T.C. İSTANBUL KÜLTÜR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRK VE ALMAN HUKUKU'NDA ONLİNE ARAMA

DOKTORA TEZİ

Nilüfer KÖKER
1210030035

Anabilim Dalı: Kamu Hukuku
Program: Kamu Hukuku

Tez Danışmanı: Prof. Dr. Dr. h.c. mult. Bahri ÖZTÜRK

HAZİRAN 2024

T.C. İSTANBUL KÜLTÜR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRK VE ALMAN HUKUKU'NDA ONLİNE ARAMA

DOKTORA TEZİ

Nilüfer KÖKER
1210030035

Anabilim Dalı: Kamu Hukuku
Program: Kamu Hukuku

Tez Danışmanı: Prof. Dr. Dr. h.c. mult. Bahri ÖZTÜRK

Jüri Üyeleri: Prof. Dr. Durmuş TEZCAN
Prof. Dr. Ahmet GÖKCEN
Prof. Dr. Murat BALCI
Doç. Dr. Esra ALAN

HAZİRAN 2024

İçindekiler

İKİNCİ BÖLÜM
ALMAN HUKUK SİSTEMİNDE ONLİNE ARAMANIN
TARİHİ GELİŞİMİ VE MEVCUT YASAL DÜZENLEMELER

ÜÇÜNCÜ BÖLÜM
TÜRK HUKUK SİSTEMİNDE ONLİNE ARAMA-
HUKUKİ ÇERÇEVE, UYGULANABİLİRLİK
İLE ÖNERİLER

Önsöz

Tez konumu öneren, olağanüstü yoğunluğuna rağmen bana vakit ayıran, her zaman bilgi ve tecrübelerinden yararlanma fırsatı bulduğum çok kıymetli danışman hocam saygıdeğer Prof. Dr. Dr. h.c. mult. Bahri ÖZTÜRK'E,

Kıymetli görüş ve dönüşleriyle çalışmama katkı sağlayan Tez İzleme Komitesi Üyeleri saygıdeğer hocalarım Prof. Dr. Durmuş TEZCAN ve Prof. Dr. Murat BALCI ile Tez Jüri Üyeleri saygıdeğer hocalarım Prof. Dr. Ahmet GÖKCEN ve Doç. Dr. Esra ALAN'A,

T.C. İstanbul Kültür Üniversitesi Hukuk Fakültesinin bana kazandırdığı, her daim yanımda olan ve tez çalışmam süresince her sorunuma çözüm bulan canım arkadaşım Dr. Öğr. Üyesi Efser ERDEN TÜTÜNCÜ'ye,

Tez sürecindeki destek, motivasyon ve dayanışmaları için başta Doç. Dr. Münevver MERTOĞLU, Dr. Öğr. Üyesi Muharrem TÜTÜNCÜ, Dr. Akif Hilal ÖZTÜRK, Dr. Beste GEMİCİ FİLİZ, Fatma Aslım HAŞLAMACIOĞLU KATIRCI ve Gülendam SADİ ZEVZİR olmak üzere T.C. İstanbul Kültür Üniversitesi Hukuk Fakültesi ile Adalet Meslek Yüksekokulu'ndaki kıymetli çalışma arkadaşlarıma,

Yetişmemde ve bugünlere gelmemde büyük emeği olan, haklarını hiçbir zaman ödeyemeyeceğim canım annem ve babama,

Yaptığım her seçimde yanımda olan, bana her koşulda desteğini, sevgisini ve güvenini hissettiren, çalışmalarım boyunca fedakarlıkta bulunan kıymetli eşim Berkay KÖKER'e,

Sevgileriyle, yaşamımda olmalarıyla bana enerji veren en değerli varlıklarım, kızlarım Nil KÖKER ve Alin KÖKER'e sonsuz teşekkür ederim.

Haziran, 2024

Nilüfer KÖKER

Kısaltmalar

AB : Avrupa Birliği
AfD : Alternative für Deutschland
AİHS : Avrupa İnsan Hakları Sözleşmesi
AK : Avrupa Konseyi
AY : Anayasa
AYM : Anayasa Mahkemesi
BeckOK : Beck'scher Online-Kommentar
BGB : Bürgerlisches Gesetzbuch
BGH : Bundesgerichtshof
BGHSt : Entscheidungen des Bundesgerichtshofes in Strafsachen
BKA : Bundeskriminalamt
BMJ : Bundesministerium der Justiz
BT : Bilişim Teknolojileri
BT-Drucks : Bundestagsdrucksache
BVERFG : Bundesverfassungsgericht
BVERFGE **:** Bundesverfassungsgerichtsentscheidung
BvR : Bundesverfassungsgericht
CDU : Christlich Demokratische Union
CMK : Ceza Muhakemesi Kanunu
CSU : Christlich Soziale Union
DLL : Dynamic Link Library
DSL : Digital Subscriber Line
DUD : Die Zeitschrift "Datenschutz und Datensicherheit"
EGM : Emniyet Genel Müdürlüğü
ErfK : Erfurter Kommentar
FETÖ : Fettullahçı Terör Örgütü
GG : Grundgesetz
GPS : Global Positioning System
GVG : Gerichtverfassungsgesetz
IBAN : International Bank Account Number

IOCTA : Internet Organised Crime Threat Assessment

IÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

IP : Internet Protokolü

JS : Juristenzeitung

JTK : Jandarma Teşkilat Kanunu

JuS : Juristische Schulung

KK **:** Karlsruher Kommentar

KMR : Kommentar zur Strafprozessordnung

KHK : Kanun Hükmünde Kararname

KriPoZ : Kriminalpolitische Zeitschrift

KVKK : Kişisel verilerin Korunması Kanunu

M : Madde

MİT : Milli İstihbarat Teşkilatı

MİTK **:** Milli İstihbarat Teşkilatı Kanunu

MMS : Multi Media Messaging Service

MüKO : Münchener Kommentar

MvSHS : Medeni ve Siyasi Haklar Sözleşmesi

NStZ : Neue Zeitschrift für Strafrecht

NRW : Nordrhein-Westfalen

NJW : Neue Juristische Wochenzeitung

NZWiSt : Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht

NVwZ : Neue Zeitschrift für Verwaltungsrecht

PAG : Polizeiaufgabengesetz

PDY : Paralel Devlet Yapılanması

PVSK : Polis Vazife ve Salahiyet Kanunu

SIM : Smart Card Indise Mobile Phone

SMS : Short Mesage Service

SPD : Sozialdemokratische Partei Deutschlands

StPO : Strafprozessordnung

StV : Zeitschrift Strafverteidiger

TBMM : Türkiye Büyük Millet Meclisi

TBBD : Türkiye Barolar Birliği Derneği

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

USB : Universal Serial Bus

VoIP : Voice Over Internet Protokol

ZD : Zeitschrift für Datenschutz

ZJS : Zeitschrift für das Juristische Studium

ZIS : Zeitschrift für Internationale Strafrechtswissenschaft

Özet

Gizli bir soruşturma tedbiri olan online arama ile devlet tarafından bilgi teknolojisi sistemlerine uzaktan erişim sağlanarak, veri toplanması amaçlanmaktadır. Bu doğrultuda hakkında tedbir uygulanan kişinin bilgisi olmadan teknik araçlarla sitemine sızılarak, internet bağlantısı üzerinden bilişim sisteminde bulunan tüm verilere erişim sağlanabilir. Online arama özellikle organize suçluluk ve terör örgütleriyle mücadelede önemli bir tedbirdir.

Almanya da gerek istihbari bilgi elde etmek amacıyla, gerekse tehlikeyi önleme ve adli amaçlı uygulanan bu tedbir, Türk Hukuk sisteminde düzenleme altına alınmamıştır.

Bu çalışma ile öncelikle online arama tedbiri hakkında genel bilgiler verilecek olup, online arama kavramına, amacına, bağlantılı olduğu ilkelere, teknik sınırları ile hukuki niteliğine değinilecektir. Devamında ise Alman Hukuk sisteminde online aramanın tarihi gelişimi ile yasal düzenlemeleri ele alınacaktır. Çalışmanın üçüncü ve son bölümünde ise, Türk Hukuk sisteminde online aramanın hukuki çerçevesi incelenecek olup, uygulanabilirliğine ve önerilere yer verilecektir.

Anahtar Kelimeler: Online Arama, Çevrimiçi, Arama, Elkoyma, Bilgisayar

Abstract

Online search, which is a secret investigation measure, aims to collect data by remote access to information technology systems by the state. In this direction, the system can be infiltrated by technical means without the knowledge of the person against whom the measure is applied, and all data in the information system can be accessed via internet connection. Online search is an important measure, particularly in the fight against organised crime and terrorist organisations.

This measure, which is applied in Germany for the purposes of obtaining intelligence information, preventing danger and for judicial purposes, has not been regulated in the Turkish legal system.

In this study, firstly, general information about the online search measure will be given, and the concept of online search, its purpose, the principles to which it is related, its technical limits and its legal nature will be mentioned. Subsequently, the historical development and legal regulations of online search in the German legal system will be discussed. In the third and final part of the study, the legal framework of online search in the Turkish legal system will be analysed, and its applicability and recommendations will be given.

Keywords: Online Search, Online, Search, Seizure, Computer

Giriş

Küreselleşme ve dijitalleşmenin bir sonucu olarak, günümüzde bilgi teknolojisi sistemlerinin kullanımı artmıştır. Akıllı telefonlar, tabletler ve bilgisayarlar günlük yaşamın ayrılmaz bir parçası haline gelmiş olup, sadece iletişim amacıyla değil, aynı zamanda birçok günlük ihtiyacı karşılamak için de kullanılmaktadır. Bilgi ve iletişim teknolojisi sayesinde, bilgi teknolojisi sistemleri özel kullanım, iş dünyası ve bilim için vazgeçilmez veri depolama cihazları haline gelmiştir. Bu sistemler, internet bağlantısı ile çok sayıda uygulama ve platform aracılığıyla çeşitli şekillerde kullanılabildiğinden, internet de hayatın vazgeçilmez bir parçası olmuştur.

Bununla birlikte, modern teknolojilerin yaygın kullanımı aynı zamanda kötüye kullanım riskini de beraberinde getirmektedir. Kullanıcılar, teknolojik gelişmelerden ve buna bağlı olarak veri trafiğindeki muazzam performans ve hızdan memnuniyet duymaktadırlar. Nitekim herhangi bir uzmanlık bilgisi gerekmeden, internetin çalışma şeklini ve buna bağlı riskleri anlamak zorunda kalmadan, herkes küresel internet ağına bağlanabilmektedir. Bu nedenle çoğu kullanıcı internetin tehlikelerinin farkında olmadan, kendisini bu tehlikelere maruz bırakarak, kolayca siber suç mağduru olabilmektedir.

Modern dünyanın sunduğu kazanımlar, bireylerin internet kullanımı yoluyla bu mecrada birçok iz bırakmasının yanı sıra kendisi hakkında da birçok veriyi açığa çıkarmasına katkıda bulunmaktadır. Sosyal ağların kullanımı yoluyla insanlar, kişisel verilerini tanımlanamayan bir kitleyle paylaşmak üzere bilinçli olarak yaymaktadırlar. Akıllı cihazların ve ilgili uygulamaların özel ve profesyonel ortamlarda kullanımı da kişisel veri hacminin hızla artmasına neden olmaktadır. Örneğin, *Alexa* veya *Siri* gibi sesli yardım sistemleri sadece kendisine verilen komutları yerine getirmekle kalmayıp aynı zamanda kullanıcıları hakkında öğrendikleri bilgileri işlemektedirler. Bunun ötesinde örneğin otomobillerde sürücünün ağırlığı, yolcuların koltuk pozisyonu ve benzeri kişisel bilgiler kaydedilmektedir. Bu tür teknolojileri kullanarak, insanlar bilinçli veya bilinçsiz olarak üçüncü taraflarca kullanılabilecek bilgileri erişilebilir kılarlar. Bilgi teknoloji sistemlerinde kişisel bilgi ve veriler sadece saklanmakla kalmaz, bunlar sayesinde, kullanıcıların yaşantılarının adeta bir şablonu oluşturulmak

suretiyle, kapsamlı bir bireysel sosyal, hareket ve faaliyet profili oluşturmak da mümkündür.

Teknolojinin bu avantajlarından yararlanılmak suretiyle yürütülen ceza muhakemelerinde, böylesi profillemeler sayesinde "şeffaflaşan" bir sanık[1] hakkında kolaylıkla muhakeme yürütüleceği düşünülebilirse de meseleyi madalyonun iki yüzünü de gözeterek ele almak gerekmektedir. Zira, suç örgütleri bu küresel bilgi toplumunun gelişmelerinden büyük ölçüde istifade etmektedir. Kaldı ki ceza muhakemesinde yetkili merciler, gözetilmesi zorunlu olan bir takım ceza muhakemesi güvenceleri ile donatılmış tedbirleri uygularken hukukun çizdiği sınırlar içerisinde kalmak mecburiyetindedirler. Suç örgütleri ise teknolojinin sağladığı tüm olanaklardan tabir caiz ise ölçüsüzce faydalanabilmektedirler.

Görüldüğü gibi bilgi ve iletişim teknolojilerindeki gelişmeler soruşturma makamları için yeni zorluklar ortaya çıkarmaktadır. Teknolojik ilerleme nedeniyle bilgi toplama ve soruşturmalar giderek zorlaşmaktadır. Başta terörizmle ilgili olanlar olmak üzere her türlü suçun failleri suçları planlamak ve hazırlamak için bu yeni teknolojileri serbestçe kullanmakta ve suç ortaklarıyla modern veri ağları üzerinden, genellikle şifreleme kullanarak iletişim kurmaktadır. Bu durum hukukun üstünlüğü açısından ciddi tehlikeler ve zorluklar barındırmaktadır. Bu tehditlere karşı koymak amacıyla, bilgi teknolojisi sistemlerine gizli erişim yöntemi olarak bilinen "online arama" tedbiri son yıllarda çeşitli ulusal mevzuatlarda yer almaya başlamıştır. Zira soruşturma makamları yeni teknolojilerin kullanımında geri kalmamak ve bunları etkin bir şekilde kullanmakla yükümlüdür. Veri toplamak için yeni teknolojilerin kullanılması, verimli ve etkili soruşturma çalışmaları için vazgeçilmez bir yöntemdir.

Almanya'da ilk olarak uluslararası terörizmle mücadelede önleyici amaçlarla kullanılmaya başlandıktan sonra, Alman Ceza Muhakemesi Kanunu'na getirilen "online arama" tedbiri ile artık adli amaçla da bu yönteme başvurmak mümkün hale gelmiştir. Özellikle dijital çağın ilerlemesi ve bilgi teknolojileri sistemlerinin önem kazanmasıyla birlikte dijital izlerin sayısı da artmaktadır. Bilgi ve iletişim teknolojisindeki hızlı gelişmeler sebebiyle, soruşturma makamları dijital iz takibinde zorluklarla karşı karşıya gelmekte, arama ve el koyma gibi geleneksel koruma

[1] "Şeffaflaşan" sanık kavramı için bkz, Erişim: BA-AnnamariaNockemann.pdf (hs-mittweida.de), Erişim tarihi: 01.06.2024; Aynı yönde bkz, Erişim: Analyse: Gläserne Menschen per Bundestrojaner? | heise online, Erişim tarihi: 01.06.2024.

tedbirlerine başvurulması yetersiz kalmaktadır. 2017 yılında Alman Ceza Muhakemesi Kanunu'nda adli nitelikte düzenleme altına alınan "online arama" tedbiri ile bilgi teknoloji sistemlerine sızılarak bilgi ve veri toplamak suretiyle dijital iz takibi etkin bir şekilde gerçekleştirilebilmektedir.

Bir gizli soruşturma yöntemi olan bu tedbir, yalnızca gizliliği ve olası süresi nedeniyle değil, özellikle erişime açık verilerin sayısı ve hassasiyeti nedeniyle başta kişilik hakları olmak üzere anayasal temel hak ve özgürlüklere müdahale oluşturduğundan, bu tedbirin amacı ve orantılı olup olmadığı oldukça tartışmalıdır. Burada "online arama"nın, bir yandan tedbire maruz kalanların hakları ve çıkarları ile diğer yandan devletin önleme ve adli amaçlı çıkarları arasında uygun bir denge sağlayıp sağlamadığı sorusu ortaya çıkmaktadır.

Devlet bir yandan teknolojinin ve dijitalleşmenin beraberinde getirdiği değişimlere tepki vermeli, diğer yandan da vatandaşlarının temel hak ve özgürlükleri arasında uygun bir denge sağlamalıdır. Nitekim mutlak özgürlük ve mutlak güvenliğin aynı anda garanti edilemeyeceği açıktır.

Bu çalışmada Alman Hukuku'nda halihazırda yasal düzenlemeye kavuşturulmuş olan online arama tedbiri ile Türk Hukuku'nda Alman Hukuku'ndaki online arama tedbirine benzeyen mevcut gizli soruşturma tedbirleri karşılaştırmalı şekilde incelenecektir. Çalışma üç bölümden oluşmakta olup, birinci bölüm online aramanın tanımı, amacı, bağlantılı olduğu temel hak ve ilkeler, teknik sınırları ile hukuki niteliğini ortaya koymaktadır. Çalışmanın ikinci bölümünde Alman Hukuk sistemindeki online arama tedbiri ele alınacak olup, tedbirin tarihi gelişimi ile bu süreçteki yasal düzenlemeler incelenecektir. Üçüncü bölüm ise öncelikle Türk Hukuk sisteminde henüz açık bir yasal düzenlemeye kavuşturulmamış olan online aramanın, muhtemel yasal dayanağı tartışılarak, Türk Hukukunda uygulanabilirliği irdelenecektir. Ardından Alman Hukuku'ndaki düzenlemenin olumlu ve olumsuz yönleri göz önünde bulundurulmak suretiyle, Türk Hukuku bakımından önerilerde bulunulacaktır.

BİRİNCİ BÖLÜM
ONLINE ARAMA KAVRAMI, ONLINE ARAMANIN AMACI, BAĞLANTILI OLDUĞU TEMEL İLKELER, TEKNİK SINIRLARI İLE HUKUKİ NİTELİĞİ

I. Kavram

Online *(Çevrimiçi[2])* arama devlet tarafından izleme yazılımı kullanılarak iletişim ağları aracılığıyla üçüncü taraf bilgi teknolojisi sistemlerine gizli bir erişim tedbiri olarak tanımlanmaktadır[3].

Bir bilgi teknoloji sistemine gizlice erişmek için mevcut bir internet bağlantısı kullanılır. Bu sayede gerek belirli dosyaların aranması suretiyle sisteme ve dolayısıyla depolanan verilere tek seferlik erişim gerekse yansıtma *(Daten-Spiegelung)* olarak tanımlanan veri taşıyıcısının tamamının bir kopyasının oluşturulması sağlanabilir[4]. Bununla birlikte sabit disk alanlarının ve harici veri taşıyıcılarının şifrelenmiş olduğu hallerde, online arama ile uzun süreli izleme (Daten-*Monitoring)* de mümkündür[5].

Online arama tedbiri, gerek önleyici tedbir *(Praeventivmassnahme*) gerekse adli tedbir olarak (*Repressivmassnahme*) mevzuatta yer almaktadır. Ancak Federal Kriminal Dairesi Kanunu online aramayı, "bilgi teknoloji sistemlerine gizli erişim"

[2] Çalışmanın devamında çevrimiçi yerine "online" kavramı tercih edilecektir.
[3] BT-Drucks 18/12785, s. 46; Meyer-Gossner/Schmidt, §100 b, Rn. 1.
[4] Ulf Buermeyer, Die "Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 4/2007, s. 160.
[5] Buermeyer, s. 160 vd.

olarak tanımlamaktadır *(Federal Kriminal Dairesi Kanunu m. 49)*. Önleyici veya adli amaçlı olup olmadığına bakılmaksızın terimleri ve tanımları incelediğimizde, her ikisinin de üçüncü taraflara ait bir bilişim sistemine, kullanımını izlemek, depolanan içeriği ele geçirerek kaydetmek amacıyla teknik araçlar, özellikle de izleme yazılımları kullanarak gizlice erişimi tanımladığını görmekteyiz[6].

Federal Almanya İçişleri Bakanlığı, online arama yerine online inceleme (*Online-Durchsicht)* ile online izleme (*Online-Überwachung*) terimlerini tercih etmiştir. Online aramaya ilişkin hazırlamış olduğu soru kataloğunda online incelemeyi tek seferlik bir eylem, online izlemeyi ise belirli bir süre boyunca gözetim olarak tanımlamış olup, online izlemenin temel haklara yönelik müdahaleyi derinleşmesini temsil ettiğini ve tedbirin niteliğini önemli ölçüde değiştirmediğini belirtmiştir[7]. Ayrıca her iki tedbirin amaçları bakımından farklılık gösterdikleri, online incelemenin amacının ilgili kişinin geçmişte bilgi teknoloji sistemiyle ne yaptığını araştırmak suretiyle mevcut durumu tespit etmek olduğu, online izlemenin amacının ise yasal olarak tanımlanmış bir süre boyunca ilgili kişinin bilgi teknoloji sistemi kullanımı ile ilgili tüm faaliyetlerinin izlenip kaydedilmesi yönünde olduğu vurgulanmıştır[8]. Bunun sonucunda online arama teriminin, online inceleme ve online izlemeye yönelik genel bir terim olarak kullanıldığı ifade edilmiştir.

Online arama tedbirinin temel hak ve özgürlüklere yönelik ciddi müdahaleler içermesi sebebiyle, bunların gerekçelendirilmesi özellikle orantılılık bakımından yüksek gereksinimlere bağlanmıştır[9]. İzleme tedbirleri özel hayatın gizliliğine ne kadar müdahale ederse, bu gereklilikler o kadar katı olmalıdır. Nihayet, kişiliğin mutlak çekirdek alanı dokunulmazdır[10].

Online arama, bilginin kendi kaderini tayin etme hakkının bağımsız bir ifadesi olarak bilgi teknolojisi sistemlerinin bütünlüğü ve gizliliği temel hakkının korunmasına özellikle ciddi bir müdahale teşkil etmektedir[11].

---

[6] Karlsruher Kommentar, KK-StPO/Henrichs/Weingast, §100b Rn. 3.
[7] Fragenkatalog des Bundesministeriums der Justiz (netzpolitik.org), Erişim tarihi: 01.06.2024.
[8] Bundesinnenministerium beantwortet Fragen zur Online-Durchsuchung (netzpolitik.org), Erişim tarihi: 01.06.2024.
[9] BT-Drucks 18/12785, s. 46
[10] BVerfG, 20.04.2016 – 1 BvR 966/09.
[11] BT-Drucks 18/12785, s. 54; Meyer-Gossner, Lutz/Schmitt-Bertram, Strafprozessordnung: StPO – Gerichtsverfassungsgesetz, Nebengesetz und ergaenzende Bestimmungen, 65. Auflage, C.H.Beck, München 2022. § 100b, Rn. 1.

II. Amaç

Bilgi teknolojisinin giderek gelişmesi bilgi teknoloji sistemlerinin insanların hayatlarının neredeyse her alanında yer edinmelerine ve vazgeçilmez olmalarına yol açmıştır. Bu durum özellikle akıllı telefon, tablet veya bilgisayarların kullanımı için geçerlidir. Bu tür cihazların gerek performansları gerekse hafıza (RAM) ve buna bağlı bulut ("Cloud") olarak adlandırılan harici depolama ortamlarının kapasitesi artmıştır[12]. Bunun sonucunda mobil cihazların kullanımı giderek geleneksel telekomünikasyon biçimlerinin yerini almaktadır. Bu çerçevede internet bir yandan bilgi teknoloji sistemi kullanıcılarına ağa bağlı diğer sistemler tarafından alınmaya hazır tutulan muazzam bir bilgi zenginliğine erişim sağlarken, diğer taraftan kullanıcılarına aktif olarak sosyal bağlantılar kurmalarını ve sürdürmelerini sağlayan çok sayıda yeni iletişim hizmetleri sunar[13].

Bilgi teknolojisi sistemlerinin yaygın kullanımı, suçların önlenmesi ve soruşturulmasında da önemli bir rol oynadıkları anlamına gelmektedir. Başta uluslararası terörizmle mücadele etmek için önleyici amaçlarla uygulamaya konulan online arama tedbiri, sonrasında soruşturma makamlarına başkaca amaçlarla ve bilhassa adli amaçlı kullanımı için de yeni olanaklar yaratmaya başlamıştır.

Dijital çağ ilerledikçe ve bilgi teknolojisi sistemlerinin önemi arttıkça, dijital izlerin önemi de artmaktadır. Bu nedenle örneğin konuşulan sözler, gönderilen mesajlar ve e-postalar gibi iletilen ve diğer geleneksel teknik araçlarla okunabilen verilerin yanı sıra, soruşturma makamları isim listeleri, planlama belgeleri, konum bilgileri vb. gibi yalnızca depolanan verileri de analiz etmek gerekmektedir. Ancak bu bilgi teknoloji sistemlerinin verilerine, gizli bir erişimi gerektirir[14]. Sonuç olarak teknolojik ilerleme nedeniyle bilgilerin toplanması ve soruşturmaların yürütülmesi

[12]Fredrik, Roggan, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektroniische Überwachungsmaßnahme mit Risiken für Beschuldigte und die Allgemeinheit. In: Strafverteidiger (StV) 2017, Nr. 12, s. 825.
[13] BT-Drucks 18/12785, s. 46.
[14] Hartmut Pohl, Zur Technik der heimlichen Online-Durchsuchung, DuD 31/2017 S. 684

giderek zorlaşmakla kalmamakta[15], aynı zamanda bu ilerleme bazı durumlarda mevcut soruşturma araçlarının sınırlarını zorlamaktadır[16].

Arama ve elkoyma gibi geleneksel koruma tedbirleri bakımından, her ne kadar donanım veya harici veri taşıyıcılarına el konulması ve içerdikleri verilerin okunması mümkün olsa da[17] bunlar açık bir şekilde gerçekleştirildiğinden soruşturma taktikleri açısından örneğin delillerin yok edilmesi gibi dezavantajlar doğurabilir[18]. Ayrıca kullanıcı davranışı yalnızca el koyma zamanına kadar analiz edilebilir, bu da sistemin yalnızca anlık bir görüntüsünün görüntülenebileceği anlamına gelir[19]. Bunun dışında veri taşıyıcılarındaki verilerin elde edilmesi geleneksel soruşturma araçlarıyla her zaman çözümlenememekte; örneğin silinen veriler kurtarılamamakta veya harici veri taşıyıcılarındaki veriler bulunamamaktadır. Şifreleme yazılımının kullanımının engellenemediği hallerde ise geleneksel el koyma tedbiriyle bu veri taşıyıcılarının analiz edilmesi genelde imkansızdır[20].

Telekomünikasyon yoluyla yapılan iletişiminin geleneksel şekilde denetlemesi bakımından ise her türlü haberleşmenin tespit edilmesi, gizli bir şekilde dinlenmesi, kayda alınması veya sinyal bilgilerinin değerlendirilmesi mümkündür. Buna karşılık online arama ile devam eden bir iletişime değil, aynı zamanda bir bilgi teknoloji sisteminde depolanan tüm verilere erişilebilmesi mümkündür[21].

