemine Yetkisiz Erişim*" suçunu düzenlemiştir. Söz konusu hükmün 1. fıkrasında, veri iletim donatısı yoluyla bilişim sistemine yetkisiz olarak erişim sağlayan kimselerin, şikâyet üzerine üç yıla kadar hapis yahut para cezasıyla cezalandırılmaları öngörülmüştür. Ancak bu madde kapsamında kanun koyucu suçun oluşması bakımından, bilişim sistemine girmeyi engelleyen özel önlemlerin alınmış olmasını aramaktadır.[6]

---

4 Yenisey, Feridun, Plagemann Gottfried, Alman Ceza Kanunu, Strafgesetzbuch (StGB), İstanbul, Mayıs, 2015, s. 311.

5 https://www.legifrance.gouv.fr/content/download/1957/13715/.../Code_33.pdf, (Erişim Tarihi: 14.02.2018), Kanunun ingilizce çevirisi Cambridge Üniversitesi hukuk profesörü John Rason SPENCER'ın katkılarıyla gerçekleştirilmiştir.

Kanunun orijinal ve 24.07.2015 tarih ve 2015-912 sayılı Kanun'un 4. maddesiyle yapılan değişiklikleri de içeren metni için ayrıca *bkz*., https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719, (Erişim Tarihi: 14.02.2018).

6 http://www.legislationline.org/documents/section/criminal-codes, (Erişim Tarihi: 14.02.2018).

5237 sayılı Kanun'da düzenlenen bilişim sistemine girme suçuna benzer bir suç, Hollanda Ceza Kanunu'nun (HCK) II. Kitabı'nın "*Kamu Düzenine Karşı Suçlar*" başlıklı IV. Bölümü'nün 138ab maddesinde düzenlenmiştir. Söz konusu düzenlemeye göre, bir kimsenin bilgisayar özellikleri gösteren bir aygıt yahut sistemin bütününe veya bir kısmına kasten ve hukuka aykırı olarak girmesi suç olarak düzenlenmiş ve karşılığında bir yıla kadar hapis veya para cezası öngörülmüştür. Söz konusu sistem ya da aygıta, güvenlik önlemlerinin ihlal edilmesi, teknik müdahalede bulunulması, aldatıcı sinyaller gönderilmesi veya sahte (aldatıcı) şifreler kullanılması yahut sahte kimlik kullanılmak suretiyle girilmesi halinde de bu suç oluşacaktır. Maddenin 2. fıkrası, sistem ya da aygıttaki verilerin kopyalanması, kaydedilmesi, depolanması, transfer edilmesi gibi bazı fiilleri, suçun cezasını artıran nitelikli hali olarak öngörmüştür.[7]

İspanyol Ceza Kanunu'nda ise benzer nitelikte bir suç, "*Özel Hayata, Kişi Haysiyeti ve Konut Dokunulmazlığına Karşı Suçlar*" başlıklı 10. Bölümde ve "*Gizliliğin İhlali*" adlı I. Kısmın 197. maddesinde ve 3. fıkrasında düzenlenmiştir. Nitekim söz konusu düzenlemeyle İspanyol Kanun Koyucusu, bir bilgisayar sisteminin bütünü yahut bir kısmındaki veri ya da programlara yetkisiz erişimini ve hak sahibinin rızasına aykırı olarak bu sistemde kalmaya devam edenin altı aydan iki yıla kadar cezalandırılabileceğini öngörmüştür.[8]

Kanada Ceza Kanunu'nun (KCK) 342.1 maddesi de benzer düzenlemelere yer vermiştir. Adı geçen maddede "*bilgisayarın yetkisiz kullanımı*" başlığı altında bilişim sözcüğüne karşılık gelen "*data-processing*" ibaresi değil, "*bilgisayar*" (computer) sözcüğü tercih edilmiştir. Diğer yandan 342.1 maddesinin "*Tanımlar*" başlıklı 2. fıkrasında, bilgisayar verisi, bilgisayar şifresi, bilgisayar programı, bilgisayar servisi vs. gibi ibarelerden ne anlaşılması gerektiği açıklanmaya çalışılmıştır. Kanunun 342.1 maddesinde suç teşkil eden fiiller, 4 bent halinde sayılmıştır. İlk bentte, bir bilgisayar servisinin tamamen ya da kısmen ele geçirilmesi, ikinci bentte, bir bilgisayar sisteminin çalışmasına elektromanyetik, akustik, mekanik yahut sair bir yöntemle doğrudan ya da dolaylı olarak müdahale edilmesi veya müdahale edilmesine neden olunması suç olarak düzenlenmişken, üçüncü bentte, birinci ve ikinci bentte öngörülen

---

Ücretsiz çevrimiçi yasama veri tabanı ve mevzuat kılavuzu olan Legislationline, AGİT'e katılan Devletlerin mevzuatlarını, uluslararası insan hakları standartlarıyla uyumlu hale getirmelerinde yardımcı olmak amacıyla 2002 yılında kurulmuştur. http://www.osce.org/odihr/legislationline, (Erişim Tarihi: 14.02.2018).

7 http://www.legislationline.org/documents/section/criminal-codes, (Erişim Tarihi: 15.02.2018).

8 http://www.legislationline.org/documents/section/criminal-codes, (Erişim Tarihi: 01.03.2018).

suçları yahut bilgisayar verisi ya da bilgisayar sistemi ile bağlantılı olarak 430. maddedeki suçu işlemek maksadıyla, doğrudan ya da dolaylı olarak bir bilgisayar sistemini kullanmak veyahut kullanılmasına neden olmak, dördüncü bentte ise, a, b ve c bentlerindeki suçların işlenmesine olanak sağlayacak nitelikteki bir bilgisayar şifresini kullanmak, bulundurmak, yasa dışı ticaretini yapmak yahut bu şifreye başkasının erişmesini sağlamak cezalandırılmıştır.[9]

Bunun dışında KCK'da suçun konusunun bilgisayar olduğu yahut bilgisayar yoluyla işlenen diğer bazı suçlar da öngörülmüştür (m. 342.2, 430 (1.1), 487.0194 (1)).

I.2. Suçun Unsurlarının Arz Ettiği Özellikler

I.2.1. Suçun Konusu Olarak Bilişim Sistemi ve Anlamı

5237 sayılı TCK'nun 243. maddesinin 1. fıkrasında, "*Bir bilişim sisteminin bütününe veya bir kısmına*" girilmesi veya orada kalmaya devam edilmesi suç teşkil eden fiil olarak öngörülmüştür. Bu nedenle suçun konusu, "*bilişim sistemi*" olarak ortaya çıkmaktadır. Diğer yandan adı geçen maddenin 2. fıkrasında "*bedeli karşılığı yararlanılabilen bilişim sistemleri*" ve 3. fıkrasında ise, "*bilişim sisteminin içerdiği veriler*" suçun konusu bakımından önem arz etmektedir.

Belirtmek gerekir ki, bir sistemin bilişim sistemi olup olmadığı hususu teknik nitelikte bir husustur ve somut olayın özelliklerine göre bu konuda uzman olan kişiler tarafından çözülmesi gereken bir meseledir. Ancak konumuzun arz ettiği özellikler gereğince bizim de bilişim sistemi, bilgisayar, veri gibi bir takım kavramlara değinmek ve doktrinde ne şekilde anlaşıldığını açıklamamız gerekmektedir. Bu kapsamda ilk olarak değinmek istediğimiz kavram, "*bilgisayar*" olmakla birlikte, "*bilişim*", "*bilişim sistemi*" ve "*bilişim suçu*" kavramlarının da açıklanması gerektiği kanaatindeyiz.

Bilgisayar sözlükte, bilgileri işleme tabi tutan, depolayan ve görüntüleyen aygıt olarak tanımlanmıştır. Bir zamanlar hesaplamalar yapan cihaz olarak algılanan bilgisayarlar, günümüzde evrensel olarak otomatik elektronik makinelerin genel adı olarak kullanılmaktadır.[10]

Diğer yandan belirtmek gerekir ki, bilgisayar gerek fonksiyonu ve/veya gerek ise donanımı ele alınarak çeşitli açılardan tanımlanmakta ancak bu tanımlar dahi teknolojinin hızlı gelişiminin karşısında bilgisayarın tanımlanmasında yetersiz kalmaktadır. Zira günümüzde, klasik bilgisayarlar donanımlarına (monitör, kasa, klavye, fare gibi) sahip olmamakla bereber bilgisayarların

---

9 http://www.legislationline.org/documents/section/criminal-codes, (Erişim Tarihi: 15.02.2018).

10 www.britannica.com/computer, (E.T. 15.02.2018).

bir kısım özelliklerini barındıran ya da bilgisayarların yaptığı bir kısım işleri yapan makineler de (laptop, tablet vs.) ortaya çıkmıştır.[11]

Son tahlilde, aslında bilgisayarları benzer makinelerden ayıran temel özelliğin bilgisayarların, hesap makineleri gibi salt bir konuya özgülenmemiş genel amaçlı bir makine olmasından kaynaklandığı ifade edilmektedir. Böylece bilgisayarlar bakımından, işletim yahut uygulama yazılımlarının silinip yerine yenisinin yüklenebilmesi yahut varolan yazılımların yanına yenisinin eklenebilmesinin mümkün olduğunu ifade etmek gerekmektedir.[12]

5237 sayılı TCK'da "*bilgisayar*" ibaresinden değil, "*bilişim sistemi*"nden bahsedilmektedir. Diğer yandan 5237 sayılı TCK'nunda düzenlenen bilişim sistemine girme suçunun tam karşılığına 765 sayılı TCK'da yer verilmemiş, mülga Kanun'da adı geçen suç bakımından "*bilgileri otomatik işleme tabi tutan sistem*"den bahsedilmiştir.[13]

Bilişim sözlükte, "*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" olarak tanımlanmaktadır.[14]

Avrupa Konseyi Siber Suç Sözleşmesi'nde "*bilişim*" yahut "*bilişim suçu*" kavramlarına yer verilmemiş, onun yerine "*siber suç*" , "*bilgisayar sistemi*", "*bilgisayar verisi*" kavramları tercih edilmiştir.

Sözleşme'nin 1/a maddesine göre bilgisayar sistemi, "*herhangi bir cihaz ve birbiriyle bağlantılı bir grup veya cihazlar yoluyla bir veya birden fazla program tarafından devam ettirilen verinin otomatik olarak işlenmesi, bu işlemin yerine getirilmesi*" olarak tanımlanmıştır.

---

[11] Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 2013, s. 51, 52, 53. Bilgisayarın donanım (hardware) ve yazılım (software) unsurlarına ilişkin daha ayrıntılı açıklamalar için *bkz*., Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 54 vd., Taşkın, Şaban Cankat, Bilişim Suçları, Beta Basım A.Ş., İstanbul, 2008, s. 5 vd., Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, 2013, s. 38-40.

[12] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 57 vd.

[13] 765 Sayılı TCK m. 525/a) (Ek madde: 06/06/1991 - 3756/21 md.).

"*Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir."

14 www.tdk.gov.tr.

Bilişim sistemi ayrıca 243. maddenin gerekçesinde de açıklanmıştır. Buna göre bilişim sistemi, "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tutma olanağı veren manyetik sistemlerdir*".

Mülga 765 sayılı Kanundaki düzenlemelerde tercih edilen otomatik işleme tabi tutma kavramına, TCK'nın 243. maddenin gerekçesinde yer verilmiştir. 765 sayılı Kanun'un gerekçesinde ise "*bilgileri otomatik işleme tâbi tutan*" kavramının bilgisayarları karşıladığı ifade edilmiştir. 765 sayılı TCK döneminde bilgisayarı tanımlamak için düzenlemelerde yer verilen bilgileri otomatik işleme tabi tutan sistem ifadesi, kavramın bilgisayarları karşılamakta tamamen yanlış bir ifade olması ve bilgisayarları anlatmak bakımından yetersiz kalması nedeniyle eleştirilmiştir.[15] Çünkü hesap makineleri gibi birçok araçta bilgileri depo etme, bunları işleyebilme ve anlamlı sonuçlar üretme özelliği görülebilmektedir. Ancak bunları bilgisayar olarak nitelendirebilmek mümkün olmadığı gibi, bilişim suçlarının işlenmesine imkân veren başka bir sistem özelliğine sahip oldukları da söylenemez. Zira bunlar hafızalarında bulunan sabit programlarla belirli bir amaç doğrultusunda kullanılabilmeye uygun, bilgileri aktarma özelliğine sahip bulunmayan cihazlardır. Ayrıca bilgisayarların yalnızca manyetik özelliği bulunmamakta, elektronik, optik gibi nitelikleri de söz konusudur.[16] Diğer yandan bilgisayarları, programlama yeteneğine sahip elektronik araç olarak da tanımlamak onları elektronik çamaşır makineleri ve TVlerden ayırmaya yeterli değildir.[17]

Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmeliğin 3/1-b maddesine bilişim sistemi, "*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi*" ifade etmektedir. Görüldüğü gibi burada da bilişim sistemi, bilgisayar ve ona bağlantılı sistemleri ifade etmek için kullanılmıştır.