Online arama ile gerçekleşen müdahalenin boyutunun çeşitli açılardan geleneksel telekomünikasyon yoluyla yapılan iletişimin denetlenmesinden çok daha ciddi olduğu vurgulanmalıdır. Zira online arama gizlice ve zamana yayılmış şekilde uzun bir süre gerçekleştirilebilir. Bu şekilde tüm veriler kayıt altına alınabildiğinden, tedbirin uygulandığı sistemi kullanan kişinin tüm kullanım davranışı izlenebilir[22] ve kapsamlı kişilik profili oluşturulabilir[23].

---

[15] BVerfG, NJW 2008, 829.
[16] BT-Drucks 365(08); s. 1, 5.
[17] Lisa Blechschmitt, Strafverfolgung im digitalen Zeitalter: Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, 363 vd.
[18]Manfred Hofmann, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?"NStZ 2005, 123 vd.
[19] Buermeyer, HRRS 2007, S. 158.
[20] Arndt Sinn, Sinn, Arndt, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334,), 2017, s. 2.
[21] Thomas Knierim/Anna Oehmichen in: Beck/Geisler, Gesamtes Strafrecht aktuell, 1. Auflage 2018, Kapitel 20: Quellen-TKÜ und Online Durchsuchung, 2018. §100b, Rn. 59.
[22] Meyer-Gossner/Schmitt, §100b, Rn. 1.
[23] BVerfG 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833 vd; Grossmann, GA 2018, 433.

Bu doğrultuda online aramanın amacı, üçüncü taraf bilgi teknolojisi sisteminin kullanımını gizlice izlemek, depolanan içeriği kaydetmek ve bu bilgileri soruşturma makamlarına üzerindeki şifreleme tekniklerini aşarak analiz etmek üzere internet aracılığıyla iletmektir[24]. Günümüz bilgi ve iletişim teknolojilerindeki gelişmelerle daha fazla mücadele edebilmek için dijital verilerin elde edilmesi ve değerlendirilmesi bakımından online arama gibi yeni tedbirlere başvurulması vazgeçilmez bir nitelik taşımaktadır. Tedbirin amacına ulaşabilmesi için en önemli husus ise verilerin şifrelenmeden veya internette herhangi bir iz bırakılmayarak gizlenmesinden önce elde edilmesidir[25].

III. Tedbirin Bağlantılı Olduğu Temel Haklar ve İlkeler

Toplumda suçun önlenmesi veya suç işlendikten sonra suçun delillerinin ve faillerinin ortaya çıkarılması için bazı önlemlerin alınması gerekmektedir. Bunların bir kısmı, suç işlenmeden önce suçun veya tehlikenin önlenmesine hizmet eden önleyici tedbirlerdir. Bir kısmı ise suç işlendikten sonra şüphe sebeplerinin aranması ve delillerin elde edilmesi ve muhafazasına yönelik koruyucu tedbirlerdir[26]. Online arama tedbiri de hem suç işlenmesinin önlenmesi hem de işlenmiş suçlarla ilgili muhakeme süreçlerinde önemli role sahip olan bir koruma tedbiridir[27].

Amacı maddi gerçeğe ortaya çıkarmak olan ceza muhakemesinde bu tedbirlere başvurulup, örneğin şüphelinin hazır bulunmasını, delillerin karartılmamasını, hükmün yerine getirilmesini sağlamak suretiyle süjelere ve eşyalara zorlayıcı bir takım tedbirler uygulanması gerekebilir. Ancak bunun neticesinde tedbire maruz kalan kişinin, anayasa ile güvence altına alınmış, bireylerin birbirleriyle, toplumla veya devletle olan ilişkilerinde sahip oldukları haklar olarak tanımlanan temel hak ve özgürlüklerine müdahale söz konusu olabilmektedir. Zira koruma tedbirleri nitelikleri

[24]Rückert in: Münchener Kommentar zur StPO 2. Auflage, 2023 (MüKO StPO/Rückert), §100b, Rn. 1.

[25] KMR StPO/Baer, §100b, Rn. 2.

[26] Feridun, Yenisey, Uygulanan ve Olması Gereken Ceza Muhakemesi Hukukunda Hazırlık Soruşturması ve Polis, Beta Basın Yayım Dağıtım, İstanbul, 1996, s. 152.

[27] Çalışmanın devamında inceleyeceğimiz gibi Alman Hukuk sisteminde online arama hem adli amaçlı hem önleme amaçlı düzenleme altına alınmıştır.

itibariyle kişilerin bir veya birden çok temel hak ve özgürlüğüne müdahale teşkil etmektedir[28]. Bu nedenle maddi gerçeği ortaya çıkarmaya ve adaleti tesis etmeye çalışırken, kişilerin haklarına saygı gösterilerek adil bir muhakeme yürütülmelidir. Gerek soruşturma gerekse kovuşturma evresinde kişilerin haklarının korunması bakımından adil bir muhakemenin gerçekleştirilebilmesi için bazı temel ilkelerin dikkate alınması gerekir[29].

Özellikle kişilerin özel ve aile hayatlarına ağır bir müdahale teşkil eden online arama bakımından da ceza muhakemesinde korunması ve gözetilmesi gereken temel hak ve ilkelere uygunluk değerlendirmesinde bulunulması gerekmektedir. Çalışmanın bu kısmında online arama tedbiriyle bağlantılı olan temel hak ve ilkeler, söz konusu tedbirin amaçları da gözetilmek suretiyle irdelenecektir. Ancak bahse konu temel hak ve ilkeler bağlamında somut önerilerimize çalışmanın son bölümünde detaylıca yer verileceğinden, bu başlık altında yalnızca genel açıklamalarda bulunulmakla yetinilecektir.

A. Hukuk Devleti İlkesi

Hukuk devlet ilkesi, 1982 Anayasası'nın 2'nci maddesinde Cumhuriyetin nitelikleri arasında yer almaktadır. En kısa tanımıyla hukuk devleti, faaliyetlerinde hukuk kurallarına bağlı olan, vatandaşlarına hukuki güvenlik sağlayan devlet olarak tanımlanabilir[30]. Bu bağlamda, hukuk devletinin, insan vakar ve haysiyetine saygı duyan, insan haysiyetine en yüksek değeri veren, insanı devletleştirmek yerine devleti insanlaştırmaya çalışan bir anlayışa sahip olması gerektiği ifade edilir[31]. Bu nedenle hukuk devleti, insan hakları ile ilgili tüm ilkelerin anası ve kaynağı olarak kabul

[28] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi, s. 449; Taner, Ceza Muhakemeleri Usulü, 3. Bası, İstanbul 1995, s. 131 vd.
[29] Ahmet Gökçen/Murat Balcı/Mehmet Emin Alşahin/ Kerim Çakır, Ceza Muhakemesi Hukuku, Adalet Yayınevi, 6. Baskı, Ankara, 2022, s. 113.
[30] Mert Gümüşay, Türk Hukukunda Adli ve Önleme Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, 2009, s. 14.
[31] Turhan Tufan Yüce, Ceza Muhakemesinde Hukuk Devleti Esasları, Ankara Barosu Dergisi, Sayı:5, Yıl:1968, s. 5.

edilir[32]. İnsana güvenlik içerisinde özgür ve onurlu bir ortamda hayat sunan devletin hukuk devleti olduğu vurgulanır[33].

Anayasa Mahkemesi de birçok kararında hukuk devletini tanımlamıştır. Buna göre hukuk devleti, *"insan haklarına saygılı ve bu hakları koruyan, toplum hayatında adalete ve eşitliğe uygun bir hukuk düzeni kuran, bu düzeni sürdürmekle kendini yükümlü sayan, tüm davranışlarında hukuk kurallarına ve anayasaya uyan, eylem ve işlemleri yargı denetimine bağlı olan devlet"*tir[34]. Bu tanımdan da anlaşılabileceği üzere, hukuk devleti ilkesinin işleyebilmesi için devletin karar ve eylemlerinin yargı denetimine tabi olması gerekir. Hukuk devletinin faaliyetlerinde hukuk kurallarına bağlı olması, vatandaşlarına hukuki güvenceler sağlaması ve yasama, yürütme ve yargı erklerinden oluşması sebebiyle, hukuk devletinin üç temel gereği olduğu belirtilebilir. Bunlar, yasama, yürütme ve yargı organlarının hukuka bağlı olmasıdır.

Hukuk devleti ilkesi gereği, millet adına yasama, yürütme ve yargı gücünü kullanan bu anayasal organlar, bu yetkilerini ancak hukukun genel ilkeleri, Anayasa ve kanunlar çerçevesinde insan onurunu korumak, insan hakları ile temel hak ve hürriyetleri gerçekleştirmek, adaleti ve hukuk güvenliği ve hukuki belirliliği sağlamak amacıyla kullanılabilirler[35]. Ancak hukuk devletinin temelinde kuvvet ile hukuk arasında karmaşık ve zorunlu bir bağlantı bulunduğu da ifade edilmelidir. Bu anlamda hukuk devleti, kural koyucuların ve kural uygulayıcıların devletin hukuk sisteminin kurallarına kendiliklerinden uymaları, uymamaları durumunda ise yasal bağlamın izin verdiği ölçüde uymaya zorlanmaları anlamına gelir[36]. Hukuk düzenindeki normlar hiyerarşisini dikkate aldığımızda, tabandaki alt normlarda kuvvetin hukukun hizmetinde, en üst normlarda ise hukukun kuvvetin hizmetinde olduğu ileri sürülür. Başka bir deyişle, bir hukuk sisteminde, bir dizi kurala uyulmasını sağlamak için

[32] Bahri Öztürk/Durmuş Tezcan/Mustafa Ruhan Erdem/Özge Sırma Gezer/Yasemin F. Saygılar/Esra Alan/Efser Erden Tütüncü/Özdem Özaydın/Mehmet Can Tok, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 17. Baskı, Ankara, 2023, s. 113; Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 114.

[33] Yargıtay 7. CD. 20.06.2005 tarihli, 13539/8098 sayılı karar gereği, *"devlet, vatandaşına her an gözaltına alınabileceği, sorgulanabileceği, evinde arama yapılabileceği endişesini yaşatmamalıdır."*; Yener Ünver/Hakan Hakeri, Ceza Muhakemesi Hukuku, 19. Baskı, Adalet Yayınevi, 2002, s. 53.

[34] AYM 10.02.2016 Tarihli ve 18/12 Sayılı karar; AYM 29.01.1980 tarihli ve E. 1979/38, 1980/11 sayılı karar; AYM 25.05.1976 tarihli ve E. 1976/1, 1976/28 sayılı karar; AYM 21.06 1991 Tarihli ve E: 1990/20, 1991/17 sayılı karar.

[35] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 114; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 113.

[36] Zeki Hafızoğulları, Ceza Normu, Normatif Bir Yapı Olarak Ceza Hukuku Düzeni, Ankara 1996, s .157 vd.

aşağıdan yukarıya doğru zorlayıcı bir güç bulunurken; yukarıdan aşağıya doğru, kuvvetin de tabi olduğu bir kurallar sisteminin olduğu ifade edilir[37].

Yukarıda yer alan hukuk devleti tanımları ve açıklamalar bir bütün halinde değerlendirildiğinde, hukuk devletinin, insan haklarının gerçekleştirilmesi, adaletin sağlanması ve güvenliğin temin edilmesi olmak üzere üç temel esastan oluştuğu ifade edilebilir[38]. Zira bir hukuk devletinin temel görevi, insan haklarına dayalı, adil ve güvenli bir toplumsal düzen yaratmak ve bunu kesintisiz olarak sürdürebilmektir.

İnsan haklarının gerçekleştirilmesi bakımından, öncelikle insan hakları tanımlanmalıdır. Irk, renk, cins, dil, din, siyasi veya diğer herhangi bir akide, milli veya sosyal menşe, servet veya diğer herhangi bir fark gözetilmeksizin, insanın onurunu korumayı ve insanın maddi ve manevi gelişimini amaçlayan, bireylerin insan olmaları sebebiyle kazandıkları haklar insan haklarıdır[39]. İnsan haklarının teoride kalmayıp, uygulamada gerçekleştirildiği devletlerin hukuk devleti niteliği taşıdığı belirtilmelidir[40].

Adaletin sağlanmasına yönelik öncelikle adalet kavramının tanımını yapmak gerekirse, adalet, herkesin fırsat eşitliğinin bulunması ve herkesin yasa önünde eşit sayılması gerektiği anlamına gelir. Bununla birlikte bireylere kişiliklerini geliştirme fırsatının verilmesini ve bu amaca aykırılık teşkil eden bütün maddi ve manevi engellerin ortadan kaldırılıp, keyfiliğe izin verilmemesini ifade eder[41]. Bu surette adil nitelikteki devletin hukuk devleti olduğu söylenebilir.

Hukuk devletinin üçüncü sütunu olarak kabul edilen güvenliğin temin edilmesi bakımından ise ancak güvenliği ve sosyal düzeni sağlayan devletlerin hukuk devleti olarak tanımlanabileceği vurgulanmalıdır. Devletin kişilerin ve toplumun refah, huzur ve mutluluğunu sağlama görevi vardır. Bu amaçla devlet, kamu güvenliği ve düzenini sağlar. Bu bağlamda güvenliği sağlayan kolluk güçleri ile jandarmanın önemi ile yargılama bakımından soruşturma ve kovuşturma organlarının önemi vurgulanmalıdır[42].

Nihayet, temel hak ve özgürlükleri korunmak ve bu korumayı fiilen gerçekleştirmek bir hukuk devletinin asli görevlerindendir. Fakat ifade edilmelidir ki

[37] Hafızoğulları, s .157 vd.
[38] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 113.
[39] Durmuş Tezcan / Mustafa Ruhan Erdem/Oğuz Sancakdar/ Rıfat Murat Önok, İnsan Hakları El kitabı, 9. Baskı, 2021, s. 31.
[40] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 113.
[41] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 114.
[42] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 115.

bu temel hak ve hürriyetlerin devlet ve toplum düzeninin sağlanması amacıyla sınırlandırılması mümkündür. Bu sınırlandırma anayasada ve kanunlarda öngörülen esaslar çerçevesinde yapılır ve bu aşamada hukuk devleti ilkesinden kaynaklanan ölçülülük ilkesi de daima dikkate alınmalıdır[43]. Ölçülülük ilkesi, ceza muhakemesi işleminin yapılması ile sağlanması beklenen yarar ile verilmesi ihtimal dahilinde olan zarar arasında makul bir oranın bulunmasını, oransızlık durumunda işlemin yapılmamasını ifade eder[44]. Bu tanımdan anlaşılacağı üzere, oranlılık ilkesi uyarınca, iki menfaat arasında makul bir oranın bulunmamasına rağmen bir tedbirin uygulanması, işlemin hukuka aykırılığı sonucunu doğurur.

Ceza muhakemesi hukuku bakımından hukuk devleti ilkesinin diğer bir önemi ise bağımsız hakimler huzurunda gerçekleştirilecek yargılamanın açık temel kurallara göre adil bir şekilde uygulanması ve böylelikle temel hakların güvence altına alınmasıdır[45]. Hukuk devletinin etkin bir şekilde işleyebilmesi için yargı bağımsızlığı, tarafsızlık ve hâkim güvencelerinin gerçek anlamda uygulanması gerekmektedir[46].

Bununla birlikte yürütmenin eylem ve işlemlerinin bağımsız yargı organlarınca denetlenip denetlenememesi, hukuk devletinin en önemli gerekliliklerinden biridir. Yürütmenin eylem ve işlemlerinin yargı denetimi dışında bırakılması halinde, hukuk devleti ilkesi önemli ölçüde zedelenecektir[47]. Bu hususlar göz önünde bulundurulduğunda, hukuk devletinin bir gereği olarak gizli soruşturma tedbirlerinden olan online arama tedbiri hakkında uygulanan veya bu tedbirin uygulanmasından üçüncü kişi olarak etkilenen kişilere, tedbiri denetleme ve buna karşı korunma olanağı verilmelidir. Türkiye Cumhuriyeti Anayasası bu güvenceyi, *"Yargı Yolu"* başlıklı 125'inci maddesinde idarenin her türlü eylem ve işlemlerine karşı yargı yolunun açık olduğunu hüküm altına alarak karşılamıştır. Ayrıca temel hak ve hürriyetlerin korunması başlığını taşıyan Anayasa'nın 40'ıncı maddesi gereği, *"Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkına sahiptir. Devlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır."*

[43] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 115.
[44] Löwe/Rosenberg, Einl. Kap. 6. 10-12; Öztürk/Tezcan/Erdem, s. 116; Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 116.
[45] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 54.
[46] Bülent Tanör/Necmi Yüzbaşıoğlu, 1982 Anayasasına Göre Türk Anayasa Hukuku, İstanbul 2002, s.100.
[47] Ergun Özbudun, Türk Anayasa Hukuku, İstanbul 2001, s. 92.

Bu doğrultuda, online arama tedbirine hukuk sistemimiz içerisinde yer verildiği takdirde, bu tedbirin uygulanmasından sonra denetlenebilmesine olanak veren yasal düzenlemelerin de getirilmesi bir zorunluluktur. Zira niteliği gereği gizli olarak başvurulan online arama sonucu bilgi teknoloji sisteminde depolanmış tüm veriler elde edilebilmektedir. Bunun sonucunda tedbirin yöneltildiği sistemi kullanan bir kişinin tüm kullanım faaliyetleri izlenebilir[48] ve kapsamlı kişilik profilleri oluşturulabilir[49]. Bu nedenle hakkında bu tedbir uygulanan kişilerin, tedbirin sona ermesinden sonra bilgilendirilmesi ve uygulanan tedbir hakkında denetim olanağına sahip olması zaruridir. Ayrıca hakkında bu tedbirin uygulandığı konusunda şüphe duyan kimseler bakımından da bir başvuru mekanizması oluşturulmasında fayda bulunmaktadır.

Sonuç olarak online arama tedbirinin hukuk devleti ilkesi bakımından ifade ettiği en önemli husus, bu tedbirin Anayasa ve kanunlar çerçevesinde insan haysiyetini korumak, temel hak ve hürriyetleri gerçekleştirmek, adalet ve hukuk güvenliğini sağlamak suretiyle uygulanmasıdır. Online arama tedbiri başta özel hayatın gizliliği, haberleşme gizliliği ve kişisel verilerin gizliliği olmak üzere birçok temel hak ve özgürlüğe sınırlamalar getirmektedir. Bu sebeple online aramaya başvurularak temel hak ve özgürlüklere yapılan müdahalelerin, hukuk devletini fiilen gerçekleştirme amacına uygun olmasına özen gösterilmelidir.

B. İnsan Haysiyetinin Korunması (Dokunulmazlığı) İlkesi

Federal Almanya Anayasası gereği insan haysiyeti korunan en yüksek hukuksal değerdir[50]. Federal Alman Anayasası'nın 1'inci maddesinde[51] yer alan bu ilke, başta temel hakların yorumlanması olmak üzere Anayasa'nın diğer tüm hükümlerine de sirayet eden temel anayasal ilkelerden birisidir[52]. Bu madde, herkesin hayatının değerli

[48] Meyer-Gossner/Schmitt, §100b, Rn. 1.
[49] BVerfG 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833 ff; Grossmann, GA 2018, 433.
[50] BVerfGE 6, 32 (41) = NJW 1957, 297; BeckOK GG/Hillgruber GG Art. 1 Rn. 1.
[51] Federal Almanya Anayasası'nın 1'inci maddesi – İnsanın haysiyetinin korunması
"(1) İnsanın onur ve haysiyeti dokunulmazdır. Tüm devlet erki ona saygı göstermek ve onu korumakla yükümlüdür.
(2) Alman Milleti, bu nedenle dokunulmaz ve devredilmez insan haklarını, yeryüzünde her insan topluluğunun, barışın ve adaletin temeli olarak kabul eder.
(3) Aşağıda belirlenen temel haklar, yasama, yürütme ve yargı organlarını doğrudan doğruya bağlar."
[52] BVerfGE 6, 32 (36) = NJW 1957, 297; BVerfGE 109 (133, 149) = NJW 2004, 739.

olduğunu ve genç veya yaşlı, ekonomik durumu iyi veya kötü, Alman vatandaşı olan veya olmayan fark etmeksizin her bireyin haysiyetinin korunması gerektiğini kabul eder.

Federal Almanya Anayasası'nın insan haysiyetinin dokunulmazlığını ilk maddede güvence altına almasının başlıca sebebi, Almanya'nın tarihine dayanmakta olup, devletin "düşünsel-tarihsel" köklerini görselleştirmektedir. İnsan haysiyetine ve devredilemez insan haklarına bağlılık, kendisini nasyonal sosyalist adaletsizlik rejiminden keskin bir şekilde ayırma istemine, doğal hukuk geleneğine ve 26 Ağustos 1789 tarihli Fransız İnsan Hakları Beyannamesi'ne dayanmaktadır[53]. İnsan haysiyetinin güvence altına alınmasının sadece etik bir taahhüt olmadığı, aynı zamanda anayasal kimliğin bir parçası olan, göreceleştirilemeyen "yol gösterici bir karar" niteliği taşıyan objektif bir anayasa hukuku normu olduğu konusunda görüş birliği olduğu söylenebilir[54]. Bu doğrultuda temel hak ve özgürlükler, insan haysiyetinin korunması adına gerekli görüldükleri için hepsinin temelinde yatan ortak düşünce olan insan haysiyetinden kaynaklanırlar ve insan haysiyetinin bağımsızlaşmış parçaları olarak kabul görürler[55].

Türkiye Cumhuriyeti Anayasası'nda doğrudan insan haysiyetinin dokunulmazlığı ilkesi başlığı altında bir düzenleme bulunmasa da "devletin temel amaç ve görevleri" başlıklı 5'inci maddesinde bu ilkenin dolaylı şekilde düzenleme altına alındığı ifade edilebilir. Buna göre, *"Devletin temel amaç ve görevleri, Türk milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır."* Ayrıca Anayasa'nın 17'nci maddesinin 3'üncü fıkrasında, *"Kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tabi tutulamaz."* şeklinde bir düzenlemeye yer verilerek, insan haysiyetinin önemi vurgulanmıştır. Önemle ifade edilmelidir ki Türkiye Cumhuriyeti Anayasası burada "kimse" kelimesini kullanmak suretiyle, ırk, din, dil ve benzeri

[53] ErfK/Schmidt GG Art. 1 Rn. 1.
[54] BVerfG 15.12.2015, NJW 2016, 1149.
[55] Gören, Zafer, Anayasa Hukukuna Giriş, İzmir 1997, s. 376.

şekillerde ayrım yapmaksızın herkesin haysiyetinin korunmasının önemini belirtmiştir[56].

Anayasa ve kanunlarda tanımlanmamış olsa da öğretide insan haysiyeti, kişiye, bilinçli olma, kendi kaderini tayin etme ve çevresini şekillendirme yeteneği veren kişiliksizliği ortadan kaldıran manevi güç olarak tanımlanmıştır[57]. İnsan haysiyeti insanı bir obje ve bir araç derecesine indirmeyi yasaklar[58]; onun bizzat amaç sayılmasını, bu amaca uygun işlem görmesini sağlar[59]. İnsanın hakları ve yükümlülükleri olan bir hukuk süjesi olduğu ve ancak belirli hak ve özgürlüklere sahip olan bir kişinin çevresini şekillendirebileceği belirtilmektedir. Bu bağlamda insan haysiyetinin, özgürlükçü demokrasilerin, hukuk devletinin işlevini sağlayabilmesi bakımından vazgeçilmez bir koşul olduğu ifade edilir[60]. İnsan haysiyetinin dokunulmazlığı ilkesi hukuk devletinin gereği[61] olması nedeniyle, insan haysiyetinin en yüksek değer olarak anlaşılmadığı toplumların demokratik hukuk devleti olduğu kabul edilemez.

Türk ceza hukuku mevzuatı incelendiğinde, kimi düzenlemelerde dolaylı dahi olsa *"insan haysiyetine aykırı"* işlemlerden bahsedildiğini görmekteyiz. CMK m. 148/1 gereği, şüpheli ve sanığın iradesini özgür olmaktan çıkaran usuller yasaklanmakta ve insan haysiyetine aykırı bir işleme ve bunun neticesinde elde edilecek delillerin yargılamada kullanılmasına gösterilecek rızayı kabul etmemektedir. TCK'nın 94'üncü, 95'inci ve 96'ncı maddelerinde ise hukuka aykırı fiil olan ve insan haysiyetini ihlal eden işkence ve eziyet fiilleri suç olarak düzenleme altına alınmıştır. Benzer şekilde TCK m. 125'te onur, şeref ve saygınlığa saldırı teşkil eden hakaret fiili bir suç olarak düzenlenmiştir[62]. Bu düzenlemelerin sonucunda, ilk bakışta ahlaki bir değer niteliğinde görünen insan haysiyetinin bağlayıcı bir hukuki değer olduğu belirtilmelidir[63]. Özetle, bu ilkenin ihlali söz konusu olduğunda, hem usulî hem de maddi hukuk bakımından sonuçlar doğacaktır.

---

[56] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 118.
[57] Öztürk, Bahri, Ceza Muhakemesi Hukukunda Kovuşturma Mecburiyeti (Hazırlık Soruşturması), Ankara 1991, s.68; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 117; Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 117.
[58] BVerfGE 30, 25.
[59] Yüce, Turhan Tufan, Sanığın Savunması ve Korunması Açısından Ceza Soruşturmasının Ümanist İlkeleri, TBBD, 1998, S.1, s.158,159.
[60] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 52.
[61] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 117.
[62] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 52.
[63] Şahin, Cumhur, Sanığın Kolluk Tarafından Sorgulanması, Doktora Tezi, Ankara 1994, s.71.

Ayrıca insan haysiyeti işkence yasağı örneğinde olduğu gibi dokunulmaz olmakla birlikte, bir hukuk devletinde özgürlükler sınırsız şekilde kullanılamaz. Bu çerçevede temel hak ve özgürlüklere müdahalenin sınırının hukuk devleti ilkesi olduğu ifade edilmelidir[64]. Bu bağlamda özellikle gizli soruşturma metodu teşkil eden koruma tedbirleri, görünüşte insan haysiyetine aykırıymış gibi bir tablo çizseler de hukuk devleti ilkesinin sınırları içerisinde uygulanmaları halinde, ceza muhakemesinin maddi gerçeği ortaya çıkarma amacına hizmet eden müdahaleler olarak hukuka uygun kabul edilirler.

Online arama tedbiri ile getirilen sınırlama özellikle özel hayat alanına yönelik olduğundan, bu tedbirin insan haysiyetine tehdit oluşturabileceği göz önünde bulundurularak sıkı koşullara tabi tutulması; bu tedbirin Anayasa ve kanunların öngördüğü çerçevede her somut olayda objektiflik kriterinin ve ölçülülük ilkesinin uygulanması; online aramaya hukuk devleti ilkesinin bir gereği olarak ancak zorunluluk halinde ve sonuca ulaşmaya elverişli olduğunda başvurulması gerektiği dikkate alınmalıdır.