Kanaatimizce ***bilişim sistemi*** kavramı, bilgisayarı da içine alan daha geniş bir alanı ifade etmektedir.[18] Zira bilişim sistemi, verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerine sahip olan ve bu fonksiyonları çok yönlü olarak otomatik işlemlere tabi tutma olanağı veren bir sistemdir. Bu yönüyle bilişim sistemi, veri-işleme

---

15 Akbulut, s. 25-26.

16 Akbulut, s. 25-26.

17 Yazıcıoğlu, Yılmaz, Bilgisayar Suçları, Alfa Basım Yayım, Dağıtım, 1997, s. 28.

18 Akbulut, Berrin, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C: 24, S: 2, Y: 2016, s. 24, Özbek, Veli Özer, Doğan, Koray, Bacaksız, Pınar, Tepe, İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Eylül, 2017, s. 942.

Karagülmez, s. 37.

ve veri-iletme özelliğine sahiptir. Oysa bilgisayar, verileri toplama, saklama, işleme ve yeniden değerlendirme faaliyeti nedeniyle verileri işleme özelliğine sahiptir.[19]

Bilişim, hem verilerin işlenmesini (veri işlemi) hem de bilgi işlemin sonucunun aktarılmasını (veri iletişimi) ifade eden bir kavramdır. Verilerin işlenmesi ve aktarılmasında kullanılan bileşenlerin, teknolojilerin bütününe ise bilişim sistemi adı verilmektedir.[20] Böylece, bilgisayarın teknik tanımına uymamakla beraber, onun yerine getirdiği işlevin bazılarını yerine getiren (android cep telefonları, cep bilgisayarları, kişi/araçları elektronik olarak tanıyan güvenlik araçları, göz retinası yahut parmak izi tespit ederek aktif hale gelen sistemeler vs.) yahut bilgisayarın çözemediği türden problemleri çözebilen bazı sistemlerin bilişim suçlarının konusu olması mümkündür.[21] Diğer yandan, dekoder, barkod okuyucu, binalara girişi sağlayan kartlar, telefon kartları, çamaşır makinası vs. gibi bilgiyi işleme ve iletme yeteneğine sahip olup da bunu genel amaçlı olarak değil de tek yönlü yapabilen cihazlar bu suç kapsamında bilişim sistemi olarak kabul edilemezler.[22] Bu anlamda bilişim suçlarını da bilgisayar suçları olarak dar kapsamda ele almamak gerekir.

Bilişim suçlarını tanımlamak için "*siber suç*", "*elektronik suç*", "*dijital suç*", "*yüksek teknoloji suçları*", "*bilgisayar suçu*" gibi kavramlar da kullanılmaktadır. Bu ibarelerin, sözlük anlamıyla alınırsa, içerisinde bir veya birden fazla eksikliği barındırdığı ifade edilmektedir. Zira bu görüşe göre, bilgisayara odaklanan terimler "*ağları*" içermedikleri gibi, siber suçlar veya sanal suçlar gibi diğerleri ise yalnızca internete odaklanmış olarak görülürler.[23] Dijital, elektronik veya ileri teknoloji suçları gibi terimler ise anlamını yitirecek kadar geniş görünürler. Örneğin, ileri teknoloji suçu, nanoteknoloji ya

---

[19] Koca, Mahmut; Üzülmez, İlhan; Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, Ankara, 2017, s. 810.

[20] Akbulut, s. 24.

[21] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 53, 63. Diğer bilişim tanımları için *bkz*., Taşkın, s. 3-4.,

"*Cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtları ile karşılaştırılmak suretiyle program yükleme veya internetten gönderme şeklinde suça konu mesaj gönderilip gönderilmediğinin araştırılması gerekir. Cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak hüküm kurulması doğru değildir*." Yarg. 8. C. D., 2014/30037 E., 2015/14023 K., 18.03.2015.

[22] Koca/Üzülmez, s. 811.

[23] İnternet kavramına ilişkin ayrıntılı bilgi için *bkz*.. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 72 vd., Taşkın, s. 13 vd.

da biyomühendislik gibi diğer ileri teknoloji gelişmelerini içerecek kadar ağa dayalı bilgi teknolojilerin ötesine gidebilirler.[24] Diğer yandan, bu nitelikteki suçlarla mücadele edilirken gerektiğinde birden fazla yargı yerine yetki verilmesi söz konusu olduğundan, "*çok yargısal suçlar*" kavramına da literatürde rastlanılmaktadır.[25] Kanaatimiz, terminolojik olarak "*bilişim suçları*" kavramının tercih edilmesinin isabetli olduğudur.

Son olarak, bilişim suçları salt bilişim sisteminin kendisine yönelik hukuka aykırı girme veya orada kalma fiillerinden ibaret değildir. Bir diğer ifadeyle, fiziksel temas ile bilişim sisteminde yer alan dosya, program ya da diğer unsurlara erişmek dışında diğer bazı fiiller de bu kapsamda değerlendirilebilirler.[26] Nitekim internet ağını kullanmak suretiyle ve mağdurun rızası olmaksızın bu kişinin e-mail, facebook, instagram, twitter vs. gibi hesaplarına girmek ve orada kalmaya devam etmek de TCK'nun 243. maddesi kapsamında suç teşkil edecektir.[27]

---

24 Dülger, Murat Volkan, Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması, Taad, Y:8, S:31, 2017, s. 146., Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 66, 67. Elektronik ve dijital kelimeleri için *bkz*., Karagülmez, s. 40 vd.

25 Karagülmez, s. 43-44.

26 "*Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır*." Yarg. 8. C. D., 2016/12839 E., 2017/11114 K., 11.10.2017.

27 "*…sanığa ait internet hattıyla katılanın e-mail hesabına izinsiz girildiği sabitse de şifresini değiştirmek sureti ile erişimi engellediğine dair tespit bulunmaması karşısında eyleminin TCK.nun 243. maddesi kapsamında değerlendirilmesi gerekirken suç vasfında yanılgı sonucu yazılı şekilde hüküm kurulması…*" Yarg. 8. C. D., 2017/10095 E., 2017/13454 K., 29.11.2017.

243. Maddenin 2. fıkrası bakımından da suçun konusu "*bilişim sistemi*"dir.

Kanun koyucu bu fıkrada, bilişim sisteminin niteliğinden kaynaklı olan bir cezayı azaltan nitelikli unsura yer vermiştir. Bu anlamda 2. fıkra bakımından da suçun oluşması, sistemin "*bilişim sistemi*" özelliği göstermesine bağlıdır. Ancak burada cezanın indirilmesi aynı zamanda bu bilişim sisteminin "*bedeli karşılığı yararlanılabilen*" nitelikte olmasını gerektirmektedir. Her ne kadar doktrinde, kanun koyucunun belirli bir ücret karşılığı yararlanılabilen bilişim sistemlerine girilmesi halinde cezanın indirileceği görüşleri savunulsa da[28] biz bu bedelin illa ki para karşılığında ödenmesi gerektiğini düşünmüyoruz. Bedelin sözlük anlamının bir şeyin karşılığı olması dolayısıyla gündelik yaşamda bir hizmetin karşılığı olarak genellikle para ödense de bazen başka şeylerin de bedel olarak ödenmesi mümkündür. Örneğin internet ortamında abonelerine hizmet sunan bir site, kendisine makale gönderilmesini ya da sitesine en az beş kişinin abone edilmesinin sağlanmasını bedel olarak kabul etmişse, TCK'nun 243'üncü maddesinin 2'nci fıkrası kapsamında değerlendirilecektir.[29]

Değinmek istediğimiz bir diğer kavram ***veri*** kavramıdır.

Veri (data), bilgilerin belirli bir formata dönüştürülmüş hali olup, bilgisayarın çalıştığı bilgiler olarak ifade edilmektedir.[30]

Veri, AKSSS'nin 1. maddesinde, "*bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi*" olarak tanımlanmıştır.

5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*"un tanımlar başlıklı 2. maddesinde ise; "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*" veri olarak tanımlanmaktadır.

Veri, her türlü bilginin, bilgisayarların işlem yapabileceği, sonuçlar üretebileceği, saklayabileceği ve gerektiğinde yeniden okuyabileceği şekilde sayısal birimlere dönüştürülmüş hali olarak tanımlanmıştır.[31] Bu kapsamda programlar da veri kavramı içinde olup, sisteme girilen, sistemde işlenen ve saklanan her tür değer, veri olarak ifade edilmektedir. Bu kavramın kapsamına rakamlar, harfler, virgül, nokta, noktalı virgül, tire, tırnak işareti gibi diğer birtakım özel simgeler de dâhildir.[32]

---

[28] Karakehya, Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, TBB Dergisi, Sayı 81, 2009, s. 17.

[29] Apaydın, Cengiz, Bilişim Sistemine Girme Suçu, TAAD, Y: 7, S: 24, Ocak, 2016, s. 271.

[30] Yazıcıoğlu, s. 29.

[31] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 71.

[32] Akbulut, s. 26.

Dikkat edilmesi gereken husus, burada ifade edilen veriyi salt "*bilgisayar/bilişim sistemi verisi*" şeklinde dar anlamamak gerektiğidir. Kanaatimiz, 243. maddenin 3. fıkrasında ifade edilen "*sistemin içerdiği veri*", CD, USB yahut taşınabilir bellek gibi bilişim sistemi/bilgisayar dışındaki araçlarda bulunan verileri de kapsamına alacak şekilde yorumlanması gerektiği yönündedir.[33] Zira bilişim sistemi yahut bilgisayarlar en temel işlevlerini "*veri*" üzerinden yerine getirmektedir. Bu anlamda, bilgisayarın mütemmim cüzü olmayan ve fakat onun fonksiyonunu yerine getirmesi bakımından neredeyse mütemmim cüz niteliğindeki bir unsuru (veriyi) sağlayan diğer unsurların "*sistem içindeki veri*" olarak yorumlanması mümkündür. Bu anlamda bir bilişim sistemine girilmesiyle, CD, USB yahut taşınabilir bellek gibi araçlarda bulunan verinin yok olması yahut değiştirilimesine neden olunması halinde 243. maddenin 3. fıkrası uygulama alanı bulacaktır. Kanaatimizce, 5237 sayılı TCK'nun 243. maddesinde, "*bir bilişim sisteminin bir kısmına*" girilmesi veya orada kalınmasıyla ifade edilmek istenen bir diğer husus da budur.

I.2.2. Suç Teşkil Eden Fiil

243. maddenin 1. fıkrasında suç teşkil eden fiil, hangi yolla olursa olsun, bir bilişim sisteminin bütününe veya bir kısmına "*hukuka aykırı şekilde girmek*" veya "*orada kalmaya devam etmek*" olarak öngörülmüştür.

Belirtmek gerekir ki 24/3/2016 Tarihli ve 6698 sayılı Kanun'un 30. maddesiyle "*bu fıkrada yer alan 've' ibaresi 'veya' şeklinde değiştirilmiştir*" şeklinde yapılan düzenlenme öncesinde suçun oluşması için, sadece bilişim sistemine girmek yeterli olmayıp, belirli bir süre sistemde kalmaya devam etmek de gerekmektedir.[34]

---

[33] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 72, Akbulut, s. 26-27.,

Aksi yönde görüş için *bkz*., Koca/Üzülmez, s. 817.

[34] Mahmutoğlu, s. 860, Karagülmez, s. 183, Taşkın, s. 26.

Bazı yazarlar, söz konusu suçun oluşması bakımından, girmek ve kalmak şeklinde biri icrai, diğeri ise ihmali iki hareketin bir arada oluşması gerektiğini savunmaktadırlar. MAHMUTOĞLU, s. 860. Diğer bazı yazarlar ise, kalmaya devam etmenin mutlaka ihmali nitelikte olması gerekmediğini, aksine failin, sistemde bulunan güvenlik önlemleri nedeniyle sistemde kalmaya devam etmek için, çeşitli işlemler yapmaya devam edebileceği ve bu hareketlerinin de ihmali değil, icrai olacağını ifade etmektedirler. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 342.

Belirtmek gerekir ki, 5237 sayılı Kanun'un 243. maddesinin 1. fıkrasındaki suç tipinin tam karşılığı 765 sayılı TCK'da bulunmamaktadır. Zira 765 sayılı TCK'nun 525/a maddesinde suçun oluşabilmesi, "*verilerin ele geçirilmesi*"ne bağlıyken, 5237 sayılı TCK'da suçun oluşması failin, "*sisteme girmek*" veya "*kalmaya devam etmek*" fiillerini işlemesine bağlıdır. Böylece, 5237 sayılı Kanun'da suçun oluşması bakımından "*verilerin ele geçirilmesi*" şartı aranmamaktadır.

Bilişim sistemine "*hukuka aykırı şekilde girmek*" suçuyla kastedilen, bilişim sistemlerine yapılacak olan fiziki bir müdahale değildir.[35] Burada "*girmek*" sözcüğüyle anlatılmak istenen, "*bilişim sistemlerinin oluşturduğu soyut sanal alana girmek*"tir.[36] Bir başka ifadeyle, bir bilişim sisteminin tamamına ya da bir kısmına ulaşmak, içeriğine dâhil olmak, sanal bir alana erişmek, girmek olarak anlaşılmalıdır.[37] Sözgelimi, bilgisayarın kasasını açarak içindeki donanıma zarar vermek bu suçu oluşturmaz; bu durumda koşulları varsa "*mala zarar verme*" suçu oluşur.[38]

Girmek (erişim) fiili, bir kimsenin emanet ettiği bilgisayarın açılması ve içindeki verilerin gönderilmesi[39] şeklinde gerçekleşebileceği gibi kamusal veya yerel telekomünikasyon ağları yoluyla veya internet üzerinden de gerçekleşebilir. Erişimde, bağlantının kablolu-kablosuz olması, mesafenin yakınlığı-uzaklığı suçun oluşumunda etkili değildir. Sisteme e-posta mesajı ya da dosya gönderilmesi durumunda ise bilişim sistemine girme değil, veri gönderme söz konusu olduğundan, girmeden söz edilemeyecektir. Ancak gönderilen dosyanın içinde yer alan programlar aracılığıyla bilişim sistemine girmek mümkün ise bu durumda da bilişim sistemine girmeden bahsedebiliriz. Bu durumda mail yoluyla gönderilen dosyayı alan kişinin bu dosyayı açmaması halinde ise teşebbüs tartışması yapılacaktır.[40]

2016 Yılında yapılan değişiklik sonrasında suç seçimlik hareketli hale gelmiştir. Zira suçun oluşması için sisteme girmek yeterli olup, kalmaya devam etme aranmamaktadır.[41] Bu nedenle sisteme mağdurun rızasıyla girildikten sonra, rızası dışında kalınması halinde de suç oluşacaktır. Dikkat çeken husus, kanun koyucunun burada "*kalan*" kelimesini değil, "*kalmaya devam*

---

35 Taşkın, s. 25.

36 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 342, Karagülmez, s. 184, Apaydın, s. 262.

37 Mahmutoğlu, s. 860.

38 Taşkın, s. 25.

39 Her ne kadar yazar burada "*ve içindeki verilerin gönderilmesi*" şeklinde bir ifade kullanılmışsa da 765 sayılı TCK'dan farklı olarak 5237 sayılı Kanun'da suçun oluşması için "*veriye ulaşma*" yahut "*veri gönderilmesi*" şartları aranmadığından, bilgisayarın hukuka aykırı olarak açılması ve orada kalmaya devam edilmesi fiili yeterli olacaktır.

40 Mahmutoğlu, s. 860-861.

41 Önceki düzenlemede suçun oluşabilmesi için failin bilişim sistemine hukuka aykırı girmesi yetmemekte, aynı zamanda orada kalmaya devam etmesi gerekmekteydi. Bu anlamda adı geçen suç, çok hareketli bir suç olmakla birlikte ayrıca kesintisiz (mütemadi) niteliktedi. Mahmutoğlu, s. 860, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 379.

eden" ibaresini tercih etmiş olmasıdır. Zira "*kalmaya devam eden*" ibaresi, "*kalma*"ya göre daha uzun süren bir temadiyi nitelemektedir.[42] Bu ise önceki düzenleme bakımından, bilişim sistemine girdikten sonra, kalmaya devam etme süresi için sabit bir sürenin belirlenmesini yine mümkün kılmasa da suçun oluşması bakımından yargıca bir yorum alanı açmaktaydı.[43] Değişiklik sonrasında ise kanaatimizce bu husus, cezanın belirlenmesi ve bireyselleştirilmesinde göz önünde bulundurulacaktır.

Bu anlamda, somut olayda, her bilişim sisteminin özelliği ve güvenlik yapısı dikkate alınmak suretiyle "*kalmaya devam etme*" bakımından "*yeterli süre*" yargıç tarafından değerlendirilmelidir.[44] Bazı yazarlara göre burada dikkat edilmesi gereken kıstas, failin başkasına ait bir alana girdiğini fark etmesinin ardından, bu fiilini sonlandırması için yetecek sürede buradan uzaklaşıp uzaklaşmadığıdır. Bir başka ifadeyle fail, girmiş olduğu sistemden çıkması için gerekli olan (çıkmayı olanaklı hale getiren) sürede çıkmamışsa kalmaya devam etmiş olacaktır.[45]

Bir kısım yazar, özellikle suçun seçimlik hareketli olmasından öce, bilişim sistemine girilmesinin ardından, bir verinin yahut bilginin elde edilmesi veya öğrenilmesini suçun oluşumu için yeterli kabul etmekteydi. Biz bu konuda, suç tanımında böyle bir harekete yer verilmediği ve fakat bilişim sistemine girilmesinden sonra bir verinin yahut bilginin elde edilmesinin "*kalmaya devam etme*" süresinin belirlenmesi bakımından bir yorum aracı olarak kullanılabileceği görüşüne katılıyoruz.[46] Bu bağlamda mağdurun zarara uğrayıp uğramadığının bir önemi yoktur. Böylelikle fail bilişim sistemine girip orada kalmasına rağmen, hiçbir veri ve bilgi edinmeden sistemden çıksa dahi, bu suç oluşacaktır. Böylece, bilişim sistemine girme suçu, bir tehlike suçu olarak nitelendirilebilecektir.[47]

Suçun temel şekli dışında kanun koyucu, 243. maddenin 2. fıkrasında bilişim sistemine girmenin "*bedeli karşılığı yararlanılabilen sistemler hakkında*

---

[42] Karagülmez, s. 185.

[43] "*Sanığın, sübut bulan bilişim sistemine girip, katılan adına başkaları ile konuşma yapacak kadar kalmasından ibaret eyleminin TCK'nın 243/1. maddesinde tanımlanan 'Bilişim SistemineGirme' suçunu oluşturacağı gözetilmeden, delillerin takdirinde ve suç vasfında yanılgıya düşülerek…*" Yarg. 12. C. D., 2013/11510 E., 2014/2982 K., 10.02.2014.

[44] Karagülmez, s. 185, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 344-345.

[45] Mahmutoğlu, s. 861.

[46] Karagülmez, s. 185, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 345.

[47] Mahmutoğlu, s. 861-862.

işlenmesi"ne ilişkin bir hüküm getirmiştir. Nitekim söz konusu düzenlemeye göre, "*Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.*"

Burada dikkat edilmelidir ki, 243/2 bakımından suçun konusu, "*bedeli karşılığında yararlanılabilen bilişim sistemleri*"dir. Eğer suçun konusu "*Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmet*" ise, TCK'nun 163. maddesi gereğince "*Karşılıksız Yararlanma*" suçunun oluşması söz konusu olabilecektir.[48]

Buna göre, adı geçen fıkranın uygulanabilmesi için ortada bir bilişim sistemi olması ve bu bilişim sisteminin de bedeli karşılığı yararlanılan bir sistem olması gerekir. Diğer bir değişle, failin bedelini ödeyerek hukuka uygun olarak girebileceği bir sisteme, bedeli ödemeksizin girmesi veya orada kalmaya devam etmesi durumunda bu fıkra hükümleri uygulanacaktır.[49]

Belirtmek gerekir ki, "*bedeli karşılığında yararlanılabilen bilişim sistemleri*" hakkında kanunun 243. maddesinde ya da gerekçesinde bir açıklama yapılmamıştır. Bu kavramdan genel olarak anlaşılan temel dört şey, internet üzerinden hizmet veren web siteleri (ücreti karşılığında abonelerinin kullanımına açık elektronik arşiv merkezleri, elektronik gazeteler, elektronik kütüphaneler vs.), internet kafelerde olduğu gibi bedel karşılığı bilişim sisteminin kiralanması, anlaşmayla cep telefonlarına bilişim sistemi üzerinden reklam için mesaj yollanması ve belli süreli internet bağlantı servisinin sağlanmasıdır.[50]

Ancak, "*Bedeli karşılığında yararlanılabilen*" ibaresindeki "*bedel*"in yalnızca para olarak anlaşılmaması, para dışındaki bir takım karşılıkların da "*bedel*" olarak kabul edilebileceği ifade edilmelidir. Örneğin internet ortamında abonelerine hizmet sunan bir site, kendisine makale gönderilmesini ya da sitesine en az beş kişinin abone edilmesinin sağlanmasını bedel olarak kabul etmişse, bu siteye yönelik madde kapsamındaki suçta da ikinci fıkranın koşullarının oluştuğunu kabul etmek gerekmektedir.[51]

Suçun konusu kapsamında değinmek istediğimiz son husus, 243. maddenin 3. fıkrasıdır.

---

[48] Ayrıca *bkz*., Yılmaz, Zahit; Apiş, Özge, Karşılıksız Yararlanma Suçu (TCK m.163), Prof. Dr. Nur Centel'e armağan, MÜHFHAD, Y: 2013, C: 19, S: 2, s. 1767 vd.

[49] Erdoğan, Yavuz, Bilişim Sistemine Girme ve Kalma Suçu, www.hukuk.deu.edu.tr>6-yavuzerdogan, (Erişim Tarihi: 30.01.2018), s. 1396.

[50] Erdoğan, s. 1399.

[51] Karagülmez, s. 190-191, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 352-353, Erdoğan, s. 1397.

Kanun koyucu bu maddede, 243. maddenin 1. fıkrasındaki suçun neticesi sebebiyle ağırlaşmış halini düzenlemiştir. Nitekim bir bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme neticesinde, "*sistemin içerdiği veriler yok olur veya değişirse*" failin cezası artacaktır.

Şu halde, 5237 sayılı TCK'nun "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*" suçunu düzenleyen 244. maddesinde verilere veya sisteme müdahale edilmesinin taksirli şekline yer verilmediğini, buna karşılık sisteme hukuka aykırı giriş yapılması ve orada kalmaya devam edilmesi nedeniyle sitemdeki verilerin yok olması veya değişmesi hali, yani fiilin taksirli şeklinin TCK'nın 243. maddesinin 3. fıkrasında netice sebebiyle ağırlaşmış suç olarak yaptırım altına alınmış olduğu ifade edilmiştir.[52]

Bazı yazarlar, netice sebebiyle ağırlaşmış suçların, kast-taksir kombinasyonu ile gerçekleşebilkeceği gibi kast-kast kombinasyonu şeklinde de gerçekleşebileceğinden yola çıkarak, 243/1 kapsamında hareket eden failin ister taksirle ister kasten sistemdeki verilerin yok olması yahut değişmesine sebebiyet versin 243. maddenin 3. fıkrasını ihlal etmiş olacağını savunmaktadır. Ancak bu yazarlara göre hareketin kasten işlenmesi ihtimalinde aynı zamanda 244. maddenin 2. fıkrasındaki suçun oluşması da söz konusu olacaktır.[53] Bu olasılıkta, 44. madde gereğince farklı nev'inden fikri içtima hükümlerinin uygulanması gerekecektir.[54] Bizim de katıldığımız görüşe göre ise, burada ağır neticeye ancak taksirle sebebiyet verilmesi halinde 234/3 uygulanabilir. Failin verileri yok etmek yahut değiştirmek kastı varsa, 244/2 uygulanacaktır.[55]

---

[52] Akbulut, s. 40.

[53] "*…dosya kapsamına göre, sanığın, nişanlısı olması sebebiyle daha önce bildiği mağdura ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının internet şifresini, nişanın bozulduğu ve fiilen ayrıldıkları dönemde değiştirerek, hakkı bulunmadığı halde bilişim sistemindeki mağdura özel kısma girdiği ve mağdura ait facebook hesabı üzerinden, mağdur tarafından yazılıyormuş algısı doğuracak şekilde, başka kişilerle iletişim kurup, hukuka aykırı olarak sistemde kalmaya devam ederek, mağdurun sistemdeki kendisine ait kısma erişimini engellediği anlaşılmakla, sanığın sübut bulan eyleminden dolayı TCK'nın 244/2. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mahkûmiyetine karar verilmesi gerekirken…*" Yarg. 12. C. D., 2015/475 E., 2015/6333 K., 13.04.2015.

[54] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 349.

[55] Koca/Üzülmez, s. 817.

I.3. Bilişim Sistemine Girme Suçu Bakımından Hukuka Uygunluk Nedenleri

5237 Sayılı TCK'da hukuka uygunluk nedenleri, "*hakkın kullanılması (TCK m. 26/1)*", "*kanun hükmünü yerine getirme (TCK m. 24/1)*", "*meşru savunma (TCK m. 25/1)*", ve "*ilgilinin rızası (TCK m. 26/2*" olarak öngörülmüştür.