C. Dürüst İşlem İlkesi

Dürüst işlem ilkesi, adil yargılama yükümlülüğünü ve adil yargılanma hakkını kapsayan, ceza muhakemesi işlemlerinin kandırma, yanıltma ve zorlama gibi insan iradesini engelleyen veya savunmayı kısıtlayan yollara başvurmaksızın, hukuk devleti ilkesine uygun ve önceden yasalar tarafından öngörülmüş kurallar çerçevesinde yapılması olarak tanımlanır[65]. Dürüst işlem ilkesi gerek soruşturma gerekse kovuşturma evresinde adil yargılanma şartlarının yerine getirilmesini kapsar[66]. Bu bağlamda bir yargılamanın ancak şüpheli, sanık ve mağdurunun haklarının korunması suretiyle adil olduğu kabul edilir[67].

Ceza muhakemesinin amacı olan maddi gerçeğin araştırılması bakımından ispat aracı olarak tanımlanan deliller bakımından "delil serbestisi" ilkesi geçerli olup, buna göre her şey delil niteliği taşıyabilmekte, ancak hukuka uygun şekilde elde edildiği takdirde değerlendirmeye alınabilmektedir. Duruşmada deliller incelenmekte,

[64]Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 117; Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 52.
[65] Öztürk, Koğuşturma, s.73; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 123.
[66] Özbek/Bacaksız/Dopan, Ceza Muhakemesi Hukuku, s. 54.
[67] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 119; Centel/Zafer, Ceza Muhakemesi Hukuku, s. 165.

değerlendirilmekte ve hâkim vicdani kanaatine göre karar vermektedir[68]. Delillerin aranmasında doğruluk kuralının önemi vardır, zira bu kural devlet ve suçlu arasında önemli bir denge öğesidir. Delillerin toplanması sırasında şüpheli veya sanığa yönelik hileli ve kötü niyetli davranışlar ortaya çıkabilir. Adil olmayan yöntemlerin önlenmesi ancak dürüst işlem ilkesine uyulması halinde mümkündür[69]. Bu ilke, soruşturma makamlarının adil, anlayışlı ve savunmayı kolaylaştırıcı şekilde davranmalarını da kapsar[70]. Bu da ancak adil yargılama ilkelerinin geçerli olduğu bağımsız, güvenli ve tarafsız bir adalet organı tarafından gerçekleştirilebilir[71].

Adil yargılanma esaslarının asgari olarak koşulları Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 6'ncı maddesinde[72] ve Medeni ve Siyasi Haklar Sözleşmesi'nin (MvSHS) 14'üncü maddesinin 1'inci fıkrası[73] ve devamı maddelerinde yer almaktadır.

---

[68] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 278.
[69] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 54.
[70] Yüce, Ümanist İlkeler, s. 164 vd.
[71] Kaboğlu, İbrahim Ö., Özgürlükler Hukuku, Ankara 2002, s.315

[72] AİHS Madde 6 – Adil Yargılanma Hakkı:
"1. Herkes davasının, medeni hak ve yükümlülükleriyle ilgili uyuşmazlıklar ya da cezai alanda kendisine yöneltilen suçlamaların esası konusunda karar verecek olan, yasayla kurulmuş, bağımsız ve tarafsız bir mahkeme tarafından, adil ve kamuya açık olarak ve makul bir süre içinde görülmesini isteme hakkına sahiptir. Karar alenî olarak verilir. Ancak, demokratik bir toplum içinde ahlak, kamu düzeni veya ulusal güvenlik yararına, küçüklerin çıkarları veya bir davaya taraf olanların özel hayatlarının gizliliği gerektirdiğinde veyahut, aleniyetin adil yargılamaya zarar verebileceği kimi özel durumlarda ve mahkemece bunun kaçınılmaz olarak değerlendirildiği ölçüde, duruşma salonu tüm dava süresince veya kısmen basına ve dinleyicilere kapatılabilir.
2. Bir suç ile itham edilen herkes, suçluluğu yasal olarak sabit oluncaya kadar masum sayılır.
3. Bir suç ile itham edilen herkes aşağıdaki asgari haklara sahiptir:
a) Kendisine karşı yöneltilen suçlamanın niteliği ve sebebinden en kısa sürede, anladığı bir dilde ve ayrıntılı olarak haberdar edilmek;
b) Savunmasını hazırlamak için gerekli zaman ve kolaylıklara sahip olmak;
c) Kendisini bizzat savunmak veya seçeceği bir müdafiinin yardımından yararlanmak; eğer avukat tutmak için gerekli maddî olanaklardan yoksun ise ve adaletin yerine gelmesi için gerekli görüldüğünde, resen atanacak bir avukatın yardımından ücretsiz olarak yararlanabilmek;
d) İddia tanıklarını sorguya çekmek veya çektirmek, savunma tanıklarının da iddia tanıklarıyla aynı koşullar altında davet edilmelerinin ve dinlenmelerinin sağlanmasını istemek;
e) Mahkemede kullanılan dili anlamadığı veya konuşamadığı takdirde bir tercümanın yardımından ücretsiz olarak yararlanmak."
[73] MvSHS Madde 14:
"1. Herkes mahkemeler ve yargı organları önünde eşittir. Herkes, bir suçla itham edildiğinde ya da bir hukuk davasında hak ve yükümlülükleri hakkında karar verilirken, yasalar uyarınca kurulmuş yetkili, bağımsız ve tarafsız bir mahkeme önünde adil ve kamuya açık bir duruşma hakkına sahiptir. Demokratik bir toplumda ahlak, kamu düzeni ya da ulusal güvenlik gerekçeleriyle ya da tarafların özel hayatları bunu gerektirdiğinde, ya da özel durumlarda, mahkeme, açıklığın adalete zarar vereceği düşüncesine vardığı takdirde, mahkemenin gerekli gördüğü ölçüde, basın ve dinleyiciler duruşmaların tümü ya da bir kısmının dışında tutulabilirler. Ancak, küçüklerin çıkarları aksini gerektirmedikçe, ya da duruşmalar çocukların vesayetine ilişkin evlilikle ilgili uyuşmazlıklar hakkında olmadıkça, ceza ya da hukuk davalarında verilecek herhangi bir kararın aleni olması zorunludur.

AİHS m.6/1'de yer alan *"fair trial"* ifadesiyle, *"silahların eşitliği ilkesi, dürüst işlem ilkesi, hukuki dinlenme hakkı, diğer bir ifadeyle meram anlatma ilkesi"* ile adil yargılanma kuralları sıralanmış olup, davanın kanunla kurulan, bağımsız ve tarafsız mahkeme önünde, makul sürede açık ve aleni duruşma yapılarak gerçekleştirilmesi zorunluluğu getirilmiştir. Burada yer alan *"silahların eşitliği ilkesi, dürüst işlem ilkesi ve hukuki dinlenme hakkı",* adil yargılanma hakkının çekirdeği olarak kabul edilir[74].

Ayrıca AİHS m.6/2'de *"masumiyet karinesi ile şüpheden sanık yararlanır ilkesi"* düzenleme altına alınmıştır.

AİHS m. 6/3'te ise sanık hakları yer almaktadır. Bunlar sırasıyla, *"suçlamayı öğrenme hakkı, savunma hakkı, müdafi yardımından yararlanma hakkı, muhakemeye yön verme hakkı ile tercüman yardımından yararlanma hakkı"* olarak sayılmıştır.

Türkiye Cumhuriyeti Anayasası'nda adil yargılanma hakkı "hak arama hürriyeti" başlığını taşıyan 36'ncı maddenin 1'inci fıkrasında düzenlenmiş olup, ilkenin içeriği hakkında bir açıklama yapılmamıştır. Buna göre, *"herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir*." Anayasamızda adil

---

2. Bir suçla itham edilen herkes, yasalara göre suçlu olduğu kesinleşene dek masum kabul edilmek hakkına sahiptir.
3. Herkes, itham edildiği suçla ilgili olarak, tam bir eşitlik içinde, aşağıdaki asgari garantilere sahip olacaktır:
(a) Kendisine, en kısa zamanda ve anlayacağı bir dilde, aleyhindeki iddianın niteliği ve nedenleri hakkında ayrıntılı bilgi verilmesi;
(b) Savunmasını hazırlayabilmek ve kendi seçtiği avukatla temas edebilmek için yeterli zaman ve kolaylıkların tanınması;
(c) Gereksiz bir gecikme olmadan yargılanması;
(d) Yargılanmada hazır bulunması ve kendisini ya doğrudan ya da kendi seçtiği avukat yardımı ile savunması; avukatı yoksa, bu hakkının var olduğunun kendisine bildirilmesi; adaletin gerektirdiği her durumda kendisine bir avukat tayin edilmesi ve böyle durumlarda ödeme yapma olanağı yoksa bu yardımın parasız olarak sağlanması;
(e) Aleyhindeki tanıklara soru sorabilmesi ya da soru sordurabilmesi, lehindeki tanıkların da aleyhindeki tanıklarla aynı şekilde sorgulanabilmelerinin sağlanması;
(f) Mahkemede kullanılan dili anlamıyor veya konuşamıyorsa bir tercümanın parasız yardımının sağlanması;
(g) Kendi aleyhinde tanıklıkta bulunmaya ya da suç itirafına zorlanmaması.
4. Küçükler için yargılama bu kişilerin yaşları ve topluma yeniden kazandırılmaları düşüncesi gözönüne alınarak yürütülecektir.
5. Bir suçtan hüküm giyen herkes, mahkumiyet ve cezanın yasalara uygun olarak daha yüksek bir yargı organınca yeniden incelenmesi hakkına sahip olacaktır.
6. Kesin bir kararla bir suçtan dolayı mahkum olan ve daha sonra hakkındaki hüküm, adaletin yanlış tecelli ettiğini kat'i şekilde ortaya koyan yeni veya yeni ortaya çıkan bir maddi delil dolayısıyla bozulan veya bu sebeple affa uğrayan bir kişi, evvelce bilinmeyen maddi delilin zamanında ortaya çıkmamasında kısmen ya da tamamen kendi kusuru bulunduğu ispat edilmediği takdirde, böyle bir hükmün sonucunda ceza çekmesinin karşılığı olarak yasalara uygun şekilde tazminata hak kazanır.
7. Hiç kimse, bir ülkenin yasalarına ve ceza usulüne göre daha önce kesin olarak mahkum olmuş ya da beraat etmişse, aynı fiil için yeniden yargılanamaz ve cezalandırılamaz."
[74] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 55.

yargılanma hakkının ayrıca "kanuni hâkim güvencesi" (m.37) ile "duruşmanın açık ve kararların gerekçeli olması" (m.141) kenar başlıklı maddeleriyle düzenlendiğini ifade edebiliriz. Makul süre içinde yargılanmaya ise 19'uncu maddenin 7'nci fıkrasında yer verildiğini görmekteyiz.

Sonuç olarak, delillerin toplanmasında başvurulan usul ile uygulanan yöntemlerin insan onurunu ve adaletin saygınlığını ihlal etmemesini sağlamayı amaçlayan dürüst işlem ilkesi, online arama tedbiri bakımından da önem teşkil etmektedir. Bu tedbire başvurulurken, insan hakları ihlalleri yaratmamak ve hukuk devleti ilkesine aykırı davranmamak üzere Anayasa ve kanunlarla öngörülmüş esaslara uyularak adli ve önleme amaçlı online arama tedbiri gerçekleştirilmelidir. Özellikle hâkim kararı olmadan online arama uygulanmamalı ve gecikmede sakınca olan hallerde kanunla yetkili kılınan mercinin yazılı emri aranmalıdır. Ayrıca dürüst işlem ilkesine ve kanunlarda öngörülen şartlara dayanmayıp hukuk devleti ilkesine aykırı gerçekleştirilen online arama sonucu elde edilen deliller de hukuka aykırı delil olarak kabul edilerek, ceza muhakemesinde hükme esas alınmamalıdır. Diğer yandan, kolluğun da bu konuda bilinçlendirilmesi ile dürüst işlem ilkesinden ayrılarak online arama tedbirine başvurması halinde elde ettiği delillerin muhakemede kullanılamayacağı bilincinin oluşturulması hukuka uygun hareket etmesini sağlayacak en etkin mekanizma olacaktır.

D. Ölçülülük İlkesi

Ceza muhakemesinin temel ilkelerinden biri olan ölçülülük ilkesi, elverişlilik, gereklilik ve orantılılık unsurlarından oluşmaktadır[75]. Bu bağlamda elverişlilik, öngörülen müdahalenin ulaşılmak istenen amacı gerçekleştirmeye elverişli olmasını; gereklilik ulaşılmak istenen amaç bakımından müdahalenin zorunlu olmasını, dolayısıyla aynı amaca daha hafif bir müdahale ile ulaşılmasının mümkün olmamasını ve orantılılık ise bireyin hakkına yapılan müdahale ile hedeflenen amaç arasında makul bir dengenin bulunması gerektiğini ifade eder[76].

Koruma tedbirleriyle henüz bir hüküm verilmeksizin bireylerin temel hak ve özgürlüklerine müdahale edildiğinden, bu tedbirlere başvurulurken, ölçülülük ilkesine

[75] Dülger/Taşkın, s. 349.
[76] AYM, A.A. ve diğerleri, 10.06.2021, B. No: 2017/31079; Ölçülülük ilkesi hakkında ayrıntılı bilgi için bkz. Kaygusuz, Ziyaettin, Zor ve Silah Kullanmada Standart Bir Uygulama Modeli: Ölçülülük İlkesi, Bilge Yayınevi, Ankara 2016.

uyulması gerekir. Bu bağlamda koruma tedbirine başvurmakla elde edilecek yarar ile temel hak ve özgürlüklerin sınırlanmasıyla ortaya çıkacak zarar arasında makul bir ölçü aranır, dolayısıyla araçla amacın, yöntem ve hedefin dengeli olması gereklidir[77]. Bunun sonucunda eğer beklenen yarardan çok zarar öngörülüyorsa, o koruma tedbirine başvurulmamalı ya da imkanlar dahilinde daha hafif bir koruma tedbirine başvurulmalıdır. Böylelikle ikincillik ilkesi dikkate alınarak aşırılık yasağına da uyulmuş olacağı ifade edilebilir[78].

Bazı haller için kanun koyucu tarafından doğrudan bir ölçü belirlenmiş olup, bu durumda koruma tedbirine başvurma yasağı kabul edilir. Örneğin 5395 sayılı Çocuk Koruma Kanunu gereği, on beş yaşını doldurmamış çocuklar hakkında üst sınırı beş yılı aşmayan hapis cezasını gerektiren hukuka aykırı fiiller sebebiyle tutuklama karar verilememektedir[79]. Bununla birlikte kanun koyucunun örneğin CMK m. 100/1' de veya m. 100/4' te olduğu gibi bazı düzenlemelerin içinde kısmen ölçülülük ilkesine yer verdiğini ve bu çerçevede bazı tedbirlerin uygulanamayacağını belirttiğini görmekteyiz[80].

Normatif dayanağını açıkça Anayasadan alan ölçülülük ilkesi[81], AYM'nin çeşitli kararlarında açıkça tanımlanmakta olup, ölçülülük bakımından özellikle araç ve amaç arasında hakkaniyete uygun bir dengenin bulunması, yasal önlemin sınırlama amacına ulaşmaya elverişli olması ve sınırlayıcı önlemin zorunluluk taşıması gerekliliğinden bahsedilmektedir[82].

Gizli bir erişim tedbiri olan online araman temel hak ve özgürlüklere müdahale oluşturmakta olduğu açıktır. Bu bağlamda özellikle etkilenen temel hak ve özgürlükler şu şekilde sıralanabilir:

1. Haberleşmenin gizliliği,
2. Konut dokunulmazlığı,
3. Genel kişilik hakkının yansıması olarak özel ve aile hayatının gizliliğinin korunmasını isteme ile bilgi edinme konusunda kendi kaderini tayin etme hakkı,

[77] Öztürk/Kazancı/Güleç, s. 39; Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447; Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s. 269.
[78] Özbek/Doğan/Bacaksız, s. 235.
[79] Öztürk/Kazancı/Güleç, s. 39.
[80] Yenisey/Nuhoğlu, s. 335.
[81] Dülger/Taşkın, s. 349.
[82] AYM, E. 2011/111, K. 2012/56, 11/4/2012; E. 2016/16, K. 2016737, 5/5/2016; E. 2012/100, K. 2013/84, 04.07.2013.

4. Genel kişilik hakkının yansıması olarak bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü garanti etme hakkı.

Online aramanın ölçülülük ilkesine uygun olabilmesi için yukarıda bahsi geçen temel haklara öngörülen müdahale ile meşru bir amacın bulunması, müdahalenin ulaşılmak istenen amacı gerçekleştirmeye elverişli olması, ulaşılmak istenen amaç bakımından müdahalenin zorunlu olması ve bireyin hakkına yapılan müdahale ile hedeflenen amaç arasında makul bir dengenin bulunması gerekir.

Online aramanın tüm bu temel hakların ölçülülük ilkesi bağlamında ne derecede etkilendiğini Federal Almanya Anayasa Mahkemesi'nin 27.02.2008 tarihli kararı çerçevesinde detaylı bir şekilde inceleyeceğimizden, burada yalnızca ilgili karar anılmakla yetinilecektir[83].

E. Özel Hayata ve Aile Hayatına Saygı Hakkı

Özel hayata ve aile hayatına saygı gösterilmesini isteme hakkı, Avrupa İnsan Hakları Sözleşmesi[84], İnsan Hakları Evrensel Beyannamesi[85], Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi[86] gibi uluslararası belgelerde ve hukuk devleti niteliği taşıyan devletlerin anayasalarında yer alan dokunulmaz, devredilmez ve vazgeçilmez temel hakların başında gelir.

Kişilere, maddi ve manevi varlıklarını diledikleri şekilde geliştirip şekillendirmelerini sağlayacak özel bir hayat alanın tanınması her hukuk devletinde bulunması gereken en önemli özelliklerden biri olarak kabul edilir[87]. Bu doğrultuda

---

[83] Bkz. İkinci Bölüm I E 2.

[84] Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine göre;
"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.
2. Bu hakların kullanılmasına ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, suçun ve düzensizliğin önlenmesi, genel sağlık ve genel ahlakın korunması, başkalarının hak ve özgürlüklerinin korunması amacıyla, hukuka uygun olarak yapılan ve demokratik bir toplumda gerekli bulunan müdahalelerin dışında, kamu makamları tarafından hiçbir müdahale yapılamaz."

[85] İnsan Hakları Evrensel Beyannamesi'nin 12. Maddesi gereği;
"1.Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfî olarak karışılamaz, şeref ve adına saldırılamaz.
2.Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır."

[86] Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi'nin 17. Maddesi uyarınca;
"1. Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz.
2. Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır."

[87] Öztürk, Kovuşturma, s. 76; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 141; Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 61; Gökçen/Balcı/Alşahin,Çakır, Ceza

bireylerin devlet müdahalelerinden korunabildikleri, özgürce yaşayabildikleri dokunulmaz bir alana sahip olmaları gerekir. Özel hayatın devletin özel koruması altında olması sebebiyle, bir yandan devlet gereksiz müdahalelerden kaçınmalı, diğer yandan ise başka kişilerin müdahalesini önleyici bazı tedbirler almalıdır.

Özel hayatın gizliliğine saygı, bireyin onurunu korumayı, kişiliğinin gelişmesini sağlamayı ve kendisiyle baş başa kalabileceği özerk bir dünya yaratmayı amaçlar[88]. Kişilerin diğer insanlarla sağlıklı ilişkiler kurabilmesi ve kişiliğini güven içinde geliştirebilmesi için özel hayatın gizliliği hem diğer insanlara hem de devlete karşı koruma altına alınmıştır[89].

Anayasamızın "*özel hayatın gizliliği ve korunması"nı* 20'nci maddede uluslararası düzenlemelere paralel bir şekilde hüküm altına aldığını ifade edebiliriz. *"Özel hayatın gizliliği"* başlığını taşıyan 20'nci maddenin 1'inci fıkrasında, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı düzenlenmiş; 2'nci fıkrasında, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyasının aranamayacağı ve bunlara el konulamayacağı, yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunması gerektiği, hakimin, kararını el koymadan itibaren kırk sekiz saat içinde açıklayacağı; aksi halde, el koymanın kendiliğinden kalkacağı belirtilmiş; 3'üncü fıkrasında ise herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır.

Muhakemesi Hukuku, s. 133; Özbudun, Ergun, Özel Haberleşmenin Gizliliği, AÜHFM, 50. Yıl Armağanı, Ankara 1977, s. 266.

[88] Saadet Yüksel, Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, İstanbul, Beta, 2012, s. 7.

[89] Kaymaz, s. 76.

Türk ve Alman öğretisi, insanın sosyal bir varlık olarak hayatını ancak diğer insanlarla birlikte geçirebileceği gerçeğinden yola çıkararak, insan hayatının genel ve özel olmak üzere iki yönü olduğunu varsaymaktadır[90]. Hayatın genel yönü en dış ve genel hayatı kapsar, herkes tarafından bilinir ve bu nedenle korunmasını gerektiren bir özelliği bulunmamaktadır[91]. Bu bağlamda örneğin insanların kamuya açık yerlerdeki davranışları ve sözleri herkes tarafından görülebilir ve dinlenebilir[92]. Hayatın özel yönü ise özel hayat ve hayatın giz alanı olarak ikiye ayrılır. Özel hayat bakımından bunun ancak en yakın kişilerle paylaşılabilen, esasen gizli olan bir alan olarak kabul edildiği belirtilmektedir[93]. Özel hayat bir kişinin özel alanı, ev ve aile çevresini veya kamuya açık olmayan başka herhangi bir alanı kapsar[94]. Ayrıca kişinin kamuyla paylaşılmasını istemeyeceği hesap bakiyesi veya ikamet yeri gibi bazı bilgiler de özel hayat alanına girer[95]. Mahremiyet olarak da adlandırılan hayatın gizli alanı ise kişinin kimseyle paylaşmadığı duyguları, düşünceleri ve dolayısıyla sırları kapsadığı alan olarak kabul edilir[96].

Hayatın genel yanının özel yanından nasıl ayrıldığı ve özel yanının da özel hayat ve gizli hayat alanlarının nerede başlayıp nerede bittiğini daha kolay tespit edebilmek için Alman Anayasa Mahkemesi'nce geliştirilen ve alanlar teorisi *("Sphärentheorie")* adı verilen teoriden faydalanılabilir[97]. Bu teoriye göre, insan hayatının merkezinde hayatın giz (sır) alanı *("Intimsphäre")* bulunur ve her türlü devlet müdahalesine karşı koruma altına alınmış çekirdek alan olarak kabul edilir[98]. En üst düzeyde korunmasının sebebi insan haysiyetinin dokunulmazlığı ilkesine olan yakınlığına dayanmaktadır[99]. Hayatın sır alanı kişinin bireyselliğinin gelişimi için vazgeçilmez olduğundan, bu alan dokunulmazıdır[100]. Kamu yararının ağır basması bile, özel hayatın bu mutlak koruma altındaki çekirdek alanına müdahaleyi haklı

---

[90] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 142.
[91] Gümüşay, s. 21.
[92] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 133.
[93] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 61, 62.
[94] Fechner, Nina, Wahrung der Intimität? Grenzen des Persönlichkeitsschutzes für Prominente, Düsseldorf, 2010, Peter Lang Verlag, S. 34.
[95] Autorenteam iRights.Lab für bpb.de, Das Sphärenmodell zur Bemessung von Persönlichkeitsrechtsverletzungen, Abschnitt „Die Privatsphäre", Lizenz CC BY-NC-ND 3.0 DE, Erişim: www.bpb.de, Erişim tarihi: 01.06.2024.
[96] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 142.
[97] BVerfGE 27, 1 (6) = NJW 1969, 1707; BVerfGE 27, 344 (350 vd.) = NJW 1970, 555; BVerfGE 33, 367 (376 f.) = NJW 1972, 2214; BVerfGE 49, 286 (298) = NJW 1979, 595; BVerfGE 54, 148 vd. = NJW 1980, 2070.
[98] BVerfGE 80, 367 (373).
[99] Öztürk, Bahri, Özel Hayalın Gizliliği Ve Arama, Manisa Barosu Dergisi, Yıl 11, c.4, 1992, s.5.
[100] Fechner, S. 33.

gösteremez[101]. Burada kişi kendi düşünceleriyle, inançlarıyla ve kendisiyle baş başa kaldığından, bu alana kişinin son sığınağı da denilmektedir[102]. Hayatın sır alanı bakımından düşünce ve duyguları içeren günlükler, sağlık durumuna ilişkin kişisel bilgiler veya cinsel yaşam örnek verilebilir[103]. Bu çekirdek alan özel hayat *("Privatsphäre")* olarak tanımlanan ve yine devlet müdahalelerine karşı korunma altına alınmış olan ikinci bir alan ile çevrilmiştir. Ancak bu ikinci alan dokunulmaz olmayıp, burada nisbi bir koruma sağlanır[104]. Ayrıca bu ikinci alanı çevreleyen ve hayatın genel yönü *("Sozialsphäre")* olarak tanımladığımız üçüncü bir alan daha vardır ki bu alan herhangi bir korumaya tabi değildir[105]. Özetle, hayatın sır alanı olarak kabul edilen çekirdek alana yakınlık arttıkça koruma düzeyinin de arttığı söylenebilir[106].

Günümüzde kişilerin özel yaşam alanlarının git gide daraldığını görmekteyiz. Özel hayatın gizliliğine karşı tehditler özellikle teknolojik gelişmeler bağlamında artmaktadır[107]. Teknik imkanlardan kaynaklanan bu tehditler, bazen diğer kişiler ve bazen de devletler tarafından kişinin özel hayatını ihlal edecek şekilde kullanılabilir. Dinleme, izleme ve depolama cihazlarının geliştirilmesi ve yaygın kullanımı, elde edilen verilerin ve kişisel bilgilerin internette kolayca yayılabileceği anlamına gelir ve bireylerin özel hayatlarına izinsiz erişim riskini arttırır[108].

Öte yandan, teknolojinin hızlı gelişmesiyle birlikte suçların işlenmesi de kolaylaşmış, suçu aydınlatmak için delil elde etmek giderek zorlaşmıştır. Özellikle organize şekilde işlenen suçlarda ve terörle mücadelede delil elde etmenin zorlaşmasıyla, kanun koyucuda teknolojik imkanlardan yararlanma düşüncesi doğmuş ve online arama tedbiri uygulama alanı bulmuştur.