İlgilinin rızası da bilişim sistemine girme suçu bakımından hukuka uygunluk sebebi olmakla birlikte, çalışma konumuzun sınırları gereği bizim açımızdan önem arz eden hukuka uygunluk sebebi ise, "*kanun hükmünü yerine getirme (TCK m. 24/1)*"dir. Zira "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama*" koruma tedbiri, 5271 sayılı CMK'nun 134. maddesinde düzenlenen ve kanunda belirtilen koşulları oluştuğu takdirde bilişim sistemine girme suçu bakımından hukuka uygunluk sebebi oluşturan bir koruma tedbiridir.

Bu hususa ilişkin açıklamalara aşağıda daha ayrıntılı bir şekilde yer verecek olmakla birlikte, bizim burada üzerinde kısaca durmak istediğimiz husus, "*bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden*" kimsenin cezalandırılacağını düzenleyen 243. maddenin 1. fıkrasında yer alan "*hukuka aykırı olarak*" ibaresidir. Zira bazı suç tiplerinde kanun koyucunun hukuka aykırılık unsurunu açıkça belirtmesi doktrinde "*hukuka özel aykırılık*" olarak nitelendirilmekte ve bazı yazarlar bu gibi durumlarda failde özel bir hukuka aykırılık bilincinin olmasını aramaktadırlar.[56] Bir başka ifadeyle, bu yazarlara göre, kastın hukuka aykırı-

---

[56] "*Oluşa ve dosya kapsamına göre; eş olan sanıkların şikayeti üzerine devam eden bir soruşturmada fikir ve eylem birliği içinde katılanın tanık olarak verdiği beyanlarının doğru olmadığını ortaya çıkarmak için katılanın rızası dışında Sosyal Güvenlik Kurumunun hizmet dökümü sistemine giriş yaparak katılanın hizmet bilgilerinin alınıp devam eden soruşturma dosyasına delil olarak sundukları olayda, söz konusu içerikleri üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına dair hakkında bir iddia ileri sürülmeyen sanıkların, devam eden soruşturmada iddialarını ispatlama amacını taşıyan eylemlerinde gerektiğinde soruşturmayı yürüten makam tarafından da söz konu kayıtların getirtilebileceği göz önüne alındığında hukuka aykırı hareket etme bilinciyle davrandıkları kabul edilemeyeceğinden, atılı suçların unsurlarının oluşmadığından bahisle beraat kararı verildiğine yönelik yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir*." Yarg. 12. C. D., 2015/16132 E., 2017/3999 K, 16.05.2017.

"*Katılanın üçüncü kişilerle yaptığı yazışmaların, sanık tarafından katılanla aralarında görülen boşanma davasına delil olarak vermesi biçimindeki eylemi, TCK'nın 132/2. maddesindeki haberleşmenin gizliliğini ihlal suçları kapsamında değerlendirilebilir ise de, görüşme ayrıntıları dökümünü üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına dair hakkında bir iddia ileri sürülmeyen sanığın, boşanma davasındaki iddiasını ispatlama amacını taşıyan eyleminde, hukuka aykırı hareket ettiği bilinciyle hareket etmediği anlaşılmakla, sanığın beraatine karar verilmesinde*

lığı kapsayıp kapsamadığı özellikle araştırılmalıdır.[57] Diğer yandan, hukuka özel aykırılık hallerinde failin davranışının hukuka aykırı olduğu bilinciyle hareket etmesi gerektiğinden, bu suçlar ancak doğrudan kastla işlenebilecek, bu suçların olası kastla işlenmesi mümkün olmayacaktır.[58]

Bu görüş karşısında bazı yazarlar ise, bu gibi hallerde hukuka aykırılığın değil, kastın "*özel*" bir türü yahut fiilin "*özel*" bir işlenme biçiminin söz konusu olduğunu savunmaktadırlar. Bu yazarlara göre, hukuka özel aykırılık olarak adlandırılan durumlarda, aslında kanun koyucunun ifade konusundaki özensizliği ve somut olayda hukuka uygunluk nedenlerinin bulunmaması gereğinin tekrar tekrar dile getirilmesi gereği söz konusudur.[59] Böylece aslında hukuka aykırılığın kanun koyucu tarafından üzerine basılarak ifade edilmesi alışkanlığının temel amacı da yargıçların bu hususa dikkatini çekmektir. Yoksa bu nitelikteki ibarelerin varlığı yahut yokluğu fiilin hukuka aykırılığı üzerinde herhangi bir etki yaratmamaktadır.[60]

Bu bilgiler ışığında bizim de kanaatimiz, bu nitelikteki ibarelerin varlığı yahut yokluğunun fiilin hukuka aykırılığı üzerinde herhangi bir etki yaratmadığı ve failde özel bir hukuka aykırılık bilincinin aranmasının gerekmediğidir.[61] Buna göre, CMK md. 134'te düzenlenen "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma*" koruma tedbirinin bilişim sistemine girme suçunda bir hukuka uygunluk nedeni oluşturması bakımından, failde özel bir hukuka aykırılık bilincinin aranmaması gerektiği kanaatindeyiz.

Bir diğer husus, 5237 sayılı TCK'nun 27. maddesinin 1. fıkrasıdır. Zira söz konusu düzenleme hukuka uygunluk nedenlerinde sınırın aşılmasını düzenlemekte ve "*Ceza sorumluluğunu kaldıran nedenlerde sınırın kast olmaksızın*

isabetsizlik görülmemiştir." Yarg. 12. C. D., 2015/9555 E., 2016/10731 K, 22.06.2016.

57 Artuk, Mehmet Emin; Gökcen, Ahmet; Alşahin, Mehmet Emin; ÇAKIR, Kerim; Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2017, s. 325 vd., Centel, Nur; Zafer, Hamide; Çakmut, Özlem; Türk Ceza Hukukuna Giriş, Beta Basım Yayım Dağıtım, Eylül, 2014, s. 286, Mahmutoğlu, s. 862.

58 Artuk/Gökcen/Alşahin/Çakır, s. 325.

59 Katoğlu, Tuğrul, Ceza Hukukunda Hukuka Aykırılık, Seçkin Yayıncılık, Ankara, 2003, s. 125.

60 Zafer, Hamide, Ceza Hukuku Genel Hükümler TCK m. 1-75, Beta Basım Yayım Dağıtım, Şubat, 2015, s. 285, 286, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 364.

61 Bu konuyla ilgili ayrıntılı bilgi için *bkz*., Göktürk, Neslihan, Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon, İnönü Üniversitesi Hukuk Fakültesi Dergisi C:7 S:1, 2016, s. 424 vd.

aşılması halinde, fiil taksirle işlendiğinde de cezalandırılıyorsa, taksirli suç için kanunda yazılı cezanın altıda birinden üçte birine kadarı indirilerek hükmolunur." şeklinde bir hüküm ihtiva etmektedir. Böylece, bilişim sistemine girme suçu bakımından hukuka uygunluk sebebi oluşturan "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma*" koruma tedbirinin de sınırlarının aşılması mümkündür. Bu gibi hallerde de "*bilişim sistemine girme*" suçunun oluşacağı kuşkusuzdur.

II. Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Koruma Tedbiri

II.1. Genel Açıklamalar

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama, elkoyma koruma tedbiri, arama ve elkoyma koruma tedbirlerinin özel bir şeklidir.[62] Zira aramaya ilişkin genel hükümler, 5271 sayılı CMK'nun 116 vd. ve 123. maddelerinde düzenlenmişken, inceleme konumuza ilişkin koruma tedbiri 134. maddede ayrıca hüküm altına alınmıştır. Bu anlamda örneğin konutunda yahut işyerinde yapılan bir arama sırasında şüphelinin kullandığı bilgisayar da aranacaksa, ayrıca CMK'nun 134. maddesindeki hükümlerin uygulanması gerekmektedir.[63]

Söz konusu koruma tedbiri, bilgisayar, bilgisayar programları ve kütüklerinde arama yapılması ve delil niteliği taşıyan bilgilere rastlanması halinde bilgisayar kasasına ya da bazen sadece kopyalama suretiyle verilere elkonul-

---

[62] Gökcen, Ahmet; Balcı, Murat; Alşahin, M. Emin; Çakır, Kerim; Ceza Muhakemesi Hukuku II, Adalet Yayınevi, 2018, s. 124, Özbek, Veli Özer; Doğan, Koray; Bacaksız, Pınar; Tepe, İlker; Türk Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ağustos, 2017, s. 356, 358.

Şahin, Cumhur, Ceza Muhakemesi Hukuku -I-, Seçkin Yayıncılık, Ağustos 2017, s. 328.

[63] Özbek/Doğan/Bacaksız/Tepe, Ceza Muhakemesi Hukuku, s. 360, Ünver/Hakeri, s. 411.

"*... Sulh Ceza Mahkemesi'nin kararının CMK'nın 116. maddesi uyarınca sanığın işyerinde arama yapılmasına yönelik olduğu ve CMK'nın 134. maddesi uyarınca bilgisayar ve bilgisayar kütükleri üzerinde arama yapılmasına dair hakim tarafından verilmiş bir karar bulunmadığı cihetle, arama sonucu harddisklerde bulanan 7095 adet MP3 formatında müzik/ses dosyası nın hukuka aykırı şekilde elde edilmiş delil niteliğinde olması sebebiyle hükme esas alınamayacağı ve atılı suçlamayı kabul etmeyen sanık hakkında hukuka aykırı şeklinde elde edilmiş bu delil dışında mahkumiyetine yeterli başkaca bir delil de bulunmadığı gözetilmeden, beraati yerine yazılı şekilde mahkumiyetine karar verilmesi…*" Yarg. 19. C. D., 2015/32456 E., 2016/16830 K., 02.05.2016., Yarg. 19. C. D., 2015/6392 E., 2015/9017 K., 22.12.2015.

masını ifade etmektedir.

5271 sayılı CMK'nun 134. maddesine göre,

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

Belirtmek gerekir ki, klasik suçlar bakımından delil, genelde suç işlenen alandan elde edilmesine rağmen, bilişim suçlarında bu alan çoğunlukla bilişim sistemleridir. Bu sistemler içerisinde ilk akla gelen unsur bilgisayarlar olsa da sistemle ilgili bilgi toplayabilen pek çok unsur da bilişim sistemi içerinde değerlendirilmektedir.[64] Bu ise karşımıza 5271 Sayılı CMK'nun 134. maddesine göre elde edilebilecek "*dijital delil*" yahut "*e-delil*" kavramını çıkarmaktadır.

Dijital/elektronik delil, bir suçun soruşturulmasında, ispatlanmak istenen hususu, sayısal bir formda depolanan yahut iletilen bulguyla ortaya koyan delillller olarak ifade edilmektedir. Bu kapsamda adı geçen deliller, bilgisayar sabit (hard) diskleri, çıkarılabilir USB flash sürücüleri (bellek), cep telefonları, uydular, internet yahut word veya excel dosyaları, e-postalar, anlık iletiler ya da elektronik tablolama gibi metin belgeleri, haritalar, veritabanları, dijital görüntüler, video veya ses dosyaları, GPS verileri, internet tarama geçmişi ve kılavuz verileri (metadata) gibi farklı kaynaklardan edinilebilirler.[65]

Başka bir tanıma göre ise, dijital/elektronik delil, adli bilişimle ilgili bir çalışma esnasında, bilgisayarlar, mobil telefon, dijital fotoğraf makinası, dijital videolar, dijital faks makineleri gibi bilişim sistemleri ve bu kapsamdaki aygıtları üzerinden elde edilen adli delillerdir.[66] Bunlardan elde edilecek deliller, video görüntüleri, fotoğraflar, yazı dosyaları, çeşitli bilgisayar programları, iletişim kayıtları, gizli yahut şifreli dosya ya da klasörler, bunların oluşturulma, değiştirilme veya erişim tarih kayıtları, son girilen ve sık kullanılan internet siteleri, internetten indirilen dosyalar, silinmiş dosya/klasörler vs. olabilir.[67]

---

64 Karagülmez, s. 443-44.

65 Roscini, Marco, Digital Evidence as a Means of Proof before the International Court of Justice, Oxford academic, Journal Of Conflict & Security Law, Vol. 21, Iss. 3, 2016, s. 1-2.

66 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 679.

67 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 679-80.

Bu kapsamda, dijital ya da elektronik delillerin, salt bilgisayarlardan elde edilebilecek delilleri ifade etmediğini belirtmemiz gerekmektedir. Bilgisayar niteliği göstermemekle birlikte bilişim sistemi özelliği gösteren diğer aygıtlar da elektronik delil elde etme bakımından önemli bir yere sahiptirler. Önemli olan husus, ceza muhakemesi sürecinde delil elde edilirken, CMK'nun 134. maddesinde öngörülen şartların, bu bilişim sistemlerinin aranması sırasında da uygulanıp uygulanmayacağıdır. Bu hususa aşağıda koruma tedbirinin şartlarını incelerken değinmeyi uygun buluyoruz.

Son olarak ifade etmek gerekir ki, tedbirin daha ziyade bilişim suçları için uygulanabileceği gibi bir izlenim uyansa da uyuşturucu ticareti suçuna ilişkin bilgisayardaki kayıtların elde edilebilmesi için bilgisayarda arama yapılmasında olduğu gibi, diğer suç tipleri için de söz konusu koruma tedbirinin uygulanması söz konusu olabilecektir.[68]

II.2. Koruma Tedbirinin Uygulanma Şartları

II.2.1. Bir Suç Dolayısıyla Yapılan Soruşturmanın Bulunması

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama elkoyma koruma tedbiri, soruşturma aşamasında başvurulabilen bir koruma tedbiridir. Zira 5271 sayılı CMK'nun 134. maddesinde kanun koyucu açıkça, bu tedbire "*bir suç dolayısıyla yapılan soruşturmada*" başvurulabileceğini hüküm altına almıştır.

Ancak doktrinde, bu şartın dar anlamda yorumlamaması gerektiğini, zira, kovuşturma aşamasında eksik deliller söz konusu ise, elbette bu aşamada da CMK m. 134 uyarınca koruma tedbiri kararı verilebileceğini savunan yazarlar bulunmaktadır.[69] Her ne kadar bazı yazarlar, kamu davasının açılması için gerekli olan "*yeterli şüphe*"nin işlenen fiilden dolayı bir mahkûmiyet kararı verilebilmesi için yeterli olmadığını, bu nedenle kovuşturma aşamasında mahkemenin, delilleri mahkûmiyet hükmü kurmak bakımından yetersiz görmesi ve suçun sübutunun, bilgisayarlarda yapılacak arama, kopyalama ve elkoyma tedbirlerinin alınmasını gerektirmesi halinde, CMK. m.134'teki koruma tedbirine başvurulmasına istem üzerine yahut re'sen başvurulabileceği yönünde

---

68 Özbek/Doğan/Bacaksız/Tepe, Ceza Muhakemesi Hukuku, s. 360-361.

69 Özen, Muharrem; Özocak, Gürkan; Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134), Ankara Barosu Dergisi, 2015/1, s. 62., Şahin, Cumhur, s. 329, Yaşar, Yusuf; Dursun, İsmail; Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri, MÜHFHAD, C: 19, S: 3, 2013, s. 9, Baştürk, İhsan, Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma, Fasikül Aylık Hukuk Dergisi, Sayı: 9, Ağustos 2010, (https://jurix.com.tr/article/3286, E.T. 02.03.2018), s. 25.

gerekçeler sunsalar da[70] ceza muhakemesinde maddi gerçek araştırılırken her ne pahasına olursa olsun maddi gerçeğin araştırılamayacağı kuralının hatırda tutulması gerekmektedir. Diğer yandan, ceza muhakemesine hakim olan temel ilkelerin tümü bir biriyle eşit değerde olup, pratik bir takım ihtiyaçlar nedeniyle birinin diğeri aleyhine genişletilmesi mümkün olmamalıdır. Bu nedenle mahkemenin delil toplanma ve re'sen araştırma yetkisini, hukuk devleti ilkesine uygun olarak yerine getirmesi gerekmektedir. Kanaatimiz, 134. maddenin 1. fıkrasının hatalı düzenlenmesi nedeniyle sanığın kullandığı veya ona ait bilgisayar ya da bilgisayar kürüklerinde arama yapılması olanağının bulunmadığıdır. Zira bu hükmün kovuşturma evresi için de kullanılması, koruma tedbirlerinde kanunilik ilkesine aykırı olup, bunun mümkün olabilmesi için yasal düzenlemeye ihtiyaç bulunmaktadır.[71]

Bu tedbirlere sadece CMK kapsamında yürütülen bir "*suç*" soruşturmasında imkân tanınmış olması nedeniyle idari yahut disiplin soruşturması gibi hukukun diğer alanlarında yürütülen soruşturmalarda söz konusu tedbire başvurulması da mümkün olmayacaktır.[72]

II.2.2 Kuvvetli Şüphe Sebeplerinin Bulunması

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama elkoyma koruma tedbirine başvurulması, "*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*"na bağlıdır.

Belirtmek gerekir ki, adı geçen koruma tedbiri bakımından "*kuvvetli şüphe*"nin aranması 21/2/2014 tarihli ve 6526 sayılı Kanunun 11. maddesi ile söz konusu olmuştur.[73]

Şu halde kanun koyucu, arama koruma tedbirinin (CMK m. 116) uygulanması bakımından, "*makul şüphe*", İHAM'nin nitelendirmesiyle, "*mevcut olgu ve bulguların tarafsız bir gözlemciyi, kişinin suçu işlemiş bulunmasının mümkün bulunduğu hususunda ikna etmeye yetecek ölçü ve nitelikte bulun-*

---

70 Yaşar/Dursun, s. 10.

71 Ünver, Yener; Hakeri, Hakan; Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara, 2017, s. 410.

Ayrıca *bkz*., Kunter, Nurullah; Yenisey, Feridun; Nuhoğlu, Ayşe; Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Beta Basım Yayım Dağıtım, İstanbul, Ekim 2010, s. 1098.

72 Baştürk, s. 25.

73 Bu nedenle söz konusu değişiklik yapılmadan önce doktrinde, tedbirini uygulanması için "*basit şüphe*"nin yeterli olduğunu savunanlar olduğu gibi "*makul şüphenin*" aranması gerektiğini savunanlar da olmuştur. Kunter/Yenisey/Nuhoğlu, s. 1100.

ması"[74] şartını aramaktayken, bilgisayarlar söz konusu olduğunda "*kuvvetli şüphe*" sebeleri aramaktadır.

Böylece, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama elkoyma koruma tedbirine başvurulması için, elde edilen mevcut delillere göre yapılacak muhakeme sonunda, sanığın mahkum olma ihtimalinin kuvvetle muhtemel olması gerekecektir.[75] Bu anlamda somut olayda, makul şüphenin ötesine geçen, bir suçun işlendiği yönünde çok güçlü işaretler taşıyan bulguların olması gerekecektir. Kuvvetli şüphe, hem şüphelinin soruşturma konusu suçu işlediği yönünde, hem de üzerinde arama yapılacak bilgisayarda suç delillerinin bulunacağı yönünde kuvvetli şüphe olarak algılamak gerekmektedir.[76]

Bir diğer husus, söz konusu koruma tedbirine hükmedilebilmesinin "*başka surette delil elde etme imkânının bulunmaması*" şartına bağlı olmasıdır.

Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 4/c maddesine göre, "*başka surette delil elde etme imkânının bulunmaması*"ndan anlaşılması gereken "*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*"dır.

Bazı yazarlara göre, CMK'nun 134. maddesinde yer alan "*başka surette delil elde etme imkânının bulunmaması*" ibaresi sorunlu bir alan yaratmaktadır. Zira bilişim suçları söz konusu olduğunda belki de bakılması gereken ilk yer şüphelinin bilgisayarı olabilecektir. Halbuki adı geçen düzenleme ile önce

---

[74] Cengiz, Serkan; Demirağ, Fahrettin; Ergül, Teoman; Mcbride, Jeremy; Tezcan, Durmuş, Avrupa İnsan Hakları Mahkemesi Kararları Işığında Ceza Yargılaması Kurum ve Kavramları, Şen Matbaa, Ankara, Kasım 2008, s. 20, 41 vd.

Makul şüpheye ilişkin ayrıntılı açıklamalr için *bkz*., Gökcen/Balcı/Alşahin/Çakır, s. 9-10, Özbek/Doğan/Bacaksız/Tepe, Ceza Muhakemesi Hukuku, s. 252.

Şahin, İlyas, Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi, MÜHFHAD, C. 20, S. 3, Y. 2014, s. 106.

[75] Öztürk, Bahri; Tezcan, Durmuş; Erdem, Mustafa Ruhan; Gezer Sırma, Özge; Kırıt Saygılar, Yasemin; Özaydın, Özdem; Akcan Alan, Esra; Tütüncü Erden, Efser; Nazarî ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, 2016, s. 507, Gökcen/Balcı/Alşahin/Çakır, s. 11, 124, Şahin, Cumhur, s. 292, 328, Şahin, İlyas, s. 118, Ersoy, Uğur, Bir Koruma Tedbiri Türü Olarak Şirket Yönetimi İçin Kayyım Tayini (CMK m.133), AÜHFD, 65 (4), 2016, s. 3407-3408.

[76] Ceza Muhakemesinde Sayısal (Dijital) Delil, Olgun Değirmenci'den aktaran Özen/Özocak, s. 62.

başka delillerin araştırılmasını, bu suretle delil elde edilemezse 134. maddenin uygulanmasını öngörmektedir. Bu ise bilişim suçlarının soruşturulması bakımından problemler yaratabilecek niteliktedir.[77]

Bu görüşe katılmadığımızı ifade etmemiz mümkündür. Zira bu tedbir ikincil nitelikte olmakla beraber, somut olayın durumuna göre, diğer koruma tedbirlerine başvurulması halinde amacın hâsıl olmayacağı en başından itibaren anlaşılmaktaysa, doğrudan bilgisayarlara yönelik tedbirlere başvurulabilir.[78]

II.2.3. Hâkim Kararının Bulunması

5271 Sayılı Kanun'un 134. maddesine göre, şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine cumhuriyet savcısının istemi üzerine hâkim tarafından karar verilir.

Belirtmek gerekir ki, söz konusu koruma tedbiri bakımından "*gecikmesinde sakınca bulunan hâller*" gerekçesiyle herhangi bir istisna yaratılmamıştır. Bir başka ifadeyle, yakalama, arama, elkoymada olduğu gibi, cumhuriyet savcısının, cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilemeyecektir.

Ancak 20.07.2016 tarihli ve 668 sayılı "*Olağanüstü Hal Kapsamında Alınması Gereken Tedbirlerle Bazı Kurum ve Kuruluşlara Dair Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname*"nin "*soruşturma ve kovuşturma işlemleri*" başlıklı 3. maddesinin 1. fıkrasının j bendi gereğince, 26/9/2004 tarihli ve 5237 sayılı TCK'nun ikinci kitap dördüncü kısım dördüncü, beşinci, altıncı ve yedinci bölümünde tanımlanan suçlar, 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamına giren suçlar ve toplu işlenen suçlar bakımından, olağanüstü halin devamı süresince "*5271 sayılı Kanunun 134 üncü maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve elkoyma işlemlerine, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da karar verilebilir. Bu karar, beş gün içinde görevli hâkimin onayına sunulur. Hâkim, kararını elkoymadan itibaren on gün içinde açıklar; aksi halde elkoyma kendiliğinden kalkar. Kopyalama ve yedekleme işleminin uzun sürecek olması halinde bu araç ve gereçlere elkonulabilir. İşlemlerin tamamlanması üzerine*

---

[77] Karagülmez, s. 443, Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 671-672.

[78] Öztürk/Tezcan/Erdem/Sırma/Kırıt/Saygılar/Özaydın/Akcan/Alan/Tütüncü/Erden, s. 510.

elkonulan cihazlar gecikme olmaksızın iade edilir. "[79]

Burada dikkat çekmek istediğimiz bir husus, 134. maddenin 1. fıkrasında yer alan "*kopyalama*" ibaresinin terminolojik olarak "*elkoyma*" olarak anlaşılmaması gerektiğidir. Bir başka ifadeyle 134. madde, elkoyma işlemine ayrı kopyalama işlemine ayrı anlam yüklemekte ve bu nedenle her ikisinin tabi olacağı kurallar da farklılaşmaktadır. Söz konusu olan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama olduğundan, bunlardan elde edilecek delillerin de maddi bir varlığı olmayacağı doğrudur. Bu nedenle dijital olma özellikleri olan bu delillerin elde edilmesi ise bu verilerin kopyalanması şeklinde söz konusu olabilir. Bu ise teknik anlamıyla "*kopyalama*" olarak anlaşılmalıdır. Bu nedenle bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde, ilgili araç gerecin fiziken alınması "*elkoyma*", dijital delillerin tespit edilip ele geçirilmesi "*arama*" ve "*kopyalama*" olarak nitelendirilmelidir.[80]

Son olarak belirtmek gerekir ki, bilgisayar veya bilgisayar kütüklerine elkoyma koruma tedbirine karar verecek merci, genel nitelikteki arama ve elkoyma tedbirlerinde olduğu gibi (m. 119 ve m. 127) ayrı ayrı düzenlenmemiştir. 134. Maddenin 1. fıkrasında, arama ve kopyalama işlemleri bakımından cumhuriyet savcısının istemi ve hakim kararı (sulh ceza hakimi) şartı aranmaktadır. Özel nitelikli bir koruma tedbiri olmasından kaynaklı olarak bilgisayar veya bilgisayar kütüklerine elkoyma işlemi bakımından da genel nitelikli elkoyma tedbirine karar vermeye yetkili mercilerin değil, cumhuriyet savcısının istemi üzerine hakimin bu hususta karar vermeye tek yetkili suje olduğunu söylemek mümkündür. Ancak elbette 134. madde kapsamında elkoyma kararının verilmesine ilişkin usulün Kanun'da açıkça düzenlenmesi gerekmektedir.