Online arama tedbiri ile bilgisayar, cep telefonu ve tablet gibi bilgi teknolojisi sistemlerinde suçu önlemek veya aydınlatmak için gerekli verilere ulaşılmaya çalışılırken, depolanmış tüm kişisel verilere ulaşılabilmektedir. Bununla birlikte bir kişinin tüm kullanım davranışları izlenebilmekte[109] ve hayatının sır alanına dahil tüm

[101] BVerfGE 109, 279 (313) = NJW 2004, 999 (1002); BVerfGE 34, 238 (245) = NJW 1973, 891
[102] Özbudun, Haberleşmenin Gizliliği, s. 266.
[103] BeckOK GG/Lang, 57. Ed. 15.1.2024, GG Art. 2 Rn. 84, 85.
[104] BVerfGE 90, 255 (260) = NJW 1995, 1015.
[105] BVerfG NJW 2006, 3406 (3408); Öztürk, Koğuşturma, s.75, 76.
[106] BeckOK GG/Lang, 57. Ed. 15.1.2024, GG Art. 2 Rn.75.
[107] Gümüşay, s. 25.
[108] Kaymaz, s. 80.
[109] Meyer-Gossner/Schmitt, §100b, Rn. 1.

verilere ulaşılarak kapsamlı kişilik profilleri oluşturulabilmektedir[110]. Bu nedenle online arama tedbiri özel hayatın gizliliğine yoğun müdahale teşkil eden tedbirlerden birisi olarak kabul edilir.

Tedbire suç işlenmesinin önlenmesi, suçlulara ve suç delillerine ulaşılarak kamu güvenliğinin tesis edilmesi, herkesin hak ve özgürlüklerinin güvence altına alınması amacıyla, amacına ulaşılabilecek hallerde ve ancak ölçülülük ilkesi esas alınarak başvurulması halinde özel hayatın gizliliği ilkesine bağlı kalınmış olacaktır.

F. Kişisel Verilerin Gizliliğinin Korunmasını İsteme Hakkı

Kişiye ilişkin bilgiler arasında en önemlisinin "kişisel veriler" olduğu ifade edilebilir. Teknolojik gelişmelerin temel hak ve özgürlüklere müdahale edilmesini kolaylaştırması sebebiyle bu konuda yasal düzenlenmelerin yapılması gerekliliği ortaya çıkmıştır. Bunun neticesinde 2010 yılında Anayasamızın 20'nci maddesine bir fıkra eklenerek kişisel veriler, *"özel hayatın gizliliği ve korunması hakkı"* kapsamında Anayasal güvence altına alınmıştır. AY m. 20/3 gereği, *"herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir."*

Avrupa Konseyi (AK), *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"* isimli Sözleşmesi'ni 1981'de imzaya açmış olup[111], Sözleşmeyi imzalayan devletler, iç hukuklarında Sözleşme'ye uygun şekilde düzenleme yapma yükümlülüğü altına girmişlerdir. Türkiye'de de bu doğrultuda, 2016 tarihli *"6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)"* kabul edilmiştir. Ayrıca 1995 yılında, Avrupa Birliği (AB) üyesi ülkeler arasındaki uygulamalarda bir düzen oluşturulması için *"95/46 sayılı Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı"* isimli Yönerge yürürlüğe girmiştir[112]. Yönerge'nin 2'nci maddesi uyarınca, *"kişisel veri, belirli veya belirlenebilir nitelikteki*

[110] BVerfG 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833 ff; Grossmann, GA 2018, 433.
[111] SEV 108 - Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (coe.int), Erişim tarihi: 01.06.2024:
[112] Directive - 95/46 - EN - Data Protection Directive - EUR-Lex (europa.eu), Erişim tarihi: 01.06.2024:

gerçek kişiyle ilgili her türlü bilgi" ifade edebilir; *"belirlenebilir kişi" ise, kimlik numarasıyla veya fiziksel, psikolojik, akli, ekonomik, kültürel veya sosyal kimlik gibi unsurlardan bir veya birkaçı yoluyla belirlenebilen kişidir."* Yönerge'nin 8'nci maddesinde özel bir kategori olarak "hassas verilere" yönelik tanımlama getirilmiştir. Bu maddeye göre, kişinin "ırk veya etnik kökenini, siyasi görüşünü, dinî veya felsefî inancını, sendika üyeliğini, sağlık ve cinsel hayatını içeren bilgiler" hassas veriler kategorisine girer ve bu verilerin işlenmesinin önüne geçilmelidir.

KVKK m. 3 uyarınca, kimliği belirli yahut belirlenebilir olan bir gerçek kişiye ilişkin her türlü bilgi kişisel veridir[113]. Öğretide kişisel veri, *"bireyin şahsi, mesleki ve ailesine ilişkin özelliklerini gösteren, o bireyi diğer bireylerden ayırmayı ve niteliklerini ortaya koymayı sağlayan her türlü bilgi"* şeklinde tanımlanmaktadır[114]. Bu bağlamda kişinin adı, soyadı, medeni hâli, kimlik numarası, nüfusa kayıtlı olduğu yer, doğum yeri ve tarihi gibi kimlik bilgilerinin yanı sıra, bedenindeki yara izi, ben, dövme gibi belirleyici işaretler, kişisel görüntüsü, fotoğrafı, telefon numarası, banka hesap/ IBAN numarası, kredi kartı numarası, emeklilik, kurum sicil, sosyal sigorta numarası, internet protokolü (IP) adresi, elektronik posta adresi, sosyal medya hesap bilgileri, bunlara ilişkin şifreler, güvenlik kodları, ıslak ve/ veya elektronik imzası, matbu veya dijital, örneğin e- posta yolu ile veya sosyal ağlarda yaptığı yazışma ve paylaşımlar da kişisel veri olarak kabul edilmektedir[115].

KVKK m. 6'da özel nitelikli (hassas) kişisel verilere yer verilmiş olup, buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri (kayıt ve bilgileri) ile parmak izi, retina görüntüsü, DNA özellikleri gibi biyometrik ve genetik verileri hassas verilerdir[116].

"Kişisel veri" teriminin kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmesi, terimin ne kadar geniş olduğunu açıkça

---

[113] Öztürk, Bahri/Altınok Çalışkan, Elif/ Seyhan, Serkan, Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı, 2. Baskı, Ankara 2022, s. 18.
[114] Henkoğlu, T., Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015, Yetkin. s.28
[115] Henkoğlu, s.28; Akgül, A., Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014, Legal., s. 8,9; Şimşek, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, Beta, s.121; Özdemir, H., Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması. Ankara 2009, Seçkin, s. 124; Akkurt, Sinan Sami, Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, Kişisel Verileri Koruma Dergisi, Cilt. 2 Sayı: 1, S. 21.
[116] Henkoğlu, s. 28; Özdemir, s. 126.

göstermektedir[117]. Kişisel verilerin korunmasıyla, devlet veya üçüncü kişilerin, verilere, rıza dışında toplayıp işlemek yoluyla müdahale etmesinin önüne geçilmesi amaçlanmaktadır. Kişisel verilerin hukuka aykırı olarak işlenmesi, Hukuk devletlerinde Anayasa ile güvence altına alınmış olan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı ile özel hayatın gizliliği ve korunması hakkının ihlali anlamına gelmektedir.

Kişisel verilerin gizliliği, özel hayatın gizliliği ile bağlantılı olarak en çok müdahaleye uğrayan alanlardan biri olarak karşımıza çıkmaktadır. Teknolojik ilerleme ve internet kullanımının yaygınlaşmasıyla birlikte kişiler hakkında bilgi akışı, bilgiye erişim ve bilginin yayılması çok kolay hale gelmiştir. Bu durum, kişilerin hukuki güvenliğine yönelik bir dizi tehdidin ortaya çıkmasına neden olmaktadır. Geniş yelpazeye yayılmış ve akıllı sistemler olarak insanların adeta hayatlarını ele geçirmiş olan bilgi teknoloji sistemleri birçok kişisel veriyi kaydetmektedir. Verilerin kaydedilmesi her zaman rıza dahilinde olmayıp, bilgilerin gerek devlet gerekse özel şirketler gibi üçüncü taraflarca ele geçirilmesi riski bulunmaktadır.

Online arama tedbiri bakımından ise ilgili kişinin bilgi teknoloji sisteminde bulunan tüm depolanmış kişisel ve hassas verilerinin devlet tarafından ele geçirilmesi söz konusudur. Nitekim cep telefonu, akıllı tablet veya bilgisayarlarda kişinin kimlik, iletişim, sağlık, mali ile dini inancı ve siyasi görüşü gibi özel hayatına ilişkin birçok veri bulunabilmektedir. Tedbirin gizli niteliği sebebiyle, müdahale ilgili kişinin bilgisi ve rızası dışında gerçekleşmektedir.

Online aramanın teknik kapsamı nedeniyle, bu tedbir ile kullanıcının sistemlerinden büyük miktarda veri elde edilebilir. Bu veriler bir bütün olarak analiz edildiğinde, kapsamlı bir kişilik profilinin oluşturulmasına ve ilgili kullanıcının çok yönlü olarak izlenmesine olanak sağlamaktadır[118]. Kişisel verilerin korunmasına yönelik tehdit, sistemlerin ağa bağlı yapısı ve karmaşıklığı ile yüksek kötüye kullanım potansiyeli nedeniyle daha da artmaktadır[119].

Bu gerekçelerle, tedbirin ancak suç işlenmesini önlemek, suçlulara ve suç delillerine ulaşarak kamu güvenliğini sağlamak ve tüm kişilerin hak ve özgürlüklerini

[117] Akkurt, S. 21.
[118] Kohlmann, Online-Durchsuchungen und andere Massnahmen mit Technikeinsatz 1. Auflage, 2012, s. 99; BVerfGE 120, 274, 305; Valerius in Juristische Rundschau, 2007, 274, 279.
[119] BVerfGE 120, 274, 306.

korumak amacıyla uygulandığı durumlarda ve ancak ölçülülük ilkesi temelinde kişisel verilerin gizliliğine riayet edilmiş olunacaktır.

IV. Tedbirin Kapsamı ve Teknik Çerçevesi

Online aramanın anayasal kapsamının ve bununla birlikte müdahalenin yoğunluğunun daha iyi anlaşılabilmesi için bilgi teknolojisi sistemlerinin ve bu sistemlere erişim seçeneklerinin incelenmesi önem teşkil etmektedir.

Bu nedenle çalışmanın bu bölümünde öncelikle tedbirin somut olarak hangi sistemleri hedeflediği ve bulut bilişim (Cloud-Computing) bağlamında sanal depolamanın online arama kapsamına girip girmediği incelenecektir. Devamında ise teknik araç niteliğindeki arama yazılımı detaylı bir şekilde ele alınıp, sisteme sızma (infiltrasyon) yöntemleri ile infiltrasyon sonrası hedef sistemden veri okuma ve aktarma konusunda açıklamalarda bulunulacaktır.

A. Hedef Sistemin İncelenmesi

1. Bilgi Teknolojisi Sistemleri

Online arama, yabancı bir bilgi teknolojisi sistemine kullanımı izlemek ve depolanan içeriği kaydetmek suretiyle devlet tarafından yapılan gizli erişim olarak tanımlanmaktadır[120]. Bir bilgi teknolojisi sistemi, bilgiyi kaydetmek, depolamak, işlemek, iletmek ve görüntülemek için kullanılan donanım ve yazılımın yanı sıra verilerden oluşmaktadır[121].

Tanımda "bilgi teknolojisi sistemi" kavramı kullanılarak, bilinçli bir şekilde belirli bir cihaz türüne, belirli bir işletim sistemine, programlamaya veya benzerine bağlı kalmaktan kaçınılmıştır[122]. Bu nedenle bilgi teknolojisi sistemi terimi çevrimiçi iletişim için yaygın olarak kullanılan akıllı telefonlar, tabletler ve dizüstü bilgisayarlar gibi uçtan uca cihazlarla sınırlı değildir. Her türlü elektronik veri işleme sistemi

[120] BT-Drucksache 18/12785, 54.
[121] Bundesministerium des Inneren Fragenkatalog BMJ, s. 2, erişim: Fragenkatalog des Bundesministeriums der Justiz (netzpolitik.org), Erişim tarihi: 01.06.2024: 08.03.2024).
[122] BeckOK StPO/Graf StPO §100b Rn. 8.

kapsam dahilindedir. Ancak bu geniş tanım beraberinde riskler de getirmektedir. Bilgi teknolojisi sistemlerinin pratik önemi günlük yaşamın ayrılmaz bir parçası haline gelmiş olup, günümüzde son derece karmaşık halde ve hemen hemen her cihazda bulunabilmektedirler.

Örneğin akıllı TV'ler ve „*Amazon-Alexa*", „*Apple-Siri*" veya „*Microsoft-Cortana*" gibi akıllı sesli asistanlar[123] ya da kullanıcıların kendi evlerini uzaktan izlemelerine ve kontrol etmelerine olanak sağlayan akıllı ev sistemleri veya ısınma ve aydınlatma sistemleri gibi tamamen uzaktan kontrol edilen diğer sistemler de bu sistemlerden sayılır[124]. Bununla birlikte, örneğin eski nesil bilgisayarlardan daha işlevsel olan mikro denetleyicilerden oluşan işitme cihazları da bilgi teknolojisi sistemleri olarak kabul edilmektedir. Bunlar özellikle alçak sesleri hatırlayabilme ve ses seviyesini buna göre ayarlayabilme işlevinin yanı sıra, konuşulanları da birkaç saniyelik bir süre boyunca kaydedip tekrar dinletmek imkanına sahiptirler. Böylelikle anayasal korumaya tabi olan ve özel hayatın temel alanlarından birini oluşturan „kendi kendine konuşma" da dahil olmak üzere geniş bir kapsamdan söz etmek mümkündür[125]. Bu verdiğimiz son örnekten de anlaşılacağı üzere, bilgi teknolojisi sistemlerinin kapsama alanı oldukça geniştir. Ayrıca bilgi teknoloji sistemleri kavramı, gelecekte geliştirilecek cihaz ve teknolojilere de açıktır[126].

Bilgi teknoloji sistemlerinin geniş yorumu gibi "müdahale" terimi de geniş yorumlanmalıdır. Online arama kapsamında müdahale bakımından hem güvenlik açıklarının istismar edilmesine hem de kriminalistik hilelerin kullanılmasına belirli sınırlar dahilinde izin verilir. Örneğin Alman hukukundaki düzenleme gereği, teknik yollarla gerçekleştirilen izinsiz erişim sadece soruşturma makamlarıyla sınırlı değildir. Örneğin bulut teknolojisine erişim sağlayan bilişim sağlayıcıları, internet sağlayıcıları veya şirket ağı yöneticileri gibi üçüncü kişilerin veri sahiplerine karşı bir bilgi teknolojisi sistemine gizli erişim sağlaması da mümkündür[127].

---

[123] Blechschmitt, MMR 2018, 361.
[124] Kruse/Grzesiek, S. 335; Sinn, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334), S.3, vom 30.05.2017, Erişim: https://www.bundestag.de/blob/509050/6f72dd42df72be6f2da6a024475b3f8a/s inn-data.pdf, Erişim tarihi: 01.06.2024: 08.03.2024.
[125] Stelzer, S. 15.
[126] BeckOK StPO/Graf StPO §100b Rn. 8.
[127] Rückert in: Münchener Kommentar, §100b, Rn. 36.

2. Bulut Bilişim Sistemleri

Gerek özel sektörde gerekse iş dünyasında artan veri aktarımının ve veri işlemenin bir sonucu olarak, daha büyük depolama kapasitelerine olan talep giderek artmaktadır[128]. Bu nedenle dünyanın her yerinde bu talebi karşılayan ve tüketicilere sunucular üzerinde son derece yüksek depolama hacimleri sunan sağlayıcılar ("bulut sağlayıcıları") bulunmaktadır.

İngilizce karşılığı "Cloud-Computing" olan bulut bilişimin artan kullanımı aynı zamanda siber suçların temel bir bileşenidir. Bu da sanal depolama seçeneklerinin gerek önleme gerekse adli takip bakımından soruşturma makamları tarafından giderek daha fazla hedef alınacağı anlamına gelmektedir.

Bulut bilişim bağlamında online aramanın mümkün olup olmadığı cevaplanması gereken sorulardandır. Bu çerçevede öncelikle bulut bilişim kavramını tanımlamak gerekir. Uzunca bir süre bulut bilişim terimi için ne yasal ne de yüksek mahkeme içtihatlarında tanım yapılmış idi. AB Komisyonu bulut bilişimi, başka bilgisayarlarda bulunan ve internet üzerinden erişilen verilerin depolanması, işlenmesi ve kullanılması olarak tanımlamaktadır[129]. Federal Almanya Anayasa Mahkemesi, bulut sistemlerini ağa bağlı, üçüncü taraf bilgisayarlara örnek olarak göstermiş ve kararını veri sahibinin kişisel verilerini tek başına veya teknik ağlarında içerebilecek sistemlerin korunmasına dayandırmıştır[130].

Öğretide bulut bilişim tüm verilerin, bilgilerin, belgelerin, yazılımların, uygulamaların internet bulutu üzerinde yer alan sanal bir depoda depolanmasını ve internet üzerinden ulaşılmasını sağlayan bir teknoloji olarak kabul edilmektedir[131]. Bulut bilişim, bulut kullanıcısının kendi donanımını ve/veya yazılımını tedarik etmesine ihtiyaç duymadan faydalanabileceği, bulut hizmeti sağlayıcısı tarafından sağlanan kaynaklara erişebileceği bir bilgi teknolojisi sağlama modeli olarak anlaşılmalıdır[132].

---

[128] Zerbes, Ingeborg/El-Ghazi, Mohamed, Zugriff auf Computer: Von der gegenstaendlichen zur virtuellen Durchsuchung, NStZ 2015, 425 (428).
[129] Cloud computing contracts - European Commission (europa.eu), Erişim tarihi: 01.06.2024; Pötters, Stephan, Beschaeftigtendaten in der Cloud, NZA 2013, 1055 (1055).
[130] BVerfG, MMR 2008, 315 (318).
[131] Çark, 2019. Çark, Ö. (2019). Kurumsal Kaynak Planlama (KKP) Sistemleri (1. bs.). Ankara: Gazi Kitabevi
[132] Hieramente/Fenina, StraFo 2015, 365 (366).

Bu hizmetlerin yelpazesi *Dropbox*, *Skydrive*, *Googledrive* ve *iCloud* gibi 'basit' veri depolama alanlarının sağlanmasından tüm kullanıcı arayüzlerinin ve hatta şirket sistemlerinin buluta aktarılmasına kadar uzanmaktadır[133].

Genellikle harici depolama seçeneklerinin kullanılması, özellikle de bulutta depolanan verilere farklı uç cihazlardan veya birkaç kişi tarafından birbirinden bağımsız olarak erişilebilmesi söz konusu olsa da, bulut sağlayıcısı tarafından sağlanan harici veri işleme seçeneklerinin kullanımı da artmaktadır[134].

Bulut bilişiminin ana kullanım amacı veri depolamanın sağlanması olmakla birlikte, iletişim aracı olarak kullanılması da mümkündür, zira bir bulut depolama alanında farklı kişiler birbirlerinin erişimine açık olan ve karşılıklı kullanılabilen bilgiler saklayabilmekteler[135]. Bulut bilişimin en önemli özelliği ise herhangi bir zaman ve mekân kısıtlaması olmadan kullanılabilmesidir[136].

Özetle, bulut bilişim normalde evdeki bilgisayarın içinde gerçekleşecek veri depolama ve veri işleme süreçlerinin dışarıya, yani buluta aktarılmasıdır. Sonuç olarak, evde bulunan bilgisayar sadece buluta erişim sağlayan ilkel bir araç olarak düşünülebilir[137].

Soruşturma makamlarının şüphelinin buluttaki bilgilerine ulaşılabilmesinin ön koşulu ise şüphelinin bulutta veri sakladığına dair bazı olguların varlığıdır. Bu örneğin bir bulut sağlayıcısının ilgili kişiye gönderilen, yüklemenin başarılı olduğunu onaylayan veya sağlanan depolama alanının kullanım kapsamı hakkında bilgi sağlayan kayıtlı e-postalar olabilmektedir[138]. Dolayısıyla bulut bilişim sistemlerinde saklanan verilere de online arama tedbiri kapsamında başvurulması mümkündür[139].

B. Teknik Araç Olarak Arama Yazılımı

Online arama düzenlemesinde müdahalenin teknik araçlar kullanarak gerçekleşmesi gerektiği belirtilmiştir. "İlgili kişinin kullandığı bilgi teknolojisi sistemlerine teknik yollarla müdahale etmek" ibaresi, bilişim sistemlerinden veri

---

[133] Gaehler, HRRS 2016, S. 340.
[134] Hieramente/Fenina, StraFo 2015, 365 (367).
[135] Soine, S. 500.
[136] Mathew ve Rodrigues, 2018. Mathew, H.L., Rodrigues, L. L. R. (2018). Prioritizing the Factors Affecting Cloud ERP Adoption – An Analytic Hierarchy Process Approach. International Journal of Emerging Markets, 13(6), 1559-1577. doi:10.1108/IJoEM-10-2017-0404.
[137] Heinrich, ZIS 9/2020, S. 426; Hieramente/Fenina, StraFo 2015, 365 (367).
[138] Soine, S. 500.
[139] KK-StPO/Henrichs/Weingast, StPO § 100b Rn. 4.

toplanabilmesi için gerekli teknik tedbirlerin alınabilmesini sağlamaya yöneliktir[140]. Düzenlemenin kendisinde "teknik araçlar" tanımlanmamış olup, kanun gerekçesinde ise yalnızca hedef sisteme entegre edilecek izleme yazılımının kullanılmasından bahsedilmektedir[141]. Bahse konu yazılımın, hedef kişinin bilgi teknolojisi sistemine sızması kastedilmektedir. Burada kullanılan yazılımlar genellikle "Federal Truva atları" olarak Türkçe'ye tercüme edebileceğimiz "Bundestrojaner" olarak adlandırılır. Bu ifade, önlemlerin başarısını tehlikeye atmamak için[142] kullanıcı tarafından açıkça tanınabilen bir işlevin yanı sıra gerçek amaçlarını gizleyen[143] truva atlarına bir göndermedir.

Online arama zaman alıcı ve yoğun hazırlık gerektiren bir önlemdir. Sızdırılan arama yazılımı, taktiksel soruşturma gerekliliklerine ve mahkeme kararının kapsamına uygun olarak her bir dosya için özel olarak geliştirilmelidir[144]. Bu çerçevede ilk olarak ilgili kişi tarafından kullanılan bilgisayar, akıllı telefon veya tablet gibi cihazların yanı sıra ağlar ve örneğin sistemde merkezi olarak, bilgisayarda yerel olarak veya bir bulutta harici olarak depolama konumları hakkında tüm bilgilerin toplanması önemlidir. Bu, güvenlik duvarlarının, işletim sistemlerinin ve antivirüs programlarının türü, sürümü, seviyesi ve güncelleme durumu dahil olmak üzere hedef sistemlerin donanım ve yazılım yapılandırması hakkında ayrıntılar sağlayan ortamın analiz edilmesiyle yapılır[145]. Hedef sistemin sürekli olarak izlenmesini sağlayan yazılımlara "Remote-Forensic-Software" denilir[146].

Soruşturma makamları gerekli kaynaklara sahipse ve yazılımı kullanma konusunda deneyimliyse, online arama yazılımı esnek bir şekilde tasarlanabilir ve böylece izlenen hedef sistemden gerekli olarak ortaya çıkan belirli somut olaylara uyarlanabilir. Bu aynı zamanda soruşturma dışındaki üçüncü kişileri korumak amacıyla önlemlerin ilgili kişi tarafından kullanılan sistemin bir bölümüyle, örneğin şirket ağıyla sınırlandırılmasını da mümkün kılabilir. İzleme yazılımının sistemi analiz etmesi, sisteme erişmesi, dizin genel görünümleri oluşturması, dizinleri ve bağlı veri taşıyıcılarını araması, belgeleri indirmesi, tuş vuruşlarını kaydetmesi, kendi izleme

[140] BTDrucks, 16/10121 S. 29.
[141] BTDrucks, 18/12785, 46.
[142] Roßnagel/Skistims, S. 3.
[143] Buermeyer, U.: Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, S. 155.
[144] Bundesregierung: Evaluationsbericht zu §20 k BKAG, 2017, S. 38.
[145] Kohlmann, 2012, S. 43.
[146] Derin/Golla, NJW 2010, 1111; Schlegel, GA 2007, S. 651.

yazılımının fark edilmeden silinmesi veya belirli bir süre sonra otomatik olarak devre dışı bırakılması gibi belirli işlevleri yerine getirmesi beklenilmektedir[147].

Bilgi teknolojileri sistemi üzerinde depolanan verilere erişmek için gerek sızılacak bilgi teknolojileri sistemine ilgili yazılımının yüklenmesi için gerekse ulaşılan verilerin aktarılması için internete bağlantı kurulması gerekmektedir[148]. Ancak bu durum, kullanıcının veya bilgisayar sahibinin uygun donanım bileşenleri veya örneğin bir güvenlik duvarı gibi yazılım programları aracılığıyla bilgisayarı dış müdahalelere karşı koruduğu güvenlik önlemleriyle engellenebilir[149].

C. Sisteme sızma (İnfiltrasyon) Yöntemleri

Online arama temelde iki ayrı tedbire ayrılabilir. Bunlar gerçek arama ve yedekleme şeklindeki birincil önlem ile sızma yoluyla gerçekleştirilen yazılım kurulumu şeklindeki ikincil önlemdir[150]. İnfiltrasyon olarak da adlandırılan sisteme sızma yöntemi, veri toplamaya eşlik eden bir müdahaledir. Düzenlemede herhangi bir yöntemin belirtilmemiş olmasıyla birlikte farklı yöntemlerle hedef sisteme sızılması mümkündür[151]. Bunlar iletişim hizmet tedarikçileri vasıtasıyla yazılım (software) modifikasyonu, programcılar ve üreticiler aracılığıyla yazılım veya donanım (hardware) modifikasyonu ile bilgi teknolojisi sistemine fiziksel müdahale yoluyla manuel kurulum olmak üzere üç gruba ayrılabilir.

1. Yazılım Modifikasyonu Yoluyla İnfiltrasyon

Yazılımı hedef sisteme yüklemek ve arka plan kurulumu için soruşturma makamları yazılımı iletişim hizmet tedarikçileri aracılığıyla kullanıcının kendi hatası veya sistemdeki bir güvenlik açığı nedeniyle veri sahibinin bilişim teknoloji sistemine iletebilir[152]. Kurulum daha sonra veri sahibinin katılımı ile veya katılımı olmadan tamamlanabilir. Bu örneğin, içeriği ilgili kişiyi ekteki ayrıntıları açmaya ve indirmeye ikna etmeye yönelik manipüle edilmiş e-postalar gönderilerek yapılabilir. Bu mesajların göndericisi soruşturma makamlarının kendisi, ayrı konular nedeniyle hedef

[147] Kohlmann, 2012, S. 44.
[148] Buermeyer, U.: Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, S. 155.
[149] Graf, §100b, Rn. 12.
[150] Sieber, Stellungnahme für BVerfG, S. 4.
[151] Löwe-Rosenberg StPO/Hauck, StPO § 100b Rn.103.
[152] Roßnagel/Skistims, S. 4.

kişiyle temas halinde olan diğer makamlar veya "sözde" güvenilir göndericiler olabilir[153].