II.3. Koruma Tedbirinin Konusu

5271 Sayılı Kanun'un 134. maddesinde aramanın konusunu, "*bilgisayar*", "*bilgisayar programları*" ve "*bilgisayar kütükleri*" oluşturmaktadır. Bilgisayar kavramını daha önce açıkladığımızdan burada tekrar etmek istemiyoruz.

Bilgisayar programları, verileri toplayıp yerleştirdikten sonra bunları oto-

---

[79] Aynı hükme 6755 sayılı Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler İle Bazı Kurum ve Kuruluşlara Dair Düzenleme Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 3 maddesinde de yer verilmiştir.

[80] AKSSS'ne göre, "*elkoyma*", veri ya da bilginin kaydedildiği aracın götürülmesi veya verinin bir kopyasının alınmasıdır. Kunter/Yenisey/Nuhoğlu, s. 1101.

matik işleme tabi tutma olanağını veren manyetik sistemler olarak tanımlanmıştır. ***Bilgisayar kütüğü*** ise, İngilizce "*log*"un karşılığı olan ve daha çok internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP no.larını ve diğer erişim bilgilerini depoladıkları veri tabanı olarak ifade edilmektedir. Bu terimi, sabit ya da taşınabilir her türlü veri depolama aracı olarak tanımlayanlar da vardır.[81]

"Şüphelinin kullandığı bilgisayar", şüphelinin herhangi bir nedenle kullanmakta olduğu yahut elinde bulundurduğu bilgisayarı ifade etmektedir. Burada ifade edilmek istenen husus, şüphelinin maliki olduğu bilgisayar değildir.[82] Ancak elbette şüpheli, bilgisayarın maliki de olabilir.

Burada değinmek gerekir ki, çoğu Yargıtay kararlarında bilgisayar, bilgisayar kütüğü yahut programlarında arama dar anlamda ele alınmaktadır. Böylece bilgisayar kasası yahut harddiskin aranması söz konusu olduğunda CMK'nun 134., CD'ler bakımından ise 116. madde hükümlerinin uygulanması gerektiği ileri sürülmektedir. Bu görüşe katılmamız mümkün görünmemektedir.[83] Zira klavye, fare, harddisk gibi yazıcı,[84] joystick yahut CD'ler de bilgisayarın dış

---

81 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 672.

82 Karagülmez, s. 441.

83 "*Mahkeme kararına istinaden yapılan aramada sanığa ait cd'ler ve bilgisayar kasasının muhafaza altına alındığının belirtildiği, aynı gün Sulh Ceza Mahkemesi'nden el koymanın onaylanmasına dair CMK'nın 127/1 maddesi uyarınca karar alındığı ancak, arama sonrası bilgisayarların yedeklemesinin yapılıp şüpheliye verildiğine dair bir ibareye tutanakta yer verilmediği gibi, bilgisayar kütüklerinde arama yapılmasından önce mahkemeden bu hususta karar alınmadığının anlaşıldığı, bu suretle CMK'nın 134. maddesi hükümlerine riayet edilmeyerek bilgisayar kütüklerinde bilirkişi incelemesi yaptırıldığı, bilgisayar kasasında hukuka aykırı yapılan bu arama ve el koyma sonucu elde edilen delillerin de hukuka aykırı yöntemle elde edilmiş delil niteliğinde bulunduğunun anlaşılması karşısında, yalnızca cd'lerin delil olarak kullanılabileceği*…" Yarg. 17. C. D., 2015/23959 E., 2016/6096 K., 28.03.2016., Yarg. 19. C. D., 2015/4634 E., 2015/5522 K., 13.10.2015.

84 "…*Bahse Konu Olayda Elkonulan Brother Marka, Hl-11e72064j3n407530lxtk60c011731072052000 Seri Numaralı Bir Adet Yazıcı, Hp-Photasmart 3210 All-In-One Marka-Regulatory Model Number Sdgob 0501-02 Numaralı Tarayıcı Ve Fotokopi Özellikli Bir Adet Yazıcının 5271 Sayılı Kanunu'nun 134. Maddesi Kapsamında Kalmadığı Ve Yapılan Arama Ve El Koyma İşlemlerinin Usulüne Uygun Gerçekleştirildiği Gözetilmeden, Itirazın Reddi Yerine Yazılı Şekilde Kabulüne Karar Verilmesinde Isabet Görülmediğinden 5271 Sayılı Cmk'nın 309. Maddesi Uyarınca Anılan Kararın Bozulması Lüzumu Kanun Yararına Bozma Talebine Dayanılarak Ihbar Olunmuştur*." Yarg. 15. C. D., 2014/17995 E., 2014/19487 K., 24.11.2014.

donanımı niteliğindedir. Burada şüphelinin herhangi bir eşyasından ziyade, bilgisayarın bir parçası olan ve onun yardımıyla klasik değil dijital delil elde edilmesini sağlayan özel nitelikte bir eşyanın varlığı söz konusudur. Diğer yandan, bilgisayarlar bakımından arama, kopyalama yahut elkoyma işlemlerinin daha sıkı şartlara bağlanmasının gerekçesini oluşturan "*özel hayatın gizliliği*" ilkesi, CD, Flashbellek, yazıcı yahut bu nevi dijital delil kaynakları için de aynı önemde gerekçe oluşturmaktadır. Bu nedenle bu gibi donanımlar bakımından da CMK 134. madde hükümlerinin uygulanması gerektiği kanaatindeyiz.[85] Nitekim AKSSS, arama ve elkoyma yetkisinin internet, telekomünikasyon ağlarıyla yasal olarak erişilebilen diğer sistemler ya da bilgisayar sistemine doğrudan bağlı bulunan veya veri depolama aygıtları için de genişletilebileceğini öngörmektedir.[86] Diğer yandan Adlî ve Önleme Aramaları Yönetmeliği 17. maddesi, 5271 sayılı CMK'nın 134. maddesi ile paralellik taşımakla birlikte, "*bilgisayar ağları, diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları*"nın da aramanın konusu olabileceğini kabul etmiştir.

Diğer bir husus, kişinin kullandığı bilgisayarda, yazılar, resimler, videolar vs. gibi özel hayatı ilgilendiren yüzlerce yahut binlerce doküman bulunabilir. Bu nedenle devlet, "*belki delil bulurum*" anlayışıyla hakim kararıyla da olsa bir kişinin bilgisayarının hafızasında kayıtlı bulunan bütün dosyaları tek tek açıp inceleme yapamaz. Aksi halde bu, CMK m 119'daki düzenlemenin yasakladığı "*toplu arama*"ya benzer nitelikte bir uygulama doğuracaktır.[87] Bu nedenle, yapılacak aramanın bilgisayar kütüğünde mi, bilgisayar programında mı yoksa harddisk yahut bilgisayarın hangi kısmında yapılacağı arama kararında açıkça gösterilmelidir. Aksi takdirde, bilişim sisteminin bir kısmı yahut tamamına hukuka aykırı girilmesi veya orada kalmaya devam edilmesi söz konusu olacaktır. Zira bu olasılıkta, hukuka uygunluk sebebinin sınırlarının aşılması söz konusu olacaktır.

---

85 "*Müşteki Vekilinin Şikayeti Üzerine Başlatılan Soruşturmada, Yalova 1. Sulh Ceza Mahkemesi'nin 08/05/2008 Tarihli, 2008/262 D.İş Sayılı Kararında, Cmk'nın 119. Maddesi Uyarınca Sanık Tarafından Işletilen Işyerinde Arama Yapılmasına Karar Verilmesine Karşın, Aynı Işyerinde Bulunan Bilgisayarlar Üzerinde Arama Yapılabilmesine Olanak Tanıyan Cmk'nın 134. Maddesine Göreverilmiş Bir Arama Kararı Bulunmadığı Anlaşılmakla, Işyerinde Bulunan Bilgisayarlar Üzerinde Yapılan Arama Sonucunda Elkonulan Ve Içerisinde Müşteki Firmaya Ait Lisanssız Yazılımların Olduğu Belirtilen Harddiskler Ve Cd'ler Hukuka Aykırı Delil Niteliğinde Olup Hükme Esas Alınamayacağından, Sanık Hakkında Verilen Beraat Kararı Usul Ve Yasaya Uygun Görülmüştür*." Yarg. 19. C. D., 2015/2163 E., 2015/1439 K., 13.05.2015., Yarg. 19. C. D., 2015/2092 E., 2015/1175 K., 06.05.2015.

86 Ycgk, 2017/16-956 E., 2017/370 K., 26.09.2017

87 Kunter/Yenisey/Nuhoğlu, s. 1099-1100.

Burada konumuz bakımından önemle üzerinde durulması gereken husus, bilgisayar kavramını dar anlamı ile mi yoksa bilişim sistemi özelliği gösteren ve verileri otomatik olarak depolayan, işleyebilen ve kullanabilen diğer sistemleri de içine alacak şekilde geniş yorumlamamız mı gerektiğidir.

Bazı yazarlar, CMK'nun 134. maddesinde "*bilgisayar, bilgisayar programları ve bilgisayar kütükleri*" ifadesi yerine "*bilişim sistemi*" ifadesi kullanılmamasını eleştirmektedir. Zira TCK bakımından günümüz terminolojisine uygun bir ibare kullanılmaktayken, CMK'da aynı yöntem izlenmemiştir.[88] Bu anlamda, bu yazarlara göre kişisel bilgisayarların dışında kullanılan cep telefonları, tablet bilgisayarlar, akıllı televizyonlar, harici hard diskler, flash diskler, hafıza kartları, oyun konsolları, medya oynatıcıları, navigasyon cihazları, CD ve DVD'ler vb. otomatik işlem yapan ve veri depolayabilen tüm cihazların bu kapsamda değerlendirilebilir.[89]

Bazı yazarlar ise, cep telefonu ile bir bilişim suçunun işlenmesi halinde CMK'nun 134 ve 135. maddelerinin uygulanıp uygulanamayacağı hususunu tartışmışlardır. Bu yazarlara göre, cep telefonları bilgisayar özelliği göstermediğinden 134. maddenin uygulanması mümkün değildir. Diğer yandan, aksi kabul edilse bile bu, Anayasa'nın 38/6 maddesine aykırıdır.[90] CMK'nun 135. maddesi de iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin düzenlemeler getirip, ifadeyle bilişim sistemine erişimi sağlayabilen bir koruma tedbiri olmadığından, cep telefonunun aranması mümkün olmayacaktır.[91]

Bir kısım yazar ise, CMK'nun 134. maddesinin, yalnızca bilgisayar ve bilgisayar kütüklerinde yapılacak arama, kopyalama ve el koyma işlemlerinden bahsetmesi nedeniyle bilgisayar dışındaki eşyalar üzerinde yapılacak arama ve el koyma işlemlerinin CMK m. 116 – 129 hükümleri uyarınca yapıldığını, bu nedenle bilgisayarlardan farklı olmak üzere, internet bağlantısı, e-posta haberleşmesi, kelime işlemci programlarının kullanımı, veri saklanması vb. gibi işlemler yapabilen ileri teknoloji cep telefonlarının kolluk amirinin yazılı emriyle aramaya ve el koymaya konu olduğunu ifade etmektedirler. Uygulamadaki bu sorun, temel hak ve özgürlüklere doğrudan zarar verici nitelikte olup, kişilerin kişisel verilerinin ve özel hayatlarının gizliliğine de evrensel hukuka aykırı bir biçimde müdahale anlamına geldiğinden, arama-el koyma

---

88 Dülger, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 672.

89 Dülger, Murat, Volkan, Modoğlu, Gözde, "Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi", Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet ve İletişim Hukuku Uygulama Rehberi, Avrupa Birliği - Avrupa Konseyi Ortak Projesi, www.academia.edu.tr, (Erişim Tarihi: 15.03.2018), s. 112.

90 Any. 38/6) "*Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez*."

91 Taşkın, s. 173-174.

işlemi, cihazın telefon özelliği ile ilgiliyse, örneğin, konuşma veya mesaj kayıtları incelenecekse, bu durumda genel arama hükmü olan CMK m. 119, cihazın bilgisayar özelliği ile ilgiliyse, örneğin, arama motoru, trafik kaydı, e-posta kayıtları vb. incelenecekse, bu durumda özel arama hükmü olan CMK m. 134 uygulanmalıdır.[92] Aksi halde delilin hukuka aykırı elde edilmesi nedeniyle mahkumiyet hükmüne esas alınması da mümkün olmayacaktır.[93]

Kanaatimizce, 134. maddeyi tüm bilişim sistemlerini kapsayacak şekilde

---

[92] Özen/Özocak, s. 70.

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

[93] "*Cumhuriyet Savcısının talimatıyla yapıldığı belirtilen, telefon inceleme tutanağının 20.04.2014 saat 14.10'da düzenlendiği, bu saatten daha önceki bir saatte saat 12.57'de düzenlenen "fotoğraf teşhis tutanağına" göre şüphe üzerine durdurulan sanığın cep telefonunun 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 sebebiyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı gibi*…" Yarg. 17. C. D., 2015/27517 E., 2017/1716 K., 15.02.2017.

"*Bu açıklamalar ışığında; davaya konu olaya gelince, ... Cumhuriyet Başsavcılığı tarafından CMK'nın 119. maddesi uyarınca sanığın işyerinde arama yapılmasına yönelik verilen 26.4.2012 tarihli karar uyarınca yapılan aramada ele geçen harddisklerde kolluk görevlilerince yapılan inceleme sonucu 471 adet film bulunduğundan tespit edildiği ve CMK'nın 134. maddesi uyarınca bilgisayar ve bilgisayar kütükleri üzerinde arama yapılmasına dair hakim tarafından verilmiş bir karar bulunmadığı cihetle, arama sonucu 2 adet harddiskte bulanan 471 adet filmin hukuka aykırı şekilde elde edilmiş delil niteliğinde olması sebebiyle hükme esas alınamayacağı ve atılı suçlamayı kabul etmeyen sanık hakkında hukuka aykırı şeklinde elde edilmiş bu delil dışında mahkumiyetine yeterli başkaca bir delil de bulunmadığı gözetilmeden, beraati yerine yazılı şekilde mahkumiyetine karar verilmesi*…" Yarg. 19. C. D., 2015/11396 E., 2016/1087 K., 02.02.2016.

yorumlamak yahut madde metninde yapılacak değişiklikle bilgisayar ibaresi yerine bilişim sistemi ibaresini getirmek, kanun koyucunun amacıyla örtüşmeyeceği gibi pratik bir faydası da olmayacaktır. Zira ilkin, TCK'nun 243. maddesinde kanun koyucu "*bilişim sistemi*" ibaresini kullanılmaktayken, CMK'da aynı yöntemi izlenmemiştir. Kanun koyucu, 5271 sayılı Kanun düzenlemesinde, aramanın konusunun "*bilgisayar, bilgisayar programları yahut kütükleri*" değil "*bilişim sistemi*" olmasını isteseydi, 5237 sayılı Kanundaki gibi bir tercih yapar ve bunu açıkça ortaya koyardı.

Diğer yandan söz konusu tedbir, özel hayatın gizliliğine oldukça önemli bir sınırlandırma teşkil etmektedir. Zaten kanun koyucunun madde metnindeki şartları kabul etmesinin temel sebebi budur. Özel koruma tedbirlerinin düzenlenmesinde amaçlanan hedef, maddi gerçeğe ulaşılırken müdahale edilen hak ve özgürlüklerin makul ölçüde korunmasıdır. Bir başka ifadeyle, şüphelinin kullandığı bilgisayar dışındaki bir eşyasının aranması makul şüpheyi gerektirmekteyken, 134. maddede kuvvetli şüphe sebepleri aranmaktadır. Bu nedenle özel hayatın korunmasıyla sıkı ilişki içinde olmayan herhangi bir bilişim sisteminin özel olarak düzenlenmesinin de mantıklı bir gerekçesi yoktur. Diğer yandan eğer özel hayat hakkının kullanılmasına bilgisayar kadar hizmet etmeyen ve bilişim sistemi özelliği gösteren diğer araçları da bu kapsamda değerlendirirsek, onların da aranması "*kuvvetli şüphe sebeplerine*" bağlanacak, bu sefer de uygulamada özel hayata ilişkin olmayan tüm bilişim sistemlerinin aranması 116. madde öngörülenlerden çok daha sıkı ve zor şartlara bağlanmış olacaktır. Bu nedenle, cep telefonları gibi bilgisayar özelliği taşıyan ve özel hayat hakkı ile sıkı ilişki içerisinde olan bilişim sistemleri dışındaki sistemler 134. madde kapsamında değerlendirilemeyecektir. Bu husta kıyas yapılması da mümkün olmayacaktır. Zira koruma tedbirleri, temel hak ve özgürlükleri sınırlayıcı nitelikte tedbirler olduklarından, kıyas yasağı geçerli olacaktır.

Koruma Tedbirinin Sınırlarının Aşılması

"*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama*" koruma tedbiri, 5271 sayılı CMK'nun 134. maddesinde düzenlenen ve kanunda belirtilen koşulları oluştuğu takdirde bilişim sistemine girme suçu bakımından hukuka uygunluk sebebi oluşturan bir koruma tedbiridir. İki kurumun kesiştiği nokta ise, bir bilişim sistemi olarak, şüphelinin kullandığı bilgisayar, bilgisayar kütüğü yahut programlarında arama, kopyalama yahut elkoyma işleminin yapılmasıdır. Bu anlamda, 5271 sayılı CMK'nun 134. maddesindeki koşullara bağlı kalındığı sürece, arama, kopyalama ve elkoyma koruma tedbirlerinin hukuka uygun gerçekleştirildiğini ifade etmek mümkündür. Ancak dikkatle üzerinde durulmak gerekir ki, CD, DVD, flash bellek, disket, harici

ve dâhili harddisk, yazıcı, tarayıcı, bilgisayar özelliği içeren noktaları bakımından akıllı telefon gibi araçlar da 134. madde kapsamında arama, kopyalama ve elkoymaya tabi tutulabilecektir. Böylece bu nitelikteki araçlar için de cumhuriyet savcısının istemi üzerine sulh ceza hâkimi karar verecektir.

Yukarıda açıklanan koşullara uyulmaksızın arama, kopyalama yahut elkoyma koruma tedbirlerinin uygulanması, hem hukuka uygunluk sebebinin sınırlarının aşılmasına sebebiyet verecek hem de elde edilen delilin hukuka aykırı olmasına neden olacaktır.

Diğer yandan, yapılacak aramanın bilgisayar kütüğünde mi, bilgisayar programında mı yoksa harddisk yahut bilgisayarın hangi kısmında yapılacağı arama kararında açıkça gösterilmelidir. Aksi takdirde, bilişim sisteminin bir kısmı yahut tamamına hukuka aykırı girilmesi veya orada kalmaya devam edilmesi söz konusu olacaktır. Zira bu olasılıkta, yine hukuka uygunluk sebebinin sınırlarının aşılması söz konusu olacak ve 243. madde gereğince cezai sorumluluğun gündeme gelmesi söz konusu olabilecektir.

Belirtmek gerekir ki, sisteme girmeksizin bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini bir hukuka uygunluk sebebi olmadan teknik araçlarla izlenmesi 243. maddenin 4. fıkrası kapsamında değerlendirilebilir. Zira bu ihtimalde fail, bilişim sistemine girmemekte yahut kalmaya devam etmemektedir. Aksine burada, teknik yöntemlerle verinin içeriğinin takibi ya da öğrenilmesi söz konusudur.[94] Bu nedenle soruşturma yahut kovuşturma makamlarının bir veriye, bilgisayar sistemine girmeksizin ulaşması CMK'nun 140. maddesi şartlarına uygun gerçekleştirilmişse hukuka uygun olacaktır. Böylece, sisteme erişim/girme yahut kalmaya devam etme söz konusu değilse, 134. madde kapsamında bir hukuka uygunluk değerlendirmesi yapmak da söz konusu değildir.

Söz konusu tedbirin uygulanması cumhuriyet savcısının talebi ve hâkim kararına bağlı olduğundan, istisnai haller dışında (668 sayılı OHAL KHK) cumhuriyet savcısına ulaşılamadığı hallerde kolluk amirinin yazılı emri ile bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilemeyecektir. Aksi takdirde, konusu suç teşkil eden bir emir söz konusu olacağından emri yerine getiren ile emri verenin sorumluluğu doğacaktır. (TCK m. 24/3)

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama elkoyma koruma tedbiri, soruşturma aşamasında başvurulabilen bir koruma tedbiridir. Zira 5271 sayılı CMK'nun 134. maddesinde kanun koyucu açıkça, bu tedbire "*bir suç dolayısıyla yapılan soruşturmada*" başvurulabileceğini hüküm altına almıştır.

---

[94] Koca/Üzülmez, s. 520, 522.

Ancak doktrinde, bu şartın dar anlamda yorumlamaması gerektiğini, zira, kovuşturma aşamasında eksik deliller söz konusu ise, elbette bu aşamada da CMK m. 134 uyarınca koruma tedbiri kararı verilebileceğini savunan yazarlar bulunmaktadır.[95] Her ne kadar bazı yazarlar, kamu davasının açılması için gerekli olan "*yeterli şüphe*"nin işlenen fiilden dolayı bir mahkûmiyet kararı verilebilmesi için yeterli olmadığını, bu nedenle kovuşturma aşamasında mahkemenin, delilleri mahkûmiyet hükmü kurmak bakımından yetersiz görmesi ve suçun sübutunun, bilgisayarlarda yapılacak arama, kopyalama ve elkoyma tedbirlerinin alınmasını gerektirmesi halinde, CMK. m.134'teki koruma tedbirine başvurulmasına istem üzerine yahut re'sen başvurulabileceği yönünde gerekçeler sunsalar da[96] ceza muhakemesinde maddi gerçek araştırılırken her ne pahasına olursa olsun maddi gerçeğin araştırılamayacağı kuralının hatırda tutulması gerekmektedir. Diğer yandan, ceza muhakemesine hakim olan temel ilkelerin tümü bir biriyle eşit değerde olup, pratik bir takım ihtiyaçlar nedeniyle birinin diğeri aleyhine genişletilmesi mümkün olmamalıdır. Bu nedenle mahkemenin delil toplanma ve re'sen araştırma yetkisini, hukuk devleti ilkesine uygun olarak yerine getirmesi gerekmektedir. Kanaatimiz, 134. maddenin 1. fıkrasının hatalı düzenlenmesi nedeniyle sanığın kullandığı veya ona ait bilgisayar ya da bilgisayar kürüklerinde arama yapılması olanağının bulunmadığıdır. Zira bu hükmün kovuşturma evresi için de kullanılması, koruma tedbirlerinde kanunilik ilkesine aykırı olup, bunun mümkün olabilmesi için yasal düzenlemeye ihtiyaç bulunmaktadır.[97]

Sonuç

"*Bilişim Sistemine Girme*" suçu, 5237 sayılı TCK'nun 243. maddesinde düzenlenmiş bir suç tipi olup, 5271 sayılı CMK'nun 134. maddesinde düzenlenen "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama,*

[95] Özen, Muharrem; Özocak, Gürkan; Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134), Ankara Barosu Dergisi, 2015/1, s. 62, Şahin, Cumhur, s. 329, Yaşar, Yusuf; Dursun, İsmail; Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri, MÜHFHAD, C: 19, S: 3, 2013, s.9., Baştürk, İhsan, Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma, Fasikül Aylık Hukuk Dergisi, Sayı: 9, Ağustos 2010, (https://jurix.com.tr/article/3286, E.T. 02.03.2018), s. 25.

[96] Yaşar/Dursun, s. 10.

[97] Ünver, Yener; Hakeri, Hakan; Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara, 2017, s. 410.

Ayrıca *bkz*., Kunter, Nurullah; Yenisey, Feridun; Nuhoğlu, Ayşe; Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Beta Basım Yayım Dağıtım, İstanbul, Ekim 2010, s. 1098.

kopyalama ve el koyma" koruma tedbirinin varlığı karşısında, bahse konu suç tipinin ceza muhakemesi hukuku açısındn özellik arz eden bir suç tipi olduğu ifade edilebilir. Zira bahse konu koruma tedbirinin şartlarının varlığı halinde, hukuka aykırılık unsuru gerçekleşeceğinden adı geçen suç tipi oluşmayacaktır.

Bilişim sistemi kavramı yerine bazı ülke mevzuatlarında bilgisayar kelimesinin karşılığı olarak kullanılan "*computer*" sözcüğü tercih edilmiş olsa da daha geniş bir alanı koruma altına alması hasebiyle biz, "*bilişim sistemi*" ifadesinin terminolojik olarak daha doğru olduğu kanaatindeyiz. Zira bilişim sistemi, verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerine sahip olan ve bu fonksiyonları çok yönlü olarak otomatik işlemlere tabi tutma olanağı veren bir sistemdir. Bu yönüyle bilişim sistemi, veri-işleme ve veri-iletme özelliğine sahiptir. Oysa bilgisayar, verileri toplama, saklama, işleme ve yeniden değerlendirme faaliyeti nedeniyle verileri işleme özelliğine sahiptir.