Bununla birlikte internet sunucularının sağlayıcıları, ilgili kişi tarafından sayfa açıldığında yazılımı otomatik olarak indiren bir "script programı" depolayarak web sitelerini manipüle etmekten sorumlu tutulabilir[154]. Ancak bu infiltrasyon metodu oldukça tartışmalıdır, zira bu yöntem oltalama ("phishing"[155]) olarak adlandırılan suç teşkil eden davranışlar için kullanılmaktadır. Devlet burada esasen bir ikilemdedir. Zira bir yandan Federal Almanya Güvenlik ve Bilgi Teknolojileri Dairesi, siber suçların önlenmesi konusunda vatandaşlara, suç teşkil eden saldırılara ve internetten gelen tehlikelere karşı kendilerini korumak için savunma tedbirleri almalarını tavsiye etmektedir[156]. Öte yandan ise yetkililerin soruşturmalarını etkili bir şekilde ilerletebilmeleri için bu koruma mekanizmalarını yine kendileri aşabilmelidir. Eğer yetkililer kendi geliştirdikleri koruma mekanizmalarının üstesinden gelebilecek araçlara sahiplerse, bu koruma vatandaşların internet tabanlı güvenlik ihtiyaçlarını karşılamak için yeterli olmayabilir.

Yazılım modifikasyonu yöntemiyle sisteme sızma bakımından internet sağlayıcıların manipülasyon girişimlerinden ziyade, doğrudan sistemdeki güvenlik açıklarının dikkate alınarak ilgili açığa göre uyarlanmış ve soruşturulan kişinin yardımını gerektirmeyen özel yazılımların kullanılması daha uygun bir yöntem olarak değerlendirilmektedir. Bu durum "Exploits" olarak adlandırılan açıklardan "yararlanma" olarak tanımlanır[157].

Bilgi teknoloji sistemleri güvenlik duvarları, virüs tespit programları, erişim kontrolü ve benzeri bilinen güvenlik önlemlerinden bağımsız olarak güvenlikle ilgili açıklar içerir. Böyle bir güvenlik açığının tespit edilmesi halinde, ilgili ürünün üreticisine bildirilir veya ilgili forumlarda duyurulur. Bunun üzerine üreticiler güvenlik açıklarını düzeltme, yama veya güncelleme yoluyla birlikte yayınlar[158]. Bu doğrultuda hedef sistem derinlemesine analiz edilerek, güvenlik duvarı, işletim sistemi, virüs tarama programı, casus yazılım programı vb. gibi hedef sistemin

[153] BMI, Fragenkatalog des Bundesministeriums der Justiz, S. 14, Erişim: Fragenkatalog des Bundesministeriums der Justiz (netzpolitik.org), Erişim tarihi: 01.06.2024: 11.03.2024.
[154] Fox, Stellungnahme zur Onle Durchsuhcung, S. 6.
[155] Bu kavram "passwort" ve "fishing" terimlerinin birleşmesiyle ortaya çıkmıştır. Buna ilişkin detaylı açıklamalar için: Borges, Georg, Rechtsfragen des Phishing – Ein Überblick, NJW 2005, 3313.
[156] BSI, Sicher im digitalen Alltag - Informationen, Empfehlungen und Hilfe-zur-Selbsthilfe, Erişim: BSI - Tipps für mehr Sicherheit im digitalen Alltag (bund.de), Erişim tarihi: 01.06.2024: 11.03.2024.
[157] Baer, Wabnitz/Janovski, Handbuch Wirtschafts-und Steuerstrafrecht, Kapitel 14, Rn. 106.
[158] Pohl, DuD 2007, S. 685.

donanım ve yazılım yapılandırması hakkında ayrıntılı bilgi edinilmesi, analiz sonrası hangi boşlukların bulunduğu ve hangi yazılımın uygun olduğu tespit edilmelidir[159].

Bu bağlamda iki terim öne çıkmaktadır: "Zero-Day-Exploit" ile "Less-Than-Zero-Day-Exploit". Sıfırıncı gün saldırısı olarak Türkçe'ye tercüme edilebilecek "Zero-Day-Exploit", üretici tarafından bilinen ve yayınlanan güvenlik açıklarına yönelik saldırı programlarıdır[160]. Bu tür bir saldırının, henüz karşı önlemlerin alınmadığı ve güvenlik açıklarının devam etmesi halinde, bilgi teknoloji sistemlerinde başarılı olma olasılığı yüksektir[161]. Saldırının çoğunlukla açığın yayınlandığı gün gerçekleştirilmesi sebebiyle[162], "sıfırıncı gün" saldırısı terimi kullanılmaktadır[163]. Yazılım geliştiricinin güvenlik açığına uygun güncelleştirme yayınlamasıyla birlikte güvenlik açığı kapatılmış olur ve saldırı başarısız olur.

Bu saldırılar özellikle soruşturulan kişinin cihazlarında desteklenmeyen eski işletim sistemlerini kullanması veya işletim sistemini düzenli olarak güncellememesi durumunda hedef sisteme arama yazılımını bulaştırmak için uygundur[164]. Bu tür yazılım kurulumunda, daha uzun bir süre için belirlenmiş olan online arama tedbiri sırasında güvenlik açıklarının kapatılması riski bulunsa da sıfır gün açıklarının yayınlanmasının takriben 45 günlük bir gecikme ile gerçekleşmesi sebebiyle, üreticinin bu güvenlik açıklarını yama veya güncelleme şeklinde kapatmasının biraz zaman aldığı varsayılabilir[165]. Ancak buna rağmen sıfırıncı gün saldırılarının genelde saldırı yöntemi olarak tercih edilmediği ifade edilmelidir. Zira uzun süreli online aramalarda, açıkların yamalanma riski oldukça yüksektir[166]. Online aramanın tamamlanamadığı, daha doğrusu yarıda kaldığı hallerde, bu soruşturmaya harcanmış zaman, çaba ve ekonomik masraflar boşa gitmiş olacaktır.

"Sıfırıncı günden daha az saldırı" olarak Türkçe'ye tercüme edilebilecek olan "Less-Than-Zero-Day-Exploit" yararlanma yönteminde ise[167] üretici tarafından

---

[159] Bogk, Antworten zum Fragenkatalog, S. 10 f.
[160] Pohl, DuD 2007, S. 685.
[161]Topcu/Alzoubi/Elbasi/Camalan, Social Medai Zero-Day Attack Detection Using TensorFlow, Electronics 2023, S. 2, Erişim: https://doi.org/10.3390/electronics12173554, Erişim tarihi: 01.06.2024: 13.03.2024.
[162] Endres, Zero-Day-Exploit für Internet Explorer breitet sich aus, Erişim: Zero-Day-Exploit für Internet Explorer breitet sich aus | heise online, Erişim tarihi: 01.06.2024: 13.03.2024.
[163] Pohl, DuD 2007, S. 685.
[164] Pohl, DuD 2007, S. 685.
[165] Pohl, DuD 2007, S. 685.
[166] Pohl, DuD 2007, S. 685.
[167] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von IuK-Systemen, S. 5.

bilinmeyen ve yayınlanmamış olan güvenlik açıklarına saldırı söz konusudur. Dolayısıyla bu tür bir saldırı bir güvenlik açığı yayınlanmadan önce gerçekleştirilir[168].

Soruşturma makamları söz konusu güvenlik açıklarını ya kendi personelinin yardımıyla ortaya çıkarabilir -ki bunun uzman eksikliği nedeniyle zor veya çok zaman alıcı olduğu ifade edilmelidir- ya da bu alanda uzmanlaşmış kişi veya şirketlerden destek alınabilir[169]. Bu bağlamda soruşturma makamlarının çalışmalarında "exploit" kullanımının yaygın olduğu ve istihbarat servislerinin de bu araçları sıkça kullandığı ifade edilmektedir[170].

Üreticileri tarafından bilinmemeleri ve henüz yayınlanmamış olmaları sebebiyle keşfedildikleri anda neredeyse hiçbir koruma mümkün olmadığından, online arama yapmak için "Less-Than-Zero-Day-Exploit" yöntemi tercih edilmektedir[171]. Güvenlik duvarları, saldırı tespit veya saldırı önleme sistemleri gibi güvenlik yazılımları tarafından tanınmamaları sebebiyle, prensipte başarılı olabilmektedirler[172]. Üreticinin güvenlik açıklarını kapatmak için güncellemeler sağladığı takdirde, sızmanın başarılı olma olasılığı düşer. Bu durum genelde hızlı bir şekilde gerçekleştiğinden, soruşturmalar da hızlı bir şekilde ilerlemelidir[173].

Öğretide güvenlik açıklarının yazılım veya donanım üreticileri tarafından bilinmemesi ve özellikle devlet tarafından istismar edilmesi eleştirilmektedir.[174]. Devletin bu tür güvenlik açıklarını kapatmaya çalışması yerine, aksine siber suçlularla aynı şekilde vatandaşların bilgi teknoloji sistemlerine nüfuz edip bu açıkları kullanarak vatandaşlarının bilgi teknoloji güvenliğini koruma görevini ihmal etmesi doğru bulunmamaktadır[175]. Buna karşılık, güvenlik açıklarından yararlanmanın bilinen açıklarla sınırlı olması gerekmediği ileri sürülmektedir. Devletin koruma görevi kapsamında bu tür açıkları kapatmak için çalışmalar yürütmekle ve tespit edilen açıkların üreticilere bildirmekle yükümlü olduğu vurgulanmaktadır. Bu bildirme yükümlülüğüne rağmen güvenlik açıklarının devam etmesi halinde, görevi tam da bu tür güvenlik boşluklarını bildirmek olan soruşturma makamları tarafından bu açıkların kullanılabileceği savunulmaktadır[176].

---

[168] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von IuK-Systemen, S. 5.
[169] Pohl, DuD 2007, S. 685.
[170] Sieber, Stellungnahme zum Fragenkatalog, S.6.
[171] Pohl, DuD 2007, S. 686.
[172] Pohl, DuD 2007, S. 685.
[173] Bogk; Antworten zum Fragenkatalog, S. 10 vd.
[174] MüKoStPO/Rückert, StPO §100a Rn. 206 vd.
[175] MüKoStPO/Rückert, StPO §100a Rn. 206 vd.
[176] MüKoStPO/Rückert, StPO §100a, Rn. 208.

2. Yazılım ve Donanım Üreticileri Vasıtasıyla İnfiltrasyon

Bir diğer sızma yöntemi de henüz üretim aşamasındayken bilgi teknoloji sistemine "back doors"[177] adı altında bilinen arka kapıların yerleştirilmesidir. Böylelikle sisteme sonradan sızma gibi zor bir yola ihtiyaç duyulması önlenmiş olacaktır. Bu durumda soruşturma makamlarının erişimi daha sonra bir güncellemenin parçası olarak gerçekleşir. Hedef kişi tarafından kullanılan programlar bilinerek, güncelleme için sağlanan yazılım, indirme sonucunda gözetim yazılımının hedef sisteme otomatik olarak yükleneceği şekilde hazırlanabilir[178]. Bu yöntemin temel işlevi, adeta bilgi teknolojisi sisteminin başında oturuyormuş gibi internet üzerinden kaydedilmiş tüm verilere erişimin sağlanmasıdır[179].

Ancak bu yöntemin uygulanması kolay değildir, zira üreticiler müşteri memnuniyeti ve kendi karlılıkları sebebiyle bu tür değişiklikleri yapmayı istemeyecektir. Ayrıca, bu yaklaşım kötüye kullanım riskinin artmasına da yol açacaktır. Çünkü üreticiler tarafından uygun önlemler ancak izleme yazılımının bu amaçla kendilerine sunulması halinde alınabilir[180]. Ancak üçüncü tarafların yazılımın içeriğine ve tasarımına kontrolsüz erişimi, bilgi teknolojisi sistemlerinin gizliliğiyle bağdaşmamaktadır[181]. Sonuç olarak, bu yöntem uygulanabilir olmadığından uygun bir sızma yöntemi olmadığı söylenebilir.

3. Fiziksel Müdahale Yoluyla Manuel Kurulum

Bilgi teknolojisi sistemlerinin infiltrasyonu için başvurulabilecek daha gerçekçi ve üçüncü yol ise fiziksel müdahale yoluyla manuel kurulumdur. Burada birden fazla senaryo düşünülebilir.

Manuel kurulum, örneğin bir sınır kontrolü sırasında veya bilgi teknoloji sisteminin bulunduğu yere gizlice girilerek gerçekleştirilebilir[182]. Gizli soruşturmacıların usta kılığında sistemin bulunduğu binaya erişim sağlayarak yazılım yüklemeleri düşünülebilir[183]. Ayrıca üçüncü bir tarafın fiziksel sızmayı kasıtsız bir araç

[177] Buermeyer, HRRS, 4/2007, S. 157.
[178] Pfitzmann, Möglichkeiten und Grenzen der Nutzungsüberwachung von IuK-Systemen, S. 5.
[179] Buermeyer, HRRS, 4/2007, S. 157.
[180] Sinn, Stellungnahme zur BT-Drucksache 18/11272 sowie zur Ausschussdrucksache, S. 9 f; Pohl DuD 2007, S. 686.
[181] Sinn, Stellungnahme zur BT-Drucksache 18/11272 sowie zur Ausschussdrucksache, S. 9 f.
[182] Buermeyer, 2017, S.21.
[183] Derin/Golla, NJW 2019, 1112.

olarak gerçekleştirebileceği örnekler söz konusu olabilir. Bir şirket çalışanının promosyon hediyesi olarak aldığı bir USB bellek ile bir bilgisayara virüs bulaştırması buna örnek gösterilebilir[184].

Ancak soruşturulan kişinin konutuna girilip, yazılımın yüklenmesi online arama düzenlemesi kapsamına girmemektedir, zira mahremiyetin korunmasının önemi sebebiyle konut hakkının ihlali anayasa hukuku kapsamında ciddi bir müdahale teşkil etmektedir.

Bununla birlikte konutun aranmasına yönelik bir tedbirden faydalanarak da yazılımın gizlice konut içinde sisteme yüklenmesi yasal değildir. Arama ve el koyma gibi açık koruma tedbirleri, ilgili kişinin aramanın nedeninden ve uygulanmasından haberdar olmasıyla karakterize edilir. Temel haklara yönelik online arama gibi gizli bir müdahaleyle hedeflenen bir bağlantı bu gerekliliğe ters düşecektir[185].

D. İnfiltrasyon Sonrası Hedef Sistemden Veri Okuma ve Aktarma

Arama yazılımının başarılı bir şekilde kurulmasından ve sisteme sızılmasından sonra veri okuma ve aktarmanın teknik analizi, yöntemleri ile sınırları bu bölümde incelenecektir.

1. Veri Okuma ve Aktarmanın Teknik Analizi

Teknik olarak, "Remote Capture Unit" adı altındaki sızdırılmış izleme yazılımı ile hedef sistemdeki tüm veriler kopyalanır ve soruşturma makamlarına iletilir[186]. Soruşturma makamları "Recording Unit" adı altındaki izleme birimi ile sürekli temas halindedir[187]. İzleme yazılımı bu bağlamda bir DLL dosyası ve rootkit olarak adlandırılan iki bileşen içerir. DLL dosyası çeşitli işlevlerin bir araya getirilmesini temsil eder[188]. İzleme yazılımı hedef sisteme yüklenir yüklenmez aktif hale gelir ve kayıt ünitesiyle bağlantının bir internet bağlantısı üzerinden sürdürülmesi koşuluyla düzenli aralıklarla komut almaya hazır hale gelir[189]. Soruşturma makamları DLL dosyasını kullanarak hedef sistemdeki herhangi bir uygulamaya erişebilir ve

[184] Derin/Golla, NJW 2019, 1112.
[185] Derin/Golla, NJW 2019, 1113.
[186] Schaar, Bericht über Massnahmen der Quellen-TKÜ bei den Sicherheitsbehörden des Bundes, S.7.
[187] Buermeyer, HRRS 2007, S. 156, 161; Schaar, Bericht über Massnahmen der Quellen-TKÜ bei den Sicherheitsbehörden des Bundes, S.24.
[188] Küveler/Schoch, İnformatik für Ingenieure und Naturwissenschaftler, S. 128.
[189] Küveler/Schoch, İnformatik für Ingenieure und Naturwissenschaftler, S. 128.

gerektiğinde uzaktan kontrol edebilir. Rootkit ile hedef bilgisayardaki gözetimi gizlemek mümkündür[190]. Rootkit teknikleri, bir sistemi, kullanıcının bilgisayarda herhangi bir arka kapı veya kötü amaçlı yazılım olup olmadığını artık anlayamayacağı şekilde manipüle etmek için kullanılır[191].

Verilerin yazılım vasıtasıyla aktarılabilmesi için hedef sisteme bir internet bağlantısının kurulması şarttır[192]. Burada iki alternatif düşünülebilir. Birinci alternatifte, sistem internete bağlanır bağlanmaz veriler aktarılır. Ancak DSL bağlantısının düşük bant genişliğine sahip bir DSL bağlantısı olması halinde, arka planda büyük miktarda veri aktarırken devam eden internet faaliyetini, ilgili kişinin şüphelenmesine neden olacak kadar yavaşlatacaktır[193]. Diğer alternatifte ise yazılım kendi başına internete bağlanabilir ve ilgili kişinin cihazı kullanmadığı bir zamanda otomatik bir veri aktarımı gerçekleştirebilir. Ancak bu durumda, özel yönlendirici ayarları[194] veya güvenlik duvarları aktarımı engelleyebilir veya bir alarm bildirebilir.

Önemli başka bir husus ise aktarılan verilerin manipüle edilmediğinden veya değiştirilmediğinden emin olmak ve böylece verilerin kanıt değerini garanti etmek için çıkarılan verilerin yer ve zaman damgasının alınması gerekliliğidir[195].

2. Veri Okuma ve Aktarma Yöntemleri

Online aramanın amacı, öncelikle depolanan verilerin uygunluğunu değerlendirebilmek için veri taşıyıcılarının içindekiler tablosunun bir kopyasını ve ikincil olarak ilgili dosyaların bir kopyasını elde etmektir[196].

Bu doğrultuda arama yazılımının başarılı bir şekilde kurulmasından ve sisteme sızılmasından sonra, içerik yapılarını aktarabilmek için veri taşıyıcılarının içindekiler tablosuna erişilmelidir. Aktarım daha sonra internet üzerinden soruşturma makamının bir depolama sunucusuna yapılabilir. Bir sonraki adım ise içerik yapılarının analiz edilmesidir. Depolama sunucusunda depolanan veriler taşınabilir veri taşıyıcılarına

[190] Ccc.de, Analyse einer Regierungs-Malware, S. 17.
[191] Buermeyer, HRRS 2007, 157.
[192] Pohl, DuD 2007, S. 687.
[193] Kohlmann, 2012, S. 41.
[194] Türkçe karşılığı ile "yönlendirici" olarak ifade edilen router, kısaca iki ağ arasında güvenli bir şekilde veri aktarımı sağlamak için kullanılan donanımsal cihazlardır.
[195] Warken, NZWiSt 2017, 332.
[196] Pohl, DuD 2007, S. 685.

kaydedilir ve yetkililer tarafından çevrimdışı olarak analiz edilir. Analiz sonrası ilgili dosyalar içerik tablosundan seçilir ve hedef sistemden kopyalanır[197].

Sistemdeki veriler bir kereliğine ve tek tek seçilerek elde edilebilir. Bununla birlikte, süreç çevrimiçi bir sistem içinde daha uzun bir süre boyunca da devam edebilir[198] ve sistemde depolanan verilerin görüntülenmesinin yanı sıra "Daten-Monitoring" olarak adlandırılan online izleme de yapılabilmektedir[199].

Veriler bir aktarım işlemi sırasında, örneğin internette gezinirken veya bu verilerin kaydedilmesinden sonra soruşturma makamlarına aktarılabilir[200].

Online izlemenin sunduğu teknik olanaklar çok çeşitli olup, bunlardan bazılarına kısaca değinilecektir. Keylogger ("tuş vuruşu kaydedici") olarak adlandırılan bir cihaz kullanılarak şifre girişleri ile erişim kodları belirlenip kaydedilebilir ve soruşturma makamlarına iletilebilir[201]. "Canlı erişim" veya "izlenen kişinin omzunun üzerinden gizli bir sanal bakış" olarak tanımlanan bu veri toplama yöntemi yalnızca soruşturmayı ilgilendiren bilgileri toplamak için kullanılır ve kısa bir süre için hedef cihazda yalnızca düz metin olarak bulunan verilerin kaydedilmesine olanak tanır[202]. Bu da örneğin veri taşıyıcılarına el koyma tedbiri getirildikten sonra verilerin analiz edilmesini mümkün kılar[203].

Öte yandan, donanım arayüzlerine erişim de sağlanabilir. Örneğin, bir e-posta veya metin mesajı henüz oluşturulurken ekran görüntüleri veya ekranın video kayıtları alınabilir[204]. E-posta, SMS ve WhatsApp mesajları, fotoğraf dosyaları ve diğer sosyal medya hesap bilgileri gibi güncel veya geçmiş iletişim içerikleri iletilebilir[205]. Aynı durum bulutta depolanan ve izlenen bilgi teknoloji sistemi tarafından erişilebilen veriler için de geçerlidir.

Ayrıca kamera ve mikrofona uzaktan erişim, geçici veya devamlı olmak üzere görsel-işitsel gözetim için kullanılabilir[206]. Modern akıllı telefonlarda, tabletlerde, saat

---

[197] Pohl, DuD 2007, S. 686.
[198] Roggan, StV 2017, S. 825.
[199] BMI, Fragenkatalog des Bundesministeriums der Justiz, S. 6 f., Erişim: Fragenkatalog des Bundesministeriums der Justiz (netzpolitik.org), Erişim tarihi: 01.06.2024: 11.03.2024; Löwe-Rosenberg StPO, §100b, Rn. 106; Fox, DuD 2007, 828 vd.
[200] Gaehler, HRRS 2016, 341; Soine, NStZ 2018, 502.
[201] BT Drucks, 16/10121, S. 29.
[202] Buermeyer, 2017, S.5.
[203] Henzler zu BT-Druck 18/11272, S. 6; Roggan StV 2017, 825.
[204] Kruse/Grzesiek, S. 335.
[205] Roggan, StV 2017, 825.
[206] Buermeyer, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, 2 u.15.

ve hareket takip cihazlarında standart olarak bulunan GPS alıcısına erişerek tam konum verileri belirlenebilir, kalp atış hızı monitörü, adımsayar gibi sensör verilerinin[207] kaydedilmesi suretiyle hareket profilleri oluşturulabilir[208]. Ayrıca, sistemlerin çalışma belleğinde geçici olarak saklanan şifreler veya şifreleme kodları da okunabilir[209].

Sayılan erişim seçeneklerinden anlaşılabileceği üzere, bir kişinin izlenen bilgi teknolojisi sistemindeki neredeyse tüm kullanım davranışlarının belirlenebilmesi mümkündür[210]. Ancak ölçülülük ilkesi gereği elde edilen verilerin sadece soruşturmayı ilgilendiren verilerle sınırlı olması ve özel hayatın temel alanının korunması gerektiği unutulmamalıdır[211]. Ayrıca aktarılan verilerin değiştirilmeye, yetkisiz silinmeye ve yetkisiz erişime karşı en son teknolojiye uygun olarak korunması gerektiği de belirtilmelidir[212].

3. Veri Okuma ve Aktarmanın Sınırları

Online aramaların sınırlayıcı teknik faktörleri arasında öncelikle hedef sistemin internete kısıtlayıcı bir bağlantı politikası veya örneğin kullanılmama halinde olduğu gibi fiziksel olarak bağlantının kesilmesi yer almaktadır[213]. Hedef sistemin mevcut bant genişliği de sınırlayıcı bir etkiye sahiptir. Örneğin, tüm hedef sistemlerin DSL bağlantısına[214] sahip olduğu varsayılamaz. Ayrıca, diskler ve işlemci her zaman son teknoloji ürünü olmayabilir. Bu nedenle iletim kapasitesi, hesaplama süresi ve depolama kapasitesi gibi mevcut kaynaklar kısıtlı bir şekilde kullanılmalıdır[215].

Ayrıca, online arama sırasında sistemsel bildirimler önlenmeli veya zamanında tamamen silinmelidir. Hedef sistem fark etmeden çevrimiçi aramayı gerçekleştirmek için rootkit teknikleri gibi çeşitli teknikler kullanılmalıdır[216]. Online aramanın hedef sistemde tespit edilmemesi garanti edilemediğinden, depolama sunucusunun yüksek düzeyde korunarak tespit edilmesi, arama yetkisinin izinin sürülmesi ve tehlikeye

[207] Lüdemann, ZD 2015, 247.
[208] Kruse/Grzesiek, S. 335.
[209] Henzler zu BT.-Druck 18/11272, S.9.
[210] BT-Druck 18/12785, S.54; MüKo StPO/Rückert, §100b Rn. 43.
[211] Soine, NStz 2018, 502.
[212] Graf, §100b, Rn. 30.
[213] Pohl, DuD 2017, S. 686.
[214] DSL (Digital Subscriber Line), dijital abone hattı anlamına gelir. DSL, internet bağlantısı sağlamak için kullanılan bir teknolojidir. Telefon hatları üzerinden çalışan DSL teknolojisi, daha hızlı bir internet bağlantısı sunarak, yüksek hızda internet erişimi sağlar.
[215] Pohl, DuD, S. 686.
[216] Bachfeld, 2005.

atılması zorlaştırılmalıdır. Bu, örneğin yurtdışında tanımlanamayan dinamik bir IP adresi kullanarak ya da sunucuyu kullanılmadığı zamanlarda fiziksel olarak kapatarak başarılabilir[217].

Depolama sunucusunun tanımlanmasını ve harici saldırıları önlemek için kaydedilen veriler yalnızca bir kez yazılabilen ve bu sistemde okunamayan bir veri taşıyıcısında saklanmalı ve sonrasında çevrimdışı olarak analiz edilmelidir[218].

Bilgisayar veya akıllı telefon gibi bir bilgi teknoloji sisteminin kamera veya mikrofon işlevlerinin gizlice etkinleştirilmesi online arama kapsamına girmemektedir[219]. Kanun gerekçesinde bir kişinin tüm kullanım davranışının izlenmesi gerektiği ve bunun kullanıcının görsel olarak gözlemlenmesini de içerebileceği belirtilmiş olsa da[220] online arama düzenlemesi gereği verilerin bilgi teknolojisi "sisteminden" sadece elde edilebileceği düzenlenmiştir[221]. Bu da soruşturma makamları tarafından aktif bir eylemin gerçekleştirilmesine olanak tanımamaktadır[222]. Buna ek olarak, "arama" teriminin, belirli işlevleri etkinleştirmeyi kapsamadığını, sadece pasif olarak bilgi edinme yetkisinin söz konusu olduğunu açıkça ortaya koyduğu savunulmaktadır[223].

Ancak izlenen kişinin kamera veya mikrofon sensörlerini kendi başına aktif hale getirmesi ve sistemin verileri bu nedenle işlemesi durumunda, bu verilerin elde edilip aktarılmasına engel bulunmamaktadır[224]. Bununla birlikte, hedef cihazdaki izleme yazılımı tarafından belirli bir işlevin etkinleştirilmesini öneren bir sistem mesajı oluşturabilir ve kullanıcı bilgi teknolojisi cihazındaki bir sensörü açmaya yönlendirilebilir. Soruşturma makamlarının bu tarz "kriminal kurnazlık" kullanarak yönlendirme yapmaları da online arama düzenlemesi kapsamına girmektedir.[225]

Sisteme sızdırılan yazılım en iyi senaryoda tüm ilgili verileri toplayıp iletecek ve ilgili olmayan verileri göz ardı edecek şekilde programlanmıştır. Bütün verilerin düzenli olarak iletilmesi hedeflenemez ve ilgili kişinin soruşturmayla ilgili olmayan verilerinin de korunması gerekir. Bu, iletilecek verilerin önceden seçilmesini

[217] Pohl, DuD, S. 686.
[218] Pohl, DuD, S. 686.
[219] Roggan StV 2017, 826.; Sinn zu BT-Dr. 18/11272 S. 10.
[220] BT-Druck, 18/12785, S. 59.
[221] StPO §100b/1 gereği: "…. dürfen Daten **daraus** erhoben werden, …"
[222] Meyer-Gossner/Schmitt, StPO §100b, Rn.2.
[223] Roggan, StV 2017, 821; Meyer-Gossner/Schmitt, StPO §100b, Rn.2.
[224] MüKoStPO/Rückert, §100b, Rn. 46.
[225] Soine, NStZ 2014, 248.

gerektirmektedir ki bu da kolay olmamaktadır zira verilerin önem düzeyi genellikle toplama sırasında değil veri değerlendirme aşamasında ortaya çıkmaktadır[226].

Bu teknolojiyle bağlantılı olarak ortaya çıkan soru, sadece ilgili verilerin okunmasının ve iletilmesinin nasıl garanti edilebileceği ve hatta bunun mümkün olup olmadığıdır. Çevrimiçi aramaların kullanımından kaynaklanan bir sorun, yetkisiz bir üçüncü kişinin müdahale etme veya bu yetkisiz kişinin güvenlik açıklarından yararlanma olasılığıdır ki bu ciddi bir sorun teşkil etmektedir. Sızmanın istenmeyen sonuçları, ilgili yazılımın bilgi teknolojisi sistemine yüklendiği etkilenen tarafın (yanlışlıkla) yazılımı yetkisiz üçüncü taraflara iletmesi durumunda da ortaya çıkabilir.

4. Aktarım sonrası veri analizi

Online aramadan elde edilen verileri analiz etmek için genellikle olağan adli bilimsel yöntemler kullanılır. Toplanan veriler harici depolama konumundan taşınabilir bir veri taşıyıcısına kopyalanır ve yetkililer tarafından çevrimdışı olarak analiz edilir[227]. Hangi süreçlerin personel tarafından değerlendirileceğine ve hangilerinin otomatik olarak analiz edilebileceğine duruma göre karar verilmelidir. Verilerin delil toplama amacına hizmet edip etmediği kontrol edilmeli ve delil değerlendirme zorluklarının ortaya çıkabileceği göz önünde bulundurulmalıdır[228].

Aktarılmış veri kayıtları, veri kaynağına bağlı olarak çok çeşitli veri formatlarında bulunabilir. Bunlar örneğin bilgisayarlar, tabletler, mobil cihazlar, yönlendiriciler, sosyal ağlar, akış hizmetleri, internet platformları, telekomünikasyon baz istasyonları veya depolama ortamları, video gözetim kameraları, muhasebe sistemleri veya banka hesapları gibi veri kaynakları olabilir[229]. Farklı veri formatları çeşitli işletim ve dosya sistemleri ile uygulama programlarından da kaynaklanabilir. Veri kayıtları, genellikle belirli veri paketleri için ek bilgi olarak otomatik olarak oluşturulan meta verileri de içerebilir[230]. Toplanan veriler ZIP dosyaları olarak sıkıştırılmış biçimde de mevcut olabilir.

Ham malzemeyi analiz edilebilir bir forma dönüştürmek için hem ilgili yazılım hem de ilgili bilgi teknolojisi bilgisi gerekli olup, ara adımların genelde manuel olarak uygulanması gerekmektedir. Ancak bu durum zaman alıcı ve yoğun emek gerektiren

[226] Rehak, 2011, S. 27.
[227] Kohlmann, 2012, S.46.
[228] Kohlmann, 2012, S.46.
[229] Warken, NZWiSt 2017, 330.
[230] Warken, NZWiSt 2017, 331.

işlemlere yol açmaktadır. Daha ileri adli analiz ve içerik değerlendirmesinin yapılabilmesi için verilerin okunabilir bir hale getirilmesi ana gerekliliklerdendir[231].

Verilerin analizinde başka bir zorluk ise sistemlerde ilgili kullanıcı tarafından kaydedilmiş şifrelenmiş veriler olup, bunların çözümü ise kullanılan kriptografik yönteme bağlıdır. Şifrelenmiş verilere ek olarak sistemde şifre öncesinde "keylogger" tarafından kaydedilmemiş kullanıcı şifreleri bulunuyorsa, şifrelerin çözümü daha karmaşık hale gelebilir.

Bulut bilişim sisteminden veya benzeri toplu depolama sistemlerinden aktarılan verilerin, orijinal olarak kaydedilen verilerle örtüşüp örtüşmediğini kontrol etmek ayrı bir zorluktur, zira depolama alanlarındaki veriler otomatik ve dinamik olarak kaydedilen verilerden oluşmaktadır.

Bununla birlikte "büyük veri (big data)" olarak kategorize edilebilecek büyük miktarlardaki veriler, yalnızca veri çıkarma açısından teknik zorluklar yaratmakla kalmaz, aynı zamanda veri kayıtlarını analiz ederken zaman gereksinimlerinin artmasına da neden olur[232]. Ayrıca, kişisel verilerin korunması bu bağlamda yasal bir endişe kaynağıdır[233].

5. Online aramanın sonlandırılması ve raporlama gerekliliği

Online arama tedbiri tamamlandığında, tüm önlemler derhal sonlandırılmalıdır. Bunun sonucunda sızdırılmış olan arama yazılımının hedef sistemden kaldırılması gerekmektedir[234]. Yazılımın sistemden kaldırılması teknik olarak farklı yollarla mümkün olup, yazılımının ya silme komutunu kabul etmesi ya da otomatik olarak silme komutunun yazılıma entegre edilmiş olması söz konusu olabilir. Yazılım tarafından sonlandırmanın mümkün olmadığı hallerde ise fiziksel erişim gerekli olabilmektedir.

Sızılan sistemin mümkünse eski haline getirilmesi, veri sahibinin bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü güvence altına alma temel hakkına yapılan müdahaleyi sona erdirir. Bu tedbir aynı zamanda kullanılan kolluk soruşturması metodolojisinin yetkisiz erişimden korunmasına da hizmet eder. Buna ek

[231] Warken, NZWiSt 2017, 331.
[232] Europol, IOCTA 2016, S. 53 f.
[233] Europol, IOCTA 2016, S. 54; Graf, 50. Edition, §100b Rn. 33.
[234] Kohlmann, 2012, S. 45.

olarak, üçüncü tarafların sisteme yetkisiz erişim sağlamasını ve buradaki verilere erişmesini önlemek amaçlanmaktadır[235].

Bilgi teknoloji sisteminin işlevselliğinin kalıcı ve önemli ölçüde bozulma ihtimali olsa dahi, yapılan değişiklikler yine de geri alınmalıdır[236].

Ayrıca online arama tedbirinin uygulanması bakımından raporlama koşulu getirilmiştir. İlgili kişinin temel haklarının etkili bir şekilde korunmasını ve mahkemede toplanan delillerin güvenilirliğini sağlamak için teknik araçlar kullanılırken, özel raporlama düzenlemelerine uyulmalıdır[237]. İzlenebilirliği sağlamak için özellikle aşağıdaki adımlar kaydedilmelidir:

- Teknik araçların tanımı ve kullanım zamanı.
- Bilgi teknolojisi sisteminin ve bu sistemde yapılan geçici olmayan değişikliklerin tanımlanmasına ilişkin ayrıntılar.
- Toplanan verilerin belirlenmesini mümkün kılan bilgiler.
- Tedbiri gerçekleştiren organizasyonel birim[238].

V. Hukuki Niteliği

Online Arama tedbirinin hukuki niteliğini ortaya koymadan önce genel olarak koruma tedbirlerinden bahsetmekte fayda bulunmaktadır. Bu çerçevede genel olarak koruma tedbiri kavramına, çeşitlerine ve ortak özelliklerine değinildikten sonra, koruma tedbirlerine ilişkin koşullar online arama bakımından incelenecek ve diğer koruma tedbirleri ile karşılaştırılacaktır.

[235] Soine, NStZ 2018, Rn. 502.
[236] Soine, NStZ 2018, Rn. 502.
[237] Graf, 50. Edition, §100b Rn. 34; Soine, NStZ 2018, Rn. 502.
[238] Graf, 50. Edition, §100b Rn. 35; Soine, NStZ 2018, Rn. 503.

A. Genel Olarak Koruma Tedbirleri

1. Koruma Tedbiri Kavramı

Ceza Muhakemesi hukukunun temel bir gereği olarak maddi gerçeğe ulaşılabilmesi, hükmün verilebilmesi ve verilen kararın icra edilebilmesi için temel hak ve özgürlükleri kısıtlayan ve hükümden önce yetkili merciler tarafından verilen ve geçici niteliği haiz, birtakım önlemlere başvurulması gerekmekte olup, bu önlemlere koruma tedbiri adı verilmektedir[239].

Öğretide koruma tedbirleri terimi hakkında bir görüş birliği bulunmamakta olup, söz konusu tedbirler için ihtiyati tedbir, usul tedbirleri, zorlayıcı önlem, ceza yargılaması önlemi gibi terimler kullanılmaktadır[240]. 5271 sayılı Ceza Muhakemesi Kanunu'nda "koruma tedbirleri" terimine yer verilmiştir.

Koruma tedbirinin amacı ceza muhakemesi hukukunu işlevsel kılmak ve yargılama neticesinde ortaya çıkan hükmün icra edilebilmesine olanak sağlamaktır. Bununla birlikte koruma tedbirlerinin yargılamadan önce delillerin yok edilmesini ve sanığın kaçmasını önleyici bir özelliğinin de bulunduğu ifade edilmelidir[241]. Bu amaçlara ulaşılabilmesi için koruma tedbirlerine gerek soruşturma gerekse kovuşturma evrelerinde kural olarak hâkim kararı ile başvurulabilirken, kanunda düzenlenmiş olan bazı durumlarda gecikmede sakınca bulunan hallerde Cumhuriyet Savcısının kararı ile başvurulması mümkündür[242].

Koruma tedbirleri kesinleşmiş bir mahkeme hükmü olmadan insan hak ve özgürlüklerine önemli sınırlamalar getirdiği için sadece kanunlarda değil milletlerarası sözleşmelerde ve anayasalarda da düzenlenmiştir. Bunun sebebi insan hak ve özgürlüklerini etkili bir biçimde korumaktır[243].

Koruma tedbirlerinin temel hak ve özgürlükler bakımından müdahale oluşturması sebebiyle, bu tedbirlere ancak zorunluluk bulunduğu hallerde başvurulması gerekir. Bunun neticesinde, bir yandan katalog uygulamasıyla bazı

---

[239] Bahri Öztürk/Behiye Eker Kazancı/Sesim Soyer Güleç, Ceza Muhakemesi Hukukunda Koruma Tedbirleri, 5. Bası, Ankara 2022, s. 29; Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/ Saygılar, Yasemin F./Alan, Esra/ Özaydın, Özdem/ Erden Tütüncü, Efser/ Can Tok, Mehmet, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 17. Baskı, Ankara 2023, s. 443; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, Ceza Muhakemesi Hukuku, 16. Baskı, Ankara 2023, s. 233.
[240] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 443.
[241] Şahin, Cumhur/Göktürk, Neslihan, Ceza Muhakemesi Hukuku I, 12. Baskı, Ankara, Seçkin Yayınları, 2021, s.263.
[242] Öztürk, Kazancı, Güleç, s.38.
[243] Gökçen/Balcı/Alşahin/Çakır, s. 388.

koruma tedbirlerinin uygulama alanına kanunla sınırlama getirilmiş, katalog öngörülmeyen hallerde ise, soruşturma ve kovuşturma evrelerinde herhangi bir tedbirin uygulanmasının uygunluğu ve gerekliliğinin değerlendirilmesi gerekmektedir[244].

Koruma tedbirleri kendisi ile bir takım ortak özellikleri bulunan önleyici tedbirlerle karıştırılmamalıdır. Önleme amaçlı bu tedbirler, henüz suç işlenmeden müdahalede bulunarak bir suçun işlenmesini önleme ve böylece doğacak tehlikeyi en baştan engelleme ve istihbari bilgi toplama hedefine yöneliktir. Dolayısıyla önleyici tedbirler suç şüphesi bulunmamasına rağmen bir tehlikenin ortadan kaldırılması amacıyla başvurulan tedbirler olarak tanımlanabilir. Örneğin PVSK'nın bazı maddelerinde "durdurma, kimlik sorma ve önleme araması" gibi önleyici tedbirler düzenleme altına alınmıştır[245].

Çalışmamızın devamında online aramanın benzer koruma tedbirleri ile mukayesesinde önleme amaçlı ve adli amaçlı tedbirlere ayrı ayrı değinilecektir.

2. Koruma Tedbirlerinin Çeşitleri

5271 sayılı Ceza Muhakemesi Kanunu'nda "Koruma tedbirleri" başlıklı 4. Kısımda düzenlenmiş olan koruma tedbirleri kişi özgürlüğünü sınırlayanlara öncelik verilmek suretiyle, zaman yönünden kronolojik bir sıraya göre sistematize edilmiştir[246].

Hukukumuzda koruma tedbirlerinin pek çok çeşidi bulunmaktadır. Bunlar; yakalama, tutuklama, zorla getirme, arama ve elkoyma gibi "klasik koruma tedbirleri" ile beden muayenesi, fizik kimliğinin tespiti, iletişimin denetlenmesi, gizli soruşturmacı, teknik araçlarla izleme gibi "modern koruma tedbirleri"dir[247]. Modern koruma tedbiri olarak nitelendirilen bu yeni delil elde etme yöntemleri "delilden sanığa giderek maddi gerçeğe ulaşılması" ilkesinin kolaylaştırıcı bir unsuru haline gelmiştir[248].

Koruma tedbirlerini gerek kişi özgürlüğü ve vücut bütünlüğü, özel hayatın gizliliği, mülkiyet veya konut dokunulmazlığı hakkı gibi müdahale teşkil ettikleri

[244] Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s.263, 264.
[245] Veli Özer Özbek, Polis Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler: Önleyici Tedbirler – Açık ve Gizli Koruma Tedbirleri, Seçkin, Ankara, 2021, s. 32, 33; Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 444.
[246] Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s.264 vd.
[247] Öztürk/Kazancı/Güleç, s. 30.
[248] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447.

hukuki değere göre[249] gerekse uygulanabilecekleri kişilere göre sınıflandırmak mümkündür. Soruşturma evresinde şüpheliye, kovuşturma evresinde sanığa yönelmiş olabilecekleri gibi, herhangi bir suç isnadı altında bulunmayan üçüncü kişilere yönelik olarak da uygulanabilirler. Örneğin yakalama ve tutuklama tedbirleri salt şüpheli veya sanığa karşı uygulanabilecek tedbirler iken, bazı hallerde arama ve elkoyma tedbirlerinin üçüncü kişilere yönelik olarak uygulanması da mümkündür.

3. Koruma Tedbirlerinin Ortak Özellikleri

Koruma tedbirlerine başvurmanın hukuka uygun olabilmesi için, bazı temel koşulların gerçekleşmiş olması gerekir. Bu koşullar koruma tedbirlerinin ortak özellikleri olarak, "yasal dayanak bulunması, şüphelerin belli bir yoğunlukta olması, hükümden önce temel bir hakkı sınırlaması, geçici olması, gecikmede sakınca bulunması, yetkili merci kararı ve ölçülülük ilkesi" başlıkları altında incelenecektir.

a. Yasal Dayanak Bulunması

Koruma tedbirlerinin uygulanması insan haklarına ve kişilerin temel hak ve özgürlüklerine bir müdahale teşkil ettiğinden, ancak yasalarda öngörülen durumlarda başvurulabilen bir yoldur. Bu nedenle sınırlamaya izin veren bir yasal dayanağın bulunması gerekmektedir[250]. Ayrıca yasanın ulaşılabilir ile anlaşılabilir ve de gerçekleştirilen sınırlamanın yasaya uygun olması zorunluluğu da vardır[251]. Anayasa'nın 13. maddesinde belirtilmiş olduğu üzere *"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir".*

Yasada yer verilmemiş koruma tedbiri kıyas yoluyla uygulanamayacağı gibi, bir koruma tedbiri için yasada aranan şartlar da kıyas yoluyla genişletilemez[252]. Kıyas, kanunda öngörülen durumlara ilişkin düzenlemeleri, kanunda öngörülmeyen benzer durumları kapsamına alacak şekilde genişleterek bu durumların çözümlenmesidir[253].

---

[249] Nur Centel/Hamide Zafer, Ceza Muhakemesi Hukuku, Seçkin Yayınevi, 13. Bası, İstanbul 2016, s. 319; Murat Volkan Dülger/Şaban Cankat Taşkın, Ceza Muhakemesi Hukuku, 2023, 1. Baskı, s. 344, 345.
[250] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 446; Şahin, Göktürk, Ceza Muhakemesi Hukuku I, s. 263.
[251] Öztürk, Kazancı, Güleç; s. 31.
[252] Şahin, Ceza Muhakemesi Hukuku I, s. 267.
[253] Toroslu, Nevzat, Ceza Hukuku Genel Kısım, Savaş Yayınları, 14. Baskı, Ankara, 2009, s. 61.

b. Hükümden Önce Temel Bir Hakkı Sınırlaması

Koruma tedbirleri ile hakkında tedbir uygulanacak kişilerin temel hak ve özgürlüklerinden birine veya birkaçına sınırlama getirildiği kabul edilen bir gerçektir[254]. Bu nedenle koruma tedbirleri bakımından bireylere sağlanan güvenceler konusunda titizlikle hareket edilmesi gerekir[255].

Bu doğrultuda kesinleşmiş bir yargı kararı olmadan örneğin arama tedbiri uygulanarak beden bütünlüğü, özel yaşam ve konut dokunulmazlığı, elkoyma tedbiriyle mülkiyet hakkına, yakalama/gözaltı veya tutuklama tedbiriyle kişi özgürlüğüne, iletişimin denetlenmesi suretiyle haberleşme özgürlüğüne bir müdahale gerçekleşmektedir[256].

Devletin koruma tedbirleri ile temel hak ve özgürlüklere müdahale etmesinin sebebi, şüpheli ya da sanıkların işledikleri suçun aydınlatılmasının, ispatlanmasının mümkün olabilmesidir[257].

c. Şüphelerin Belli Bir Yoğunlukta Olması

Koruma tedbiri uygulandığı evrede tedbirin uygulanmasının haklılığı noktasında kesin bir kanıya ulaşmak mümkün değildir. Bu ancak yargılamanın neticesinde ortaya çıkacaktır. Ancak her şüphe halinde de bu tedbire başvurmak hukuka uygun olmayacaktır[258]. Bu nedenle tedbirin uygulanabilmesi için şüphenin belli bir yoğunlukta olması gerekmektedir.

(1) Şüphe Kavramı

Şüphenin ansiklopedik anlamı, *"zihnin birçok düşünce arasında bir tercih yapmasında duraksamasıdır"* şeklindedir[259]. Diğer bir ifadeyle, iki kanıyı destekleyen nedenlerin eşit görünmesi sonucunda seçim yapılamaması durumuna *"şüphe"* denmektedir[260].

---

[254] Ahmet Gökcen, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma (Özellikle Telefonların Gizlice Denetlenmesi), 1.baskı, Ankara: Dokuz Eylül Üniversitesi Hukuk Fakültesi Döner Sermaye İşletmesi Yayınları, 1994, s.19; Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 446.

[255] Öztekin Tosun, Türk Suç Muhakemesi Hukuku Dersleri, C.1, 4.basım, İstanbul: Acar Matbaacılık, 1984, s.912.

[256] Öztürk, Erdem, Tezcan, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s.446.

[257] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakmesi Hukuku, s. 390.

[258] Öztürk, Erdem, Tezcan, Nazari ve Uyulamalı Ceza Muhakemesi Hukuku, s.444.

[259] Ejder, Yılmaz, Hukuk Sözlüğü, 7. Baskı, Ankara, Yetkin Yayınları, 2002, s.1157.

[260] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 444.

Koruma tedbirine başvurma esnasında, henüz tedbirin uygulanmasının haklılığı kesinleşmiş bir durumda olmadığı ve bu doğrultuda neticeye ancak yargılamanın sonucunda ulaşılabileceği ifade edilmelidir. Dolayısıyla her zaman tedbirin yanlış yere uygulanması ihtimali de var olup, koruma tedbirine başvuruda görünüşte haklı olma ile yetinme zorunluluğu bulunmaktadır[261].

Bu bağlamda ceza muhakemesi hukukunda şüphe soruşturmanın başında yetkili merciinin birtakım delillere dayanan tahmini olarak karşımıza çıkarken, daha sonraki evrelerde iddia ve savunmayı destekleyen delillerin yetkililerce eşit görülmesi olarak belirtilebilir[262].

Mevcut vakıadaki verilerin ikna edicilik derecesine göre; basit, makul, yeterli veya kuvvetli olmak üzere şüphe çeşitleri ortaya çıkmaktadır[263].

(2) Şüphenin Çeşitleri

(a) Basit Şüphe

Başlangıç şüphesi olarak tanımlanabilen basit şüphe, cumhuriyet savcısı tarafından soruşturma başlatılması için gerekli olan şüphe derecesini ifade eder[264]. Basit şüphe, bir suçun işlendiği izlenimi veren bir hal olup[265], dayandığı deliller, basit, yetersiz ve/veya sayıca az olan şüphe olarak tanımlanır[266]. Bu şekilde belirli olaylara ve belirti şeklindeki delillere dayanmayan, yalnızca tahmine dayanan şüphe ile soruşturmaya başlanması hukuka aykırı olarak kabul edilip, bu durumun soruşturma başlatılması için yeterli sayılması keyfiliğe yol açacaktır[267].

(b) Makul Şüphe

Basit şüpheyi takip eden bir sonraki şüphe derecesi olarak makul şüphe kabul edilmektedir. Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphe olarak tanımlanabilir[268]. Özellikle yakalama ve gözaltına alma tedbirleri bakımından bunlara karar verilmesi için aranan şüphe derecesi olan makul şüphe, bir kişinin suç işlemiş olabileceği hususunda objektif bir gözlemciyi ikna

---

[261] Nur Centel, Hamide Zafer, Ceza Muhakemesi Hukuku,12.Baskı, Ankara, Beta Yayınevi, 2015, s.96.
[262] Öztürk, Tezcan, Erdem, Nazari ve Uyulamalı Ceza Muhakemesi Hukuku, s. 444
[263] Öztürk, Kazancı, Güleç, s. 34 vd.
[264] Dülger/Taşkın, s. 352.
[265] Özbek/Doğan/Bacaksız/ Ceza Muhakemesi Hukuku, s. 234.
[266] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 445; Öztürk, Kazancı, Güleç, s. 34.
[267] Dülger/Taşkın, s. 352.
[268] Özbek/Doğan/Bacaksız/ Ceza Muhakemesi Hukuku, s. 235.

etmeye yeterli olgu ve bilgilerin var olmasıdır[269]. Bu çerçevede şüphenin somut olgulara dayanması ve ihbar veya şikâyeti destekleyen emarelerin de bulunması gerektiği belirtilmelidir[270].

(c) Yeterli Şüphe

Yeterli şüphe, iddianamenin düzenlenebilmesi ve kamu davasının açılabilmesi için gerekli olan şüphe olarak kabul edilip, yapılacak olan yargılama sonucunda şüpheli veya sanığın mahkûm olma ihtimalinin beraat etme ihtimalinden daha yüksek olması halini ifade eder[271].

CMK m. 170/2 gereği, soruşturma evresi sonunda toplanan delillerin, suçun işlendiği bakımından yeterli şüphe oluşturması halinde, Cumhuriyet savcısı tarafından bir iddianamenin hazırlanması düzenlenmiştir.[272] Ancak bahsedilen bu düzenleme dışında yeterli şüphenin koruma tedbirleri için aranan şüphe dereceleri arasında belirtilmediği vurgulanmalıdır. Bu nedenle yeterli şüphenin, basit makul veya kuvvetli şüphe kavramları gibi sistematik olarak koruma tedbirlerine ilişkin bir şüphe derecesi teşkil etmediği ifade edilmektedir[273].

(d) Kuvvetli Şüphe

Kuvvetli şüphe, somut delillerin dikkate alınması suretiyle yapılacak yargılama sonucunda şüpheli veya sanığın mahkûm olma ihtimalinin kuvvetle muhtemel olması olarak tanımlanır[274]. Kuvvetli şüphe temel hak ve özgürlüklere ciddi bir müdahale teşkil eden ve derinden etkileyen koruma tedbirlerine karar verilmesi bakımından aranan şüphe derecesidir[275].

Bu nedenle özellikle CMK m. 90 gereği yakalama, CMK m. 100 gereği tutuklama, CMK m. 109 adli kontrol, CMK m. 135 iletişimin tespiti ve CMK m. 139 teknik araçlarla izleme tedbirlerinde kuvvetli şüphenin varlığı aranmaktadır[276].

---

[269] Dülger/Taşkın, s. 352.
[270] Özbek/Doğan/Bacaksız/ Ceza Muhakemesi Hukuku, s. 235.
[271] Öztürk, Kazancı, Güleç, s. 35; Özbek/Doğan/Bacaksız/ Ceza Muhakemesi Hukuku, s. 234.
[272] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 445.
[273] Dülger, Taşkın, s. 352, 353.
[274] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 445; Öztürk, Kazancı, Güleç, s. 35; Özbek/Doğan/Bacaksız/ Ceza Muhakemesi Hukuku, s. 234.
[275] Dülger, Taşkın, s. 353.
[276] Öztürk, Kazancı, Güleç, s. 35; Dülger, Taşkın, s. 354.

(3) Geçici Olması

Koruma tedbirleri sürekli değil, geçici nitelikte önlemlerdir[277], zira bu tedbirlere bir delil elde etmek, elde edilmiş bir delili ya da muhakeme için gerekli bir kişiyi korumak için başvurulur[278]. Koruma tedbirleri ile sağlanmak istenen amaç gerçekleşince ve gerçekleşmeyeceğinin anlaşılmasıyla sona erer[279]. Aksi düşünüldüğünde temel hak ve özgürlüklerin belirsiz sürelerce kısıtlanması gündeme gelir ve bu durum hukuk devleti ilkesiyle bağdaşmaz[280].

Buradan anlaşılacağı üzere, koruma tedbirinin hüküm verilinceye kadar uygulanması gibi bir kural yoktur[281]. Bu koruma tedbirlerinin araç olma özelliğinin de bir gereğidir[282]. Amaç sona erdiğinde aracın kullanılmasına da gerek kalmaz. Ayrıca durum ve şartların, tedbirin tamamen kaldırılmasına olanak vermediği hallerde daha hafifi uygulanabileceği gibi daha ağır tedbire de başvurulabilir.

(4) Gecikmede Sakınca Bulunması

Tedbire başvurulmazsa tedbirle ulaşmak istenen faydanın daha sonra elde edilmesinin imkânsız veya çok güç olması halinde koruma tedbirine başvurmada yaşanan gecikmenin tehlike doğurduğu kabul edilir[283]. Bu durumda, tedbirin uygulanması bir zorunluluktur[284]. Gecikmede tehlike bulunup bulunmadığı, her somut olayda olayın özellikle dikkate alınarak değerlendirilmelidir[285]. Ayrıca tehlikenin yakın olması şartı da aranmaktadır[286].

(5) Yetkili Merci Kararı

Koruma tedbirlerinin temel hak ve özgürlüklere getirdikleri sınırlama gereği mutlaka bir karara dayanmaları gerekmektedir. Kural olarak koruma tedbirlerine

---

[277] Öztürk, Kazancı, Güleç, s. 36; Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 446.
[278] Dülger, Taşkın, s. 345.
[279] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 446; Şahin, Göktürk, Ceza Muhakemesi Hukuku I, s. 268.
[280] Ünver/Hakeri, Ceza Muhakmesi Hukuku, s.329.
[281] Öztürk, Tezcan, Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 446.
[282] Şahin, Göktürk, Ceza Muhakemesi Hukuku I, s. 268, Öztürk, Kazancı, Güleç, s. 36.
[283] Özbek, Doğan, Bacaksız, Ceza Muhakemesi Hukuku, s. 235;
[284] Şahin, Göktürk, Ceza Muhakemesi Hukuku I, s. 268; Özen, Mustafa, Öğreti ve Uygulama Işığında Ceza Muhakemesi Hukuku, 1.baskı, Ankara: Adalet Yayınevi, 2017, s.689.
[285] Şahin, Göktürk, Ceza Muhakemesi Hukuku I, s. 268.
[286] Yenisey/Nuhoğlu, s. 333.

hâkimin karar verdiği, tutuklama gibi bazı tedbirlerde bunun istisnasız geçerli olduğu ifade edilebilir[287].

Bununla birlikte kanunda belirlenmiş pek çok durumda, örneğin CMK m. 129 gereği postada elkoyma, CMK m. 134 gereği bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma, CMK m. 135 telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirlerinde olduğu gibi, gecikmenin sakınca teşkil edebileceği hallerde Cumhuriyet savcısı da karar verme yönünde yetkilendirilmiştir[288].

Ayrıca CMK m. 91 gereği gözaltı koruma tedbirinde olduğu gibi sadece Cumhuriyet savcısının tedbire yönelik karar verme yetkisinin bulunduğu durumlar ile CMK m. 119 gereği arama ve CMK m. 127 elkoyma tedbirlerinde mümkün olduğu gibi bazı hallerde kolluğun da yetkili olabileceğini görmekteyiz. Hatta CMK m. 90 gereği ise herkesin yetkili olabileceği düzenleme altına alınmıştır[289].

(6) Ölçülülük İlkesi

Koruma tedbirleriyle henüz bir hüküm verilmeksizin bireylerin temel hak ve özgürlüklerine müdahale edildiğinden, bu tedbirlere başvurulurken, ölçülülük ilkesine uyulması gerekir. Bu bağlamda koruma tedbirine başvurmakla elde edilecek yarar ile temel hak ve özgürlüklerin sınırlanmasıyla ortaya çıkacak zarar arasında makul bir ölçü aranır, dolayısıyla araçla amacın, yöntem ve hedefin dengeli olması gerekliliği bulunur[290].

B. Koruma Tedbirlerine İlişkin Ortak Özelliklerin Online Arama Bakımından İncelenmesi

Koruma tedbirlerinin ortak özellikleri, bir nevi koruma tedbirlerinde bulunması gereken asgari koşullar olarak kabul edilebilir. Çalışmamızın bu bölümünde bir koruma tedbiri olarak Türk ceza muhakemesi hukukuna kazandırılmasını önerdiğimiz

[287] Öztürk/Kazancı/Güleç, s. 38; Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447; Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s. 270.
[288] Öztürk/Kazancı/Güleç, s. 38; Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447; Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s. 270.
[289] Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447; Öztürk/Kazancı/Güleç, s. 38.
[290] Öztürk/Kazancı/Güleç, s. 39; Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 447; Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s. 269.

online arama tedbirinin, koruma tedbirlerinin ortak özelliklerini taşıyıp taşımadığı incelenecektir. Esas itibariyle çalışmanın ikinci bölümünde Alman CMK m. 100b'de yer alan adli amaçlı online arama örneği üzerinden daha detaylı açıklamalarda bulunulacağından, buradaki incelememiz koruma tedbirlerinin ortak özellikleri bakımından online arama tedbirinin incelenmesi ile sınırlı tutulacaktır[291].

İnsan haklarına ve kişilerin temel hak ve özgürlüklerine bir müdahale söz konusu olduğu için öncelikle ***yasal dayanağın bulunması*** şartı aranmaktadır. Alman Hukuku'nda düzenlenmiş olan online aramanın yasal dayanağını Alman Ceza Muhakemesi Kanunu'nun 100b maddesidir oluşturmaktadır[292]. Alman CMK m. 100b/1' de asıl yetkilendirme temeli ve gereklilikleri yer almakta olup, m. 100b/2' de ise suç kataloğu ile hangi suçlara karşı online aramanın uygulanabileceği düzenlenmiştir. Alman CMK m. 100b/3 gereği ise, bu tedbirin kimlere karşı uygulanabileceği belirtilmiştir. Online arama tedbirinin Türk hukuk sistemine kazandırılması halinde, bunun CMK'da açık ve detaylı bir şekilde kaleme alınmış bir norm ile gerçekleştirilmesi gerektiği açıktır. Bu sebeple, tedbir yasal dayanağını CMK'dan alacaktır.

Kesin hükümden önce bireylerin temel hak ve özgürlüklerine bir müdahalenin söz konusu olması sebebiyle, koruma tedbirlerinin mutlaka kanunla düzenleme zorunluluğu[293] açısından incelendiğinde, online arama ile özellikle kişilerin özel ve aile hayatının gizliliğine saygı hakkı, konut dokunulmazlığı hakkına ve kişisel verilerin gizliliğine müdahale edildiği ifade edilmelidir. Alman Hukukunda online aramanın Federal Almanya Anayasası'nda açıkça belirtilmemiş olan kendi kaderini tayin hakkının bağımsız bir ifadesi olarak bilgi teknolojisi sistemlerinin bütünlüğünü ve gizliliğini garanti etme temel hakkına da ciddi bir müdahale oluşturduğu ifade edilmektedir[294]. Türk hukukuna online arama düzenlemesinin getirilmesi halinde tedbirle birlikte müdahalede bulunulacak olan özel ve aile hayatının gizliliğine saygı gösterilmesini isteme hakkı, konut dokunulmazlığı, kişisel verilerin korunması gibi temel hak ve özgürlükler bakımından dengeleyici usulî tedbirlerin alınması gerekmektedir. Bu konudaki somut önerilerimize çalışmamızın üçüncü ve son bölümünde yer verilecektir.

---

[291] Bkz. İkinci Bölüm II C.
[292] Alman Ceza Muhakemesi Kanunu: § 100b StPO - Einzelnorm (gesetze-im-internet.de), Erişim tarihi: 01.06.2024:
[293] Öztürk, Erdem, Tezcan, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s.446.
[294] BVerfGE 120, 274

Bir başka koşul olan ***suç şüphesinin belirli bir yoğunlukta olması*** koşulu bakımından kanaatimizce Türk hukukunda bu tedbir düzenlenecek olursa, şüphe yoğunluğu bakımından kuvvetli şüphe sebeplerinin varlığının aranması, tedbirin temel hak ve özgürlükler bakımından yarattığı müdahale risklerini bertaraf etmek açısından dengeleyici bir niteliğe sahip olacaktır. Çalışmamızda esas aldığımız Alman hukukunda online arama bakımından suç kataloğunda sayılmış olan özellikle ciddi bir suçun işlendiği şüphesini doğuran belirli olguların bulunması şartı aranmaktadır. Bu çerçevede suç şüphesinin basit şüphe olarak tanımlanabilecek başlangıç şüphesi derecesinden daha yüksek gerekliliklere tabi olduğu belirtilmekte[295], ancak şüphenin yeterli veya kuvvetli şüphe yoğunluğunda olması aranmamaktadır[296]. Ancak bu bağlamda salt varsayıma dayanan ve tahminden ibaret bulunan şüphenin yetersiz olduğu, aksine bir katalog suçunun varlığının yaşam deneyimi veya kriminalistik deneyime dayanarak, tanık ifadelerinden, gözlemlerden veya diğer olgusal kanıtlardan çıkarılabiliyor olması zorunluluğu aranmaktadır[297]. Bu nedenle şüphenin somut olgularla desteklenebilir nitelikte olması ve böylelikle belirli bir somutlaştırma ve pekişme derecesine ulaşmış olması gerektiği ifade edilir[298]. Burada *"nitelikli şüphe"* olarak Türkçe'ye tercüme edebileceğimiz bir şüphe türü belirlenmiş olup, online aramaya başvurulabilmesi için katalogda yer alan bir suçun varlığına dair nitelikli şüphe aranmaktadır. Sonuç olarak, herhangi bir suçtan dolayı bir şüphenin yeterli olmadığını ifade edebiliriz. Ayrıca şüphelinin ciddi bir suç işlediğine ya da teşebbüsün cezalandırılabilir olduğu hallerde, işlemeye teşebbüs ettiğine dair şüpheyi haklı kılacak nedenlerin bulunması gerekmektedir[299].

Gecikmede halinde maddi gerçeğe ulaşılamayacağı, deliller elde edilemeyeceği ve neticede kararın yerine getirilmesi mümkün olmayacağı sebebiyle, online arama tedbirinin uygulanması bakımından ***gecikmede sakıncanın bulunup bulunmadığı***, olayın durumuna göre karar vermeye yetkili yargı mercileri tarafından tespit edilmelidir. Bu özellik Alman hukukunda doğrudan düzenlemenin kendisine yansımış olup, şüphelinin ciddi bir suç işlediğine ya da teşebbüsün cezalandırılabilir olduğu hallerde, işlemeye teşebbüs ettiğine dair somut olguların bulunması halinde, suçun özellikle münferit durumlarda ciddi olması ve soruşturmaya konu olan olayların

[295] BVerfG NJW 2004, 999 (1012); Köhler in Meyer-Gossner/Schmitt, §100b Rn. 4.;
[296] BGH BeckRS 2016, 15673; OLG Hamm BeckRS 2013, 197317; NStZ 2003, 279.
[297] BVerfG NJW 2007, 2752 (2753).
[298] Soine, Rn. 498; BGHSt 41, 30, 33; BGH BeckRS 2016, 15673.
[299] Kruse/Grzesiek, s. 345.

araştırılması veya şüphelinin nerede bulunduğunun belirlenmesi farklı bir yol ile daha zor veya mümkün olamayacağı hallerde gecikmede sakınca kabul edilmek suretiyle bu tedbire başvurulur.

Koruma tedbiri kararının kural olarak hâkim tarafından, gecikmesinde sakınca bulunan hallerde ise birçok koruma tedbirine savcı veya kolluk amiri tarafından karar verilmesi de bilindiği gibi mümkündür. Online aramanın temel hak ve özgürlüklere ağır bir müdahale oluşturması sebebiyle, Alman CMK m. 100e/2-1 gereği online arama tedbirine başvurulabilmesi için savcının yetki bölgesinde bulunduğu eyalet mahkemesinin *(Landgericht)* devlet güvenlik dairesinde talepte bulunması gerekmektedir. Tedbire kararı vermeye yetkili daire, Eyalet Yüksek Mahkemesinin yetki bölgesinde bulunan, ceza yargılamasında görevli olmayan 3 hâkimden oluşan devlet güvenlik dairesine *(Staatsschutzkammer)* aittir. Gecikmesinde sakınca bulunduğu hallerde ise yetkili daire başkanının da bu kararı vermeye yönelik yetkisi düzenlenmiş olup, bu durumda üç gün içinde bu kararın mahkeme dairesi tarafından onaylanması gerekmektedir[300]. Aksi takdirde tedbir derhal sona erdirilmelidir.

Koruma tedbirlerinin bir diğer ortak özelliği bakımından, bunların ***geçici*** nitelikte ve bu nedenle bir amaç değil bir araç olduklarından söz etmiştik. Bu kapsamda koruma tedbirlerinden beklenen amacın gerçekleşmeyeceği durumlarda, bu tedbirlere başvurulamayacağı gibi, amaca ulaşılınca da derhal sona erdirilmeleri gerekir. Alman CMK m. 100e/2 gereği, online aramaya yönelik karar, kural olarak en fazla bir ay ile sınırlı olmak üzere verilebilirken, elde edilen soruşturmanın sonuçları dikkate alınarak, koşulların devam etmesi şartıyla, kanunda bir seferde bir aydan fazla olmamak üzere bu süreyi uzatma imkanı tanımıştır. Kararın süresinin toplam altı aya uzatıldığı ve uzatmanın devam etmesinin talep edildiği hallerde kararın yüksek bölge eyalet mahkemesi ("Oberlandesgericht") tarafından verileceği düzenlenmiştir. Türk hukuku bakımından online arama düzenlemesinin getirilmesi halinde, yasada açıkça tedbirin uygulanmasına dair sürelerin şüpheye yer bırakmayacak şekilde açık bir biçimde düzenlenmesi gerekmektedir.

Koruma tedbirleri ile bağlantılı olarak ***ölçülülük ilkesi***, tedbire karar verme neticesinde elde edilecek yarar ile tedbir sonucunda ortaya çıkacak zarar arasında bir ölçünün olmasını ifade etmektedir. Online arama ile bilgi teknoloji sistemine gizli erişim sağlanarak kişinin yukarıda belirtmiş olduğumuz temel hak ve özgürlükleri

[300] Park, §4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 918.

derinden etkilenmektedir. Şöyle ki, online arama tedbirinin, tutuklamadan sonra temel hak ve özgürlüklere en ciddi müdahaleyi oluşturduğunu ifade edebiliriz. Bilgi teknolojisi sistemlerinin vatandaşların yaşamları ve günlük rutinleri için önemi göz önüne alındığında, sistemden kapsamlı ve uzun vadeli veri toplanması, anayasal olarak kabul edilemez bir şekilde çok yönlü gözetime yol açabilir. Aynı durum kapsamlı bir kişilik profili oluşturma olasılığı için de geçerlidir. Bu nedenlerle tedbire karar verilirken, devletin cezai menfaati ile ilgili kişinin temel hak ve özgürlükleri arasındaki dengenin özellikle bu ağır müdahaleci tedbirin kullanılmasını haklı gösterip göstermediği her zaman özel olarak değerlendirilmelidir[301]. Sonuç itibariyle online arama tedbirine sadece suç kataloğunda bulunan ciddi bir suçun işlendiğine dair nitelikli şüphenin bulunduğu hallerde başvurulmasının ölçülülük ilkesi ile bağdaştığı ifade edilmektedir[302]. Türk hukukunda online arama tedbirinin düzenlenmesi halinde, tedbirin sıkı koşullara bağlanması, karar merci ve şüphe yoğunluğu bakımından katı şartlar getirilmesi ve örneğin başka surette delil elde etme imkanının bulunmaması gibi şartlar getirilmesi halinde ölçülülük ilkesini ihlal etmeyen bir düzenlemeden söz edilebilir. Ölçülülük ilkesi çerçevesindeki somut diğer bazı önerilerimiz çalışmanın son bölümünde daha detaylı şekilde açıklanacaktır.

C. İkincillik İlkesinin Online Aramaya Etkisi

1. Online Arama Bakımından İkincillik İlkesi

Online arama bakımından ikincillik ilkesi ("*Subsidiaritätsklausel*") esastır. Bu esas doğrudan Alman CMK m. 100b/1-3 ile düzenlenmiş olup, tedbirin ancak soruşturmaya konu olan olayların araştırılmasının veya şüphelinin yerinin tespit edilmesinin buna bağlı olması durumunda uygulanabileceği belirtilmektedir. Bir başka ifadeyle, alternatif koruma tedbirlerinden beklenen sonucun alınmasının güç olduğu veya hiç sonuç alınamayacağının öngörüldüğü hallerde, online arama tedbirine başvurulabilecektir[303].

Kanun koyucu ölçülülük ilkesinin bir yansıması olan bu esas ile online arama emri verilmesinin önüne bizzat kendisi bir engel koymuştur[304]. Zira temel hak ve

[301] MüKoStPO/Rückert §100a Rn.60.
[302] BVerfG 24.4.2013 – 1 BvR 1215/07, BVerfGE 133, 277 Rn. 226 = NJW 2013, 1499.
[303] MüKoStPO/Günther §100c Rn. 34; Soine NStZ 2018, 499.
[304] BT-Druck 18/12785, 55.

özgürlüklere yapılan müdahale göz önünde bulundurulduğunda, gerekçelendirmenin özellikle yüksek standartları karşılaması gerekmektedir[305]. Tedbir özel hayata ne kadar derin nüfuz eder ve meşru gizlilik beklentileriyle ne kadar çatışırsa, bu gerekliliklerin o kadar katı olması gerektiği kabul edilir[306].

Online aramaya başvurmadan önce, geleneksel koruma tedbirleri olan açık arama ve el koymanın hedeflenen amaca hizmet edip etmeyeceklerinin değerlendirilmesi beklenmektedir[307]. Açık bir tedbirin uygulanmasının gizli bir tedbire göre öncelikli olması, gizli tedbirin niteliği gereği teşkil ettiği yoğun müdahale etkisi sebebiyle gayet anlaşılır bir durumdur. Aksine, temel haklara yönelik böyle bir müdahalenin gerekliliği bağlamında, mevcut tüm gizli tedbirlere özel bir önem verilmesi gerektiği savunulur[308].

Tüm bu gerekçelerle, online aramanın, benzer amaçlar taşıyan diğer koruma tedbirleri ile mukayese edilmesi, tedbirin kendine has özelliklerinin ve ikincil olma fonksiyonunun anlaşılması bakımından önemlidir. Bu sebeple, çalışmanın devamında online aramaya benzer koruma tedbirleri ile online arama tedbirinin karşılaştırılmasına yer verilecektir.

2. Online Arama Tedbirinin Benzer Koruma Tedbirleri ile Mukayesesi

a. Arama

Kelime anlamı olarak "arama" hukuk literatüründe şüphelinin veya sanığın yakalanması veya suç delillerinin elde edilmesi için bir kimsenin evinde, işyerinde, üzerinde veya eşyasında yapılan araştırma işlemini ifade etmektedir[309].

5271 sayılı Ceza Muhakemesi Kanunu'nda aramaya ilişkin bir tanıma yer verilmemiş olup, bu eksiklik Adli ve Önleme Aramaları Yönetmeliği ile giderilmiştir. Yönetmeliğin 5. maddesinde arama için "bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak

[305] Warken NZWiSt 2017, 329, (336).
[306] BVerfG NJW 2016, 1781 (1784).
[307] BT-Druck 18/12785, 55.
[308] Park, Rn. 914.
[309] Tdk Büyük Türkçe sözlük, arama ne demek TDK Sözlük Anlamı (sozluk.gov.tr), Erişim tarihi: 01.06.2024:

konutunda, iş yerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında yapılan araştırma işlemidir" şeklinde bir tanım yapılmıştır[310].

Arama gerek bir suçun işlenmesini önlemek gerekse bir suçun adli takibini soruşturma ve kovuşturma suretiyle gerçekleştirmek üzere ikiye ayrılır[311].

(1) Önleme amaçlı arama

Önleme amaçlı aramaya değinmeden önce, kısaca "ön alan"[312] olarak da ifade edilebilen suç öncesi alanda gerçekleştirilen işlemlerde amacın belirtilmesi faydalı olacaktır. Suç öncesi alanda gerçekleştirilen işlemlerin temel amaçlarından biri kamu düzeni ve güvenliğinin sağlanmasıdır. Bu alanda kurulu ve işleyen bir düzen mevcut olup, ortada henüz düzeni bozan, işlenmiş bir suç bulunmamaktadır. Bu güvenlik ortamını ve düzenin varlığını korumak ile esenlik sağlanmaya çalışılması esastır[313]. Mevcut düzenin ve güvenlik halinin devamı ise olası tehlikelerin bertaraf edilmesine bağlıdır. Bu nedenle zarar ve tehlikenin önlenmesine yönelik işlemler de suç öncesi alan işlemlerinden sayılmaktadır[314].

Tehlike kavramı için öğretide farklı tanımlar yer almaktadır. TDK'ye göre tehlike, *"Büyük zarar veya yok olmaya yol açabilecek durum"* veya *"gerçekleşme ihtimali bulunan fakat istenmeyen sakıncalı durum"* olarak tanımlanmaktadır[315]. Bir görüşe göre tehlike zarar ihtimali olup[316], diğer bir görüşe göre ise engellenmeden tamamlandığı takdirde, bir zarar doğması sonucu ile bitebilecek durumdur[317]. Farklı bir görüş ise hayatın olağan akışında genel yaşam tecrübesine dayanarak, kamu güvenliği ve düzeni açısından bir zarar meydana gelme beklentisini oluşturan durumu[318] "tehlike" olarak tanımlamaktadır. Zarar kavramı bakımından ise TDK'ya

---

[310] Adli ve Önleme Aramaları Yönetmeliği 01.06.2005 tarihinde ve 25832 sayılı Resmî Gazetede yayınlanarak yürürlüğe girmiştir.
[311] Şahin/Göktürk, Ceza Muhakemesi Hukuku I, s. 320; Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 506.
[312] Özbek, Veli, Polis Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler ve Hukuka Aykırı Müdahalelere Karşı Korunma Çareleri (Önleme ve Koruma Tedbirleri), 2. Baskı, Seçkin, Ankara, 2023, s. 34.
[313] Baran Kızılırmak, Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2018, s. 33 vd.
[314] Çağlayan, Ramazan, Kolluk ve Güvenlik Hukuku, 1. Baskı, 2022, s. 27 vd.
[315] Türk Dili Kurumu, Erişim: tehlike ne demek TDK Sözlük Anlamı (sozluk.gov.tr), Erişim tarihi: 01.06.2024: 31.03.2024.
[316] Nurullah Kunter, "Tehlike Tedbiri Genel Teorisi ve Para Cezaları İçin Haciz ve İhtiyati Haciz", İÜHFM, C.34, S:1-4, 1968, s.28.
[317] Yenisey, Kolluk Hukuku, s.11.
[318] Özbek, Veli Özer: "Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları", DEÜHFD, C:4, S:2, 2002, s. 34, 35.

göre zarar, *"bir şeyin, bir olayın yol açtığı çıkar kaybı veya olumsuz, kötü sonuç, dokunca, ziyan, mazarrat"* olarak tanımlanmaktadır[319]. Kolluk hukuku açısından zarar ise *"hukuki menfaati koruyan normun veya suç tipinin ihlali tehlikesinin oluştuğu anda gerçekleşmiş sayılır"* şeklinde tanımlama yapılmaktadır[320].

Tehlikenin niteliğine göre uygulanan tedbirin niteliğinin de değiştiği ve buna göre "*önleme ile geç kalınmış yakın bir tehlike durumunda*" koruma tedbirinin, "*tehlikenin uzak olduğu hallerde*" ise önleme tedbirinin uygun araç olduğu belirtilmektedir. Bununla birlikte önleme ve koruma tedbirlerinin arasında bir diğer farkın ise önleme tedbirlerinde korunacak bir hakkın bulunması şartı arandığı halde, koruma tedbirlerinde gecikemezlik sebebiyle hak aranmaması, haklı görünüşle yetinilmesidir. Bu nedenlerle, kamu düzeni ve güvenliği açısından zarar doğurucu etmenlerin önlenmesi, tehlike doğuranların bertaraf edilmesi amacıyla uygulanan yöntemleri "önleme tedbiri" kapsamında ele almak mümkündür[321].

Bu önleme tedbirlerinden birinin de önleme araması olduğu ifade edilebilir. Önleme aramasının gerçekleştirilebilmesi için somut olayda makul sebeplerin bulunması gerekirken, amacın ise kamu emniyetini veya kamu düzenini tehlikeye sokan kişi veya eşyaların bulunması, onların kolluğun koruması altına alınması olarak ifade edilmektedir[322].

2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun (PVSK) 9. maddesinde önleme aramasının tanımı yapılmıştır. Buna göre, *"milli güvenlik ve kamu düzeninin, genel sağlık ve genel ahlakın veya başkalarının hak ve hürriyetlerinin korunması, suç işlenmesinin önlenmesi, taşınması veya bulundurulması yasak olan her türlü silah, patlayıcı madde veya eşyanın tespiti amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde mülki amirin yazılı emriyle belli yerlerde, kişilerin üstlerinde, aracında, özel kağıtlarında ve eşyalarında yapılan arama işlemidir*."

Bununla birlikte PVSK m. 9 gereği, konutta, yerleşim yerinde ve kamuya açık olmayan işyerlerinde ve eklentilerinde önleme araması yapılamayacağı belirtilmiştir. Bunun gerekçesi ise bu tür yerlerde yapılan aramanın kişinin özgürlüğünü ciddi ölçüde etkilemesi olup, bu nedenle ölçülülük ilkesinin bir gereği olarak bu yerlerde yapılacak

[319] Türk Dili Kurumu, Erişim: zarar ne demek TDK Sözlük Anlamı (sozluk.gov.tr), Erişim tarihi: 01.06.2024: 31.03.2024.
[320] Yenisey, Kolluk Hukuku, 11.
[321] Yenisey/Nuhoğlu, Ceza Muhakmeesi Hukuku, s.291, 292.
[322] Çulha, Rıfat/Demirci, Turgay/Nuhoğlu, Ayşe/Yenisey, Feridun, Ceza Muhakemesinin Soruşturma Evresindeki Süjeler İçin CMK Cep Kitabı, 5.bs, Ankara, TBB Yayınları, 2016, s.30.

arama için bir suç şüphesinin bulunması ve hâkim kararının gerekliliği vurgulanmaktadır[323].

Ayrıca Adli ve Önleme Aramaları Yönetmeliğinin 18. maddesi gereği "denetim" adı altında kolluğun bir arama emri almaksızın kendiliğinden yapabileceği işlemler de düzenlenmiş olup, bunlar arama niteliği taşımamaktadır[324]. Bunlara örnek olarak kişilerden kimlik sorma, motorlu araç ruhsatı ve sürücü belgesi denetimi, otel, bar ve sinema gibi işletmelerin denetimi gösterilebilir.

Ayrıca Adli ve Önleme Aramaları Yönetmeliği'nin 8., 9. ve 25. maddeleriyle örneğin gözaltına alınan kişinin, nezarethaneye bırakılmadan önce yapılan üst araması gibi kolluğun bir arama kararı gerekmeksizin arama yapabileceği haller de düzenleme altına alınmıştır[325].

PVSK dışında 2803 sayılı Jandarma Teşkilat Görev ve Yetkileri Kanununda, 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanununda ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanununda önleme araması düzenlemelerine yer verilmiştir[326].

Adli aramanın yapılması gerektiği hallerde önleme aramasının yapılmasını Yargıtay hukuka aykırı olarak değerlendirmekte olup, önleme amaçlı arama ile adli amaçlı aramanın çizgisini çok net bir şekilde ortaya koymaktadır[327]. Bu bağlamda önemli bir husus, daha önceden alınan önleme arama kararına istinaden adli arama yapılamayacağıdır. Nitekim bu tür durumlarda artık adli aramaya ilişkin kurallar geçerli olacağından, adli arama kararının alınması gerekliliği vurgulanmaktadır[328]. Aksi takdirde bu tür bir arama sonucu elde edilen deliller hukuka aykırı olur ve yargılamada kullanılamaz.

(2) Adli amaçlı arama

Adli amaçlı arama Ceza Muhakemesi Kanunumuzun dördüncü Bölümü'nde "Arama ve Elkoyma" başlığı altında 116. maddede[329] düzenlenmiştir. Amacı şüpheli veya sanığın yakalanması, delil elde edilmesi veya müsadereye konu olan eşyanın ele

[323] Dülger/Taşkın, s. 426.
[324] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 405.
[325] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 405.
[326] Özbek/Doğan/Bacaksız, s. 304.
[327] Yargıtay 8. CD. 04.04.2016 tarihli E. 800/4416; Yargıtay Ceza Genel Kurul, 01.03.2022 tarihli, E. 2020/7-231.
[328] Ünver, Hakeri, s. 407.
[329] CMK Madde 116 – *"(1) Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir."*

geçirilmesidir[330]. Bunun neticesinde arama tedbirinin saklı olan şeylerin bulunmasına yönelik olduğu, dolayısıyla açıkta olan şeyler açısından aramanın geçerli olmayacağı ifade edilmektedir[331].

CMK gereği bastırıcı nitelikte olan aramanın konusu, konut, taşınabilir veya bizzat kişinin kendisi olabilir ve bu çerçevede arama kişinin üstünde, eşyasında, konutunda, işyerinde ve ona ait diğer yerlerde yapılabilir[332]. Bununla birlikte arama sanık, şüpheli ve üçüncü kişilere de uygulanabilmektedir. Bu çerçevede üçüncü kişilere yönelik arama, şüphelinin veya sanığın yakalanabilmesi veya suç delillerinin elde edilebilmesi amacıyla diğer bir kişinin de üstünün, eşyasını, konutunun, işyerinin veya ona ait diğer yerlerin aranmasını kapsamaktadır.

Eşyada arama bakımından, kişinin yanında bulundurduğu her türlü taşınabilir eşyasının aranması mümkündür. Bu bağlamda fiilen kullanılan, maddi bir varlığa sahip olan ve delil niteliği taşıyabilen her şey, aramanın konusu olabilir. Ancak bilgisayar ve bilgisayar verisi içeren eşyalar bu kapsama girmezler[333]. Onlar için gerektiğinde el koyma işleminin de yapılabilmesi için özel olarak CMK m. 134'te düzenlenmiş olan "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" tedbiri geçerlidir. Günümüzde dijital delillerin son derece önem kazanmaları sebebiyle m. 116 vd. gereği arama kararı alınırken m. 134'e göre karar alındığı ifade edilmektedir[334]. Ayrıca avukat bürolarında arama ile askeri mahallelerde yapılan aramaların da özel arama türleri olarak farklı maddelerde ve gereksinimlerle düzenleme altına alındığı belirtilmelidir.

Adli amaçlı arama tedbiri bakımından makul şüphe aranmaktadır. CMK m. 116 gereği, "*yakalanabileceği veya suç delillerinin elde edilebileceği huşunda makul şüphe varsa"*, arama tedbiri uygulanabilir. Adli ve Önleme Aramaları Yönetmeliği m. 6/1 makul şüpheyi "hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphe" şeklinde tanımlamaktadır. Makul şüphenin keyfiliğe dayanmaması gerektiği, makul bir inançtan daha azını, ihtimalden ise daha fazlasını gerektirdiği vurgulanmaktadır[335]. Bunun neticesinde arama sonunda belirli bir şeyin bulunacağına

[330] Öztürk/Tezcan/Erdem, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, s. 506.
[331] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 402.
[332] Öztürk/Kazancı/Güleç, s. 140.
[333] Öztürk/Kazancı/Güleç, s. 157;
[334] Dülger/Taşkın, s. 429.
[335] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 408.

dair ve belirli bir kişinin yakalanacağına dair somut olguların bulunması arama için yeterli kabul edilir[336].

Arama tedbiri ceza muhakemesinin en önemli delil elde etme yöntemlerinden biri olarak kabul edilir. Nitekim Ceza Muhakemesi Kanunu'nda aramanın amacı, şüpheli veya sanığın ele geçirilmesi ve suç delillerinin elde edilmesi olarak ifade edilmiştir. Bu tedbir gerek kişi gerekse konut dokunulmazlığına ciddi bir müdahale teşkil ettiğinden, özel hayata ve özel hayatın gizliliğine yoğun müdahale niteliği taşımaktadır[337].

Temel hak ve özgürlüklere oluşturduğu yoğun müdahale sebebiyle, arama tedbirinin anayasal düzeyde düzenlendiğini ifade edebiliriz. Anayasa m. 20 gereği, usulüne göre verilmiş hâkim kararı olmadıkça veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça kimsenin üstünün, özel kağıtlarının ve eşyasının aranamayacağı düzenlenmiştir. Bununla birlikte, AY m. 21 ile usulüne göre verilmiş hâkim kararı olmadıkça veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça kimsenin konutuna girilemeyeceği ve konutunun aranamayacağı hüküm altına alınmıştır. Bu düzenlemelerin neticesinde; arama tedbiri kural olarak yetkili merci tarafından verilen yazılı bir karar dayanır. Aramaya kural olarak hâkim karar verebilirken, gecikmesinde sakınca bulunan hallerde cumhuriyet savcısı yetkilendirilmiştir. Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlilerinin arama yapabilmeleri mümkündür, ancak bu durum konut, işyeri ve kamuya açık olmayan kapalı alanlar için geçerli değildir. Burada bahsi geçen aramalar yalnızca hâkim kararıyla veya gecikmesinde sakınca bulunan hallerde yalnızca Cumhuriyet savcısının kararıyla yapılabilir[338].

Geleneksel arama tedbirini online arama ile mukayese ettiğimizde, özellikle bazı hususlar göze çarpmaktadır. Geleneksel arama tedbiri soruşturma makamları tarafından açık bir şekilde gerçekleştirilir[339]. Oysa online arama tedbirinin başlıca özelliği bunun gizli bir şekilde yapılmasıdır. Ayrıca online arama çalışır durumda olan bir sistem üzerinde gerçekleştirilir. Böylelikle sistem kapatıldığında ya da

[336] Dülger/Taşkın, s. 430.
[337] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 409.
[338] Öztürk/Kazancı/Güleç, s. 147 vd.
[339] BeckOK StPO/Graf StPO §100b Rn. 1.

kilitlendiğinde sistemdeki verileri şifreleyen ve bu verileri soruşturma makamları için büyük ölçüde kullanışsız hale getiren şifreleme teknikleri atlatılır.

Online aramanın gizliliği, soruşturma makamlarının tedbire maruz kalan kişinin tedbirin farkında olmadan bir bilgi teknoloji sistemindeki verileri analiz etmelerini sağlar. Bu, delillerin imha edilmemesi bakımından önemlidir[340] ve özellikle organize suçlar alanında, tedbire maruz kalan kişinin, örgütün diğer şüpheli üyelerini uyarmasını engeller. Özellikle tüm üyelerin henüz tespit edilemediği ve bu nedenle eş zamanlı açık arama yapılamadığı durumlarda bu önemlidir[341]. Geleneksel, açık bir aramada örneğin arama anında sadece konutun içindekiler aranabilirken, online arama ile bilgi teknoloji sistemindeki içerikler ve veriler soruşturma süresince değişime uğramalarına rağmen izlenebilmekteler.

Bu nedenlerle, online aramanın açık bir aramaya göre önemli taktiksel avantajılar içerdiği belirtilip, bu avantajların düzenlemenin amacını ve soruşturma tedbirinin gerekliliğini ortaya koyduğu vurgulanmalıdır[342].

b. Elkoyma

Hukuk sözlüğü anlamıyla elkoyma, ceza hukukunda bir önlem olarak, bir eşya üzerinde zilyedinin tasarruf yetkisinin ortadan kaldırılması anlamına gelmektedir[343]. Ceza muhakemesinin işleyişini garanti etmeyi sağlayan ve geçici olan bir koruma tedbiridir[344].

Adli ve Önleme Aramaları Yönetmeliği'nde elkoyma tanımlar kısmını ele alan m. 4' te düzenleme altına alınmıştır. Buna göre elkoyma, *"Suçun veya tehlikelerin önlenmesi amacıyla veya suçun delili olabileceği veya müsadereye tâbi olduğu için, bir eşya üzerinde, rızası olmamasına rağmen, zilyedin tasarruf yetkisinin kaldırılması işlemini"* tanımlamaktadır. Buradan anlaşılacağı üzere elkoyma hem önleme amaçlı hem adli amaçlı olarak iki şekilde uygulanabilir.

[340] Hofmann, NStZ 2005, 123 f.
[341] MüKoStPO/Rückert StPO §100b, Rn. 2.
[342] MüKoStPO/Rückert StPO §100b, Rn. 2.
[343] Ejder Yılmaz, Hukuk Sözlüğü, Yetkin Yayınları, Ankara, 2006.
[344] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 347.

(1) Önleme Amaçlı Elkoyma

Tehlikenin önlenmesi amacı ile bir eşyanın bir kimsenin elinden alınması önleme amaçlı elkoyma olarak ifade edilir[345]. İdari nitelik taşıyan bu önleyici elkoyma türü ile toplumun barış ve huzurunun korunması amaçlanmaktadır[346]. Henüz işlenmiş bir suç bulunmadığından, önleyici elkoyma ceza muhakemesi işlemi olarak kabul edilmez ve adli amaçlı elkoymadan farklılıklar göstermektedir.

Hava yolculuğu amacıyla hava limanına gelen kişilerin üzerinin aranması önleyici arama için bir örnek teşkil ederken, hava yolculuğunda taşınması yasak olan bir çakının uçağa binmeden yapılan aramada görevliler tarafından el konulmak suretiyle yolcunun yanında uçağa sokmasına izin verilmemesi ise önleme amaçlı elkoyma olarak değerlendirilir[347].

Önleme amaçlı elkoyma, işlenmiş suçu aydınlatmak amacıyla yapılan adli amaçlı elkoymadan farklılıklar gösterse de bazı hallerde sınırlarının keskin olmadığını görmekteyiz. Bu çerçevede bazen idari nitelikteki önleyici elkoyma adli amaçlı elkoyma ile iç içe geçebilir, bazen önleme amaçlı elkonulan eşyanın aynı zamanda adli amaçla da el konulabilecek nitelikte olması söz konusu olabilir[348].

Ayrıca Polis Vazife ve Salahiyet Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Kanunu, Olağanüstü Hal Kanunu ve Sıkıyönetim Kanunu gibi birçok Kanunda ikisinin birbirinden ayırdedilmeden düzenlendiği belirtilmelidir[349].

(2) Adli Amaçlı Elkoyma

Ceza Muhakemesi Kanunu'nda elkoyma, *"Eşya veya kazancın muhafaza altına alınması ve bunlara elkonulması"* başlığı altında m. 123 ve devamı maddelerinde düzenlenmiştir. CMK m. 123 gereği, *"İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır. Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir."*

Bu düzenlemeden anlaşıldığı üzere, elkoyma, bir suç işlendikten sonra onu aydınlatmak için gerekli delilleri temin etmek veya kazanç ya da eşya müsaderesine

[345] Yenisey/Nuhoğlu, Ceza Muhakemesi Hukuku, s. 435.
[346] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 477.
[347] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 477.
[348] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 477.
[349] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 477.

tabi eşyayı emniyet altına almak için yapılan bir ceza muhakemesi işlemidir[350]. Eşyanın zilyedinin rızasıyla teslim edilmesi halinde bu işleme muhafaza altına alma denir[351].

Adli amaçlı elkoymanın amacı, bir yandan elkonulacak eşyanın delil değeri olmasından kaynaklı, muhakemenin yapılabilmesinin sağlanması, öte yandan müsadere konusunu oluşturan eşyaya elkonulması suretiyle, verilecek hükmün kâğıt üzerinde kalmasının engellenmesi, dolayısıyla eşyanın adliyenin eli altına alınması olarak ifade edilebilir[352].

Bu bağlamda malvarlığı terimi mamelek anlamına gelen misli şeylerle ölçülebilen hak ve alacaklar olarak tanımlanıp, buna ekonomik değeri veya yararı olan para, değerli maden, ticari senetler ve taşınır taşınmaz her türlü eşyanın dahil olduğu belirtilir[353].

Eşya, *"türlü amaçlarla kullanılan, insan yapısı, taşınabilir cansız nesneler; pılı pırtı, yük"* anlamına gelir[354]. Hukuki bakımdan eşya, *"maddi bir varlığa sahip olup üzerinde hakimiyet kurulması mümkün olan, sınırlanabilen, kişi dışı, ekonomik değer taşıyan her türlü varlık"* olarak tanımlanabilir[355]. Ceza muhakemesinde maddi gerçeğin araştırılıp bulunması için, "*ispat aracı*" olarak da adlandırılan ispat malzemelerine ihtiyaç duyulmaktadır. Bu ispat araçları hâkime sunulacak ve hâkim kararını, bunlarla doğrudan doğruya bizzat temasa geçerek ve bunları serbestçe değerlendirerek maddi gerçeğe ulaşacağı *"delillerdir"*[356]. Bu açıdan, ceza muhakemesindeki en önemli aşamanın delillerin toplanması olduğu ifade edilebilir.

Şüpheli veya sanığı ele geçirmek suretiyle delil araçlarının veya müsadereye konu eşyanın güvence altına alınmasıyla, kesin hükümden önce özellikle mülkiyet hakkı, konut dokunulmazlığı hakkı ve haberleşme özgürlüğü gibi temel hak ve özgürlükleri etkilemesi sebebiyle bir koruma tedbiridir[357].

Ceza Muhakemesi Kanunu'nda elkoyma, basit elkoyma ve özel elkoyma olarak ikiye ayrılır. Basit elkoyma CMK m. 123' te karşımıza çıkarken, özel elkoyma

---

[350] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 477; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 523.
[351] Dülger/Taşkın, Ceza Muhakemesi Hukuku, s. 438.
[352] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 478; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 523.
[353] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 481.
[354] Türk Dil Kurumu, eşya ne demek TDK Sözlük Anlamı (sozluk.gov.tr), Erişim tarihi: 01.06.2024 :
[355] 5 Kemal Oğuzman, Özer Seliçi, Saibe Özdemir Oktay, Eşya Hukuku, Gözden Geçirilmiş 11. Bası, Filiz Kitabevi, İstanbul, 2006, s. 6.
[356] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 297.
[357] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 523.

türleri ise *"taşınmazlara, hak ve alacaklara elkoyma"* olarak m. 128'te, "postada elkoyma" olarak m. 129'da, *"avukat bürolarında arama, elkoyma ve postada elkoyma"* olarak m. 130'da, *"şirket yönetimine kayyım atanması"* olarak m. 133'te, *"bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* olarak m. 134'te ve *"kaçaklara ilişkin elkoyma olarak"* m. 248'te düzenleme altına alınmıştır. Bu doğrultuda el koyma, kural olarak bazı taşınabilir malvarlığı değerlerinin zilyedinden fiilen alınarak eşya üzerindeki tasarruf yetkisinin sınırlandırılması suretiyle adliyenin eli altında bulundurulması olarak ifade edilebilirken, bazı özel elkoyma türlerinde ise malvarlığı değerlerinin fiilen kendisine bırakılan zilyedin sadece hukuken tasarrufta bulunabilmesinin engellenerek de elkoyma tedbirinin uygulanabileceğini görmekteyiz.

Elkoymaya müracaat edebilmek için aranan şüphe bakımından CMK m. 123 vd. maddelerinde herhangi bir açıklık bulunmamaktadır. Öğretideki bir görüşe göre ölçülülük ilkesi dikkate alınarak somut olaya göre şüphenin belirlenmesi gerekmektedir[358]. Diğer bir görüşe göre ise elkoyma kararının verilebilmesi için mülkiyet hakkının korunması bakımından en azından yeterli şüphenin varlığı aranmalıdır[359]. Bununla birlikte Alman doktrininde eşyaya elkoyma bakımından "basit şüphenin" yeterli olduğuna yönelik yaygın bir anlayışın bulunduğu ifade edilmelidir[360].

Elkoyma tedbirine şüpheli veya sanıkla birlikte, elkoymaya konu olan eşyayı elinde bulunduran kişi hakkında da başvurulması mümkündür.

Buna karşın, CMK ve çeşitli kanunlarca bazı eşyalara elkonulamayacağı özel olarak düzenleme altına alınmıştır. CMK m. 126 gereği, *"Şüpheli veya sanık ile 45. ve 46."ncı maddelere göre tanıklıktan çekinebilecek kimseler arasındaki mektuplara ve belgelere; bu kimselerin nezdinde bulundukça elkonulamaz" hükmüne yer verilmiştir.* Bu hüküm ile CMK m. 45 ve 46 ile getirilen tanıklıktan çekinme hakkının elkoyma tedbirine başvurarak ortadan kaldırılmasın önlenip tanıklıktan çekinmeye dair hükümlerin uygulanması güvence altına alınmak istenmiştir. Nitekim tanıklıktan çekinme hakkı tanınan kişilerden yakını oldukları şüpheli ve sanık aleyhine beyanda

[358] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 524.
[359] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 480.
[360] Löwe-Rosenberg, §94 Rn. 35.

bulunmaları beklenmemekte; suçun ortaya çıkarılmasına katkıda bulunmaya zorlanmaları önlenmek istenmekte[361].

Bununla birlikte CMK m. 125 uyarınca devlet sırrı niteliğindeki belgelere de elkonulamayacağı düzenlenmiştir. Buna göre, *"(1) Bir suç olgusuna ilişkin bilgileri içeren belgeler, Devlet sırrı olarak mahkemeye karşı gizli tutulamaz. (2) Devlet sırrı niteliğindeki bilgileri içeren belgeler, ancak mahkeme hâkimi veya heyeti tarafından incelenebilir. Bu belgelerde yer alan ve sadece yüklenen suçu açıklığa kavuşturabilecek nitelikte olan bilgiler, hâkim veya mahkeme başkanı tarafından tutanağa kaydettirilir. (3) Bu madde hükmü, hapis cezasının alt sınırı beş yıl veya daha fazla olan suçlarla ilgili olarak uygulanır."* Bu doğrultuda açıklanması devletin güvenliği, milli varlığı, savunması, bütünlüğü, anayasal düzeni ve dış ilişkilerini tehlikeye düşürebilecek nitelikte bilgiler devlet sırrı sayılmaktadır[362]. Burada vurgulanması gereken husus, bu düzenlemenin ancak belirli ağırlık derecesine ulaşmış suçlara uygulanabilirliğidir. Bu nedenle belirli ağırlık ölçüsüne ulaşmayan suçlardan dolayı bir delil veya belgeye devlet sırrı olduğundan bahisle soruşturma ve kovuşturma sürecinde elkonulması engellenebilecektir[363].

Arama tedbirinde olduğu gibi, elkoyma tedbirinin de anayasal düzeyde düzenlenmiş olduğunu ifade edebiliriz. AY m. 20 ve 21 gereği, usulüne göre verilmiş hâkim kararı olmadıkça veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin özel kağıtlarına, üstündeki ve konutundaki eşyası ile diğer eşyalarına el konulamayacağı hüküm altına alınmıştır. Bununla birlikte Anayasa'nın ilgili maddeleri uyarınca, yetkili merciin yazılı emrinin yirmi dört saat içerisinde görevli hâkimin onayına sunulması ve hâkimin, kararını elkoymadan itibaren kırk sekiz saat içerisinde açıklaması gerekmektedir. Aksi takdirde, elkoyma kendiliğinden ortadan kalkacaktır[364]. Anayasal düzeyde yapılan bu düzenlemeyle aramada olduğu gibi elkoymada da en üst düzeyde temel hak ve özgürlüklerin korunması yoluna gidildiğini vurgulayabiliriz.

Nitekim elkoyma kararı kural olarak hâkim tarafından verilir. Soruşturma evresinde sulh ceza hakiminin kararı[365], kovuşturma evresinde ise olaya bakan

[361] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 483; Löwe-Rosenberg, §97, Rn. 1.
[362] Özbek/ Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 524.
[363] Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 425.
[364] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 534.
[365] Yargıtay, 7. CD. 05.03.2007 tarihli karar, E. 11055/1307; Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 426.

mahkemenin kararı aranmaktadır. Ancak gecikmesinde sakınca bulunan hallerde savcı, savcıya ulaşılamayan hallerde ise kolluk amirinin yazılı emri ile de tedbir uygulanabilir[366].

Son olarak ifade edilmelidir ki uygulamada sıkça gündeme gelen konulardan biri hazırlanan arama talebinde ayrıca el koymaya yönelik bir istemin bulunmamasıdır. Ancak salt arama kararının soruşturma makamına aynı zamanda elkoyma hakkı vermediği kabul edilmektedir. Elkoyma işleminin konusunun genelde suçun delilleri veya bizzat suçun konusunu oluşturan malvarlığı değerleri olduğu göz önünde bulundurulduğunda, el koyma tedbiriyle asıl olarak bu malvarlığı değerlerinin elde edilmesi amaçlanmaktadır. Dolayısıyla arama taleplerinde iddia konusu suç kapsamında arama sonucu elde edilecek delillere elkoyma işleminin yapılabilmesi için bunun talep edilmesi önem teşkil eder. Bunun sonucunda yetkili makam tarafından elkoyma kararı tek başına veya arama kararı ile verilebilir[367]. Açıkça ifade edilmelidir ki, hakkında hâkim tarafından elkoyma kararı verilmeyen deliller, hukuka aykırı delil niteliği sebebiyle yargılama da değerlendirme yasağına tabidir.

Online arama ile mukayesesi bakımından ilk olarak online aramanın en önemli özelliklerinden birinin gizli bir tedbir olması hususunu hatırlatmak isteriz. Buna karşın, geleneksel elkoyma tedbirinde, her ne kadar donanım veya harici veri taşıyıcılarına el konulması ve içerdikleri verilerin okunması mümkün olsa da[368], bu açık bir şekilde ve hakkında tedbir uygulanan kişinin bilgisi dahilinde gerçekleşir. Bununla birlikte tedbire hakkında tedbir uygulanan kişinin, yani bilgi teknoloji sistemini kullanın kişinin davranışı ancak el koyma zamanına kadar analiz edilebilir, bu da sistemin yalnızca anlık bir görüntüsünün görüntülenebileceği anlamına gelir[369]. Oysa online arama tedbiri ile uzun süreli izleme mümkündür.

Bunun dışında, örneğin silinen verilerin kurutulamaması veya şifreleme tekniklerinin kullanılması sebeplerinden veri taşıyıcılarındaki verilerin elde edilip analiz edilmesi geleneksel soruşturma araçlarıyla her zaman çözümlenememektedir[370].

[366] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 524.
[367] Şahin/Göktürk, Ceza Muhakemesi Hukuku, s. 342; Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 524.
[368] Blechschmitt, MMR 2018, 363 vd.
[369] Buermeyer, HRRS 2007, S. 158.
[370] Sinn, Stellungnahme, S. 2

c. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma düzenlemesiyle kanun koyucu CMK 116. ve 123. maddelerinde yer alan genel nitelikli arama ve elkoyma hükümlerinin dışında CMK m. 134[371] ile bilişim sistemlerinde işlenen suçlar bakımından özel mahiyette bir koruma tedbiri hüküm altına almıştır[372].

Bu düzenlemeyle ceza muhakemesinin asıl amacı olan maddi gerçeğin ortaya çıkarılması için delil elde etmek amacıyla bilişim sistemlerinde arama, kopyalama ve elkoyma olanağı tanınmıştır[373]. Kanun koyucu bu hususu maddenin gerekçesinde *"ancak bilgisayarlardaki kayıtların gerçeğin açığa çıkarılması yönünden, ceza davasında delil, iz, eser ve emare oluşturacağı ortadadır"* şeklinde vurgulamıştır. Bunun neticesinde, bilişim sistemleri olarak adlandırabileceğimiz bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılan aramalarda bu düzenleme uygulanacak olup, bu madde kapsamına girmeyen durumlarda ise -bu maddeye aykırılık teşkil etmemek koşuluyla- genel arama ve elkoyma hükümlerinden faydalanılacaktır[374].

---

[371] CMK Madde 134 – *"(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. (Ek üç cümle: 25/7/2018-7145/16 md.) Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.*
(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
(5) *Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."*

[372] Dülger, Dülger, Murat Volkan, Bilişm Suçları ve İnternet İletişim Hukuku, s. 645; Yargıtay Ceza Genel Kurulu Kararı, 25.02.2020, E. 2016/544, K. 2020/127.

[373] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 562.

[374] Tanrıkulu, Cengiz, "Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma" Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s 350

Bilgisayar, bilgisayar programları ve kütüklerine yönelik özel bir düzenleme getirme sebebi olarak içinde bulunduğumuz teknolojik çağ ve dijitalleşme, bilişim sistemlerinin yaygın olarak kullanılması ve bunun neticesinde bilişim sistemleriyle bağlantılı suçların giderek artması sebebiyle etkin şekilde soruşturulma gerekliliği ileri sürülebilir. Örneğin ekonomik suçlarda, telif hakkı ihlallerinde, bilgisayar sabotajı vb. hukuka aykırı eylemlerde delil elde etmek için bilişim sistemleri aranabilir ve böylelikle büyük miktarda veriye el konulabilir[375].

Bilişim sistemlerinde arama, kopyalama ve elkoyma işlemlerin yapılabilmesi için somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı aranmaktadır. Bu bağlamda kuvvetli şüphe bakımından, bunun genellikle koruma tedbirleri bakımından bir ön koşul olarak aranan şüphe türü olduğunu ifade edebiliriz[376]. Bununla birlikte başka yolla delil elde etme olanağı bulunmamalıdır.

Bilişim sistemlerinin kullanılması suretiyle işlenen suçlarda, delil olarak kullanılacak verilerin elektronik nitelikte olması sebebiyle, klasik delil