Kavram olarak bilişim sistemi ifadesini tercih etmemizin neticesinde ve "*siber suç*", "*elektronik suç*", "*dijital suç*", "*yüksek teknoloji suçları*", "*bilgisayar suçu*" gibi kavramların da çalışmada belirttiğimiz kimi eksiklikleri barındırması nedeniyle terminolojik olarak "*bilişim suçları*" kavramının tercih edilmesinin isabetli olduğu düşüncesindeyiz.

Bilişim suçlarının doğru anlaşılabilmesi için veri kavramının da doğru bir şekilde tanımlanması önem arz etmektedir. Doktrinde veri, her türlü bilginin, bilgisayarların işlem yapabileceği, sonuçlar üretebileceği, saklayabileceği ve gerektiğinde yeniden okuyabileceği şekilde sayısal birimlere dönüştürülmüş hali olarak tanımlanmıştır. Konumuz yönünden veri kavramı bakımından dikkat edilmesi gereken husus, verinin salt "*bilgisayar/bilişim sistemi verisi*" şeklinde dar anlaşılmaması gerektiği yönündedir. Kanaatimizce bu yorum, TCK'nun 243. maddesinin 3. fıkrasında ifade edilen "*sistemin içerdiği veri*" kavramının, CD, USB yahut taşınabilir bellek gibi bilişim sistemi/bilgisayar dışındaki araçlarda bulunan verileri de kapsamına alacak şekilde anlaşılması sonucunu doğurmaktadır ki, bu yorum suçun düzenlenme amacına da uygun olacaktır. Zira bilişim sistemi yahut bilgisayarlar en temel işlevlerini "*veri*" üzerinden yerine getirmektedir. Bu anlamda, bilgisayarın mütemmim cüzü olmayan ve fakat onun fonksiyonunu yerine getirmesi bakımından neredeyse mütemmim cüz niteliğindeki bir unsuru (veriyi) sağlayan diğer unsurların "*sistem içindeki veri*" olarak yorumlanması mümkündür. Bu anlamda bir bilişim sistemine girilmesiyle, CD, USB yahut taşınabilir bellek gibi araçlarda bulunan verinin yok olması yahut değiştirilmesine neden olunması halinde 243. maddenin 3. fıkrası uygulama alanı bulacaktır. Bu açıdan bakıldığında, 5237 sayılı TCK'nun 243. maddesinde, "*bir bilişim sisteminin bir kısmına*"

girilmesi veya orada kalınmasıyla ifade edilmek istenen bir diğer hususun da bu olduğu ortaya çıkacaktır.

TCK'nun 243. maddesinde yapılan değişiklik sonrasında suç, seçimlik hareketli hale gelmiştir. Zira bilişim sistemine girmek tek başına suçu oluşturmaya yeterli olup, kişinin sisteme girdikten sonra kalmaya devam etmesi aranmamaktadır. Burada dikkat çeken husus, kanun koyucunun burada "*kalan*" ifadesini değil, daha uzun süren bir temadiyi niteleyen "*kalmaya devam eden*" ibaresini tercih etmiş olmasıdır. Suçun değişiklikten önceki halinde yer alan "*kalmaya devam etme*" suçun oluşması bakımından sabit bir sürenin belirlenmesinde bir yorum aracı olarak kullanılmaktaysa da değişiklik sonrasında bu husus, cezanın belirlenmesi ve bireyselleştirilmesinde göz önünde bulundurulacaktır.

Bir diğer husus, "*bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden*" kimsenin cezalandırılacağını düzenleyen 243. maddenin 1. fıkrasında yer alan "*hukuka aykırı olarak*" ibaresinin nasıl yorumlanacağıdır. Aksi yönde düşünen yazarlar bulunmakla birlikte biz, bu nitelikteki ibarelerin varlığı yahut yokluğunun fiilin hukuka aykırılığı üzerinde herhangi bir etki yaratmadığı ve failde özel bir hukuka aykırılık bilincinin aranmasının gerekmediği kanaatindeyiz. Buna göre, CMK md. 134'te düzenlenen "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma*" koruma tedbirinin bilişim sistemine girme suçunda bir hukuka uygunluk nedeni oluşturması bakımından, failde özel bir hukuka aykırılık bilincinin aranmaması gerektiği kanaatindeyiz.

5271 sayılı CMK'nun 134.maddesinde yer verilen "*bilgisayar"* kavramını, dar anlamı ile mi yoksa bilişim sistemi özelliği gösteren ve verileri otomatik olarak depolayan, işleyebilen ve kullanabilen diğer sistemleri de içine alacak şekilde geniş yorumlamamız mı gerektiği de tartışılması gereken bir diğer hususdur. Bu konuda doktrinde, yukarıda ayrıntılı şekilde ifade edildiği üzere çeşitli görüşlere yer verilmiştir.

Kanaatimizce, TCK'nun 243. maddesinde kanun koyucu "*bilişim sistemi*" ibaresini kullanılmaktayken, CMK'da aynı yöntemi izlenmemiştir. Kanun koyucu, 5271 sayılı Kanun düzenlemesinde, aramanın konusunun "*bilgisayar, bilgisayar programları yahut kütükleri*" değil "*bilişim sistemi*" olmasını isteseydi, 5237 sayılı Kanundaki gibi bir tercih yapar ve bunu açıkça ortaya koyardı. Diğer yandan bu hususta kıyas yapılması da mümkün olmayacaktır. Zira koruma tedbirleri, ceza muhakemesi hukukunda temel hak ve özgürlükleri sınırlayıcı nitelikte tedbirler olduklarından, bu tedbirler bakımından kıyas yasağı geçerli olacaktır.

Ayrıca 134. maddeyi tüm bilişim sistemlerini kapsayacak şekilde yorumlamak yahut madde metninde yapılacak değişiklikle bilgisayar ibaresi yerine bilişim sistemi ibaresini getirmek, kanun koyucunun amacıyla örtüşmeyeceği gibi pratik bir faydası da olmayacaktır. Nitekim söz konusu tedbirin, özel hayatın gizliliğine oldukça önemli bir sınırlandırma teşkil etmesi, kanun koyucunun madde metnindeki şartları kabul etmesinde temel sebebi teşkil etmektedir. Bahse konu koruma tedbiri gibi özel nitelikteki koruma tedbirlerinin düzenlenmesinde amaçlanan hedef, maddi gerçeğe ulaşılırken müdahale edilen hak ve özgürlüklerin makul ölçüde korunmasıdır.

Şüphelinin kullandığı bilgisayar dışındaki bir eşyasının aranması, makul şüpheyi gerektirmekteyken, 134. maddenin uygulanabilmesi için kuvvetli şüphe sebeplerinin aranması gerekmektedir. Bu nedenle özel hayatın korunmasıyla sıkı ilişki içinde olmayan herhangi bir bilişim sisteminin, bu ölçüde korunmasının tutarlı bir gerekçesinin bulunmadığı kanaatindeyiz. Diğer yandan eğer özel hayat hakkının kullanılmasına bilgisayar kadar hizmet etmeyen ve bilişim sistemi özelliği gösteren diğer araçları da bu kapsamda değerlendirirsek, onların da aranması "*kuvvetli şüphe sebeplerine*" bağlanacak, bu sefer de uygulamada özel hayata ilişkin olmayan tüm bilişim sistemlerinin aranması 116. madde öngörülenlerden çok daha sıkı ve zor şartlara bağlanmış olacaktır. Bu nedenle, cep telefonları gibi bilgisayar özelliği taşıyan ve özel hayat hakkı ile sıkı ilişki içerisinde olan bilişim sistemleri dışındaki sistemlerin, CMK'nun 134. madde kapsamında değerlendirilmemesi gerektiği düşüncesindeyiz.

Kaynakça

APAYDIN, Cengiz, Bilişim Sistemine Girme Suçu, TAAD, Y:7, S:24, Ocak, 2016,

ARTUK, Mehmet, Emin, GÖKCEN, Ahmet, ALŞAHİN, Mehmet, Emin, ÇAKIR, Kerim, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2017,

AKBULUT, Berrin, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C: 24, S: 2, Y: 2016,

BAŞTÜRK, İhsan, Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma, Fasikül Aylık Hukuk Dergisi, Sayı: 9, Ağustos 2010, (https://jurix.com.tr/article/3286, E.T. 02.03.2018),

CENGİZ, Serkan, DEMİRAĞ, Fahrettin, ERGÜL, Teoman, MCBRİDE, Jeremy, TEZCAN, Durmuş, Avrupa İnsan Hakları Mahkemesi Kararları Işığında Ceza Yargılaması Kurum ve Kavramları, Şen Matbaa,

Ankara, Kasım 2008,
CENTEL, Nur, ZAFER, Hamide, ÇAKMUT, Özlem, Türk Ceza Hukukuna Giriş, Beta Basım Yayım Dağıtım, Eylül, 2014,
DÜLGER, Murat, Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 2013,
DÜLGER, Murat, Volkan, Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması, TAAD, Y:8, S:31, 2017,
DÜLGER, Murat, Volkan, MODOĞLU, Gözde, "Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi", Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet ve İletişim Hukuku Uygulama Rehberi, Avrupa Birliği - Avrupa Konseyi Ortak Projesi, www.academia.edu.tr, (Erişim Tarihi: 15.03.2018),
ERDOĞAN, Yavuz, Bilişim Sistemine Girme ve Kalma Suçu, www.hukuk.deu.edu.tr>6-yavuzerdogan, (Erişim Tarihi: 30.01.2018),
ERSOY, Uğur, Bir Koruma Tedbiri Türü Olarak Şirket Yönetimi İçin Kayyım Tayini (CMK m.133), AÜHFD, 65 (4), 2016,
GÖKCEN, Ahmet, BALCI, Murat, ALŞAHİN, M. Emin, ÇAKIR, Kerim, Ceza Muhakemesi Hukuku II, Adalet Yayınevi, 2018,
GÖKTÜRK, Neslihan, Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon, İnönü Üniversitesi Hukuk Fakültesi Dergisi C:7 S:1, 2016,
KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, 2013,
KARAKEHYA, Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, TBB Dergisi, Sayı 81, 2009,
KATOĞLU, Tuğrul, Ceza Hukukunda Hukuka Aykırılık, Seçkin Yayıncılık, Ankara, 2003,
KOCA, Mahmut, ÜZÜLMEZ, İlhan, Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, Ankara, 2017,
KUNTER, Nurullah, YENİSEY, Feridun, NUHOĞLU, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Beta Basım Yayım Dağıtım, İstanbul, Ekim 2010,
MAHMUTOĞLU, Fatih, Selami, Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, İÜHFM, C:71, Sayı: 1, 2013,
ÖZBEK, Veli, Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Eylül, 2017,
ÖZBEK, Veli, Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, Türk Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ağustos, 2017,

ÖZEN, Muharrem, ÖZOCAK, Gürkan, Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134), Ankara Barosu Dergisi, 2015/1,

ÖZTÜRK, Bahri, TEZCAN, Durmuş, ERDEM, Mustafa, Ruhan, GEZER, SIRMA, Özge, KIRIT, SAYGILAR, Yasemin, ÖZAYDIN, Özdem, AKCAN, ALAN, Esra, TÜTÜNCÜ, ERDEN, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, 2016,

ROSCİNİ, Marco, Digital Evidence as a Means of Proof before the International Court of Justice, Oxford academic, Journal Of Conflict & Security Law, Vol. 21, Iss. 3, 2016,

ŞAHİN, Cumhur, Ceza Muhakemesi Hukuku -I-, Seçkin Yayıncılık, Ağustos 2017,

ŞAHİN, İlyas, Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi, MÜHFHAD, C. 20, S. 3, Y. 2014,

TAŞKIN, Şaban, Cankat, Bilişim Suçları, Beta Basım A.Ş., İstanbul, 2008,

ÜNVER, Yener, HAKERİ, Hakan, Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara, 2017,

YAŞAR, Yusuf, DURSUN, İsmail, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri, MÜHFHAD, C: 19, S: 3, 2013,

YAZICIOĞLU, Yılmaz, Bilgisayar Suçları, Alfa Basım Yayım, Dağıtım, 1997,

YENİSEY, Feridun, PLAGEMANN Gottfried, Alman Ceza Kanunu, Strafgesetzbuch (StGB), İstanbul, Mayıs, 2015,

YILMAZ, Sacit, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, TBBD, S: 92, 2011,

YILMAZ, Zahit, APİŞ, Özge, Karşılıksız Yararlanma Suçu (TCK m.163), Prof. Dr. Nur Centel'e armağan, MÜHFHAD, Y: 2013, C: 19, S: 2,

ZAFER, Hamide, Ceza Hukuku Genel Hükümler TCK m. 1-75, Beta Basım Yayım Dağıtım, Şubat, 2015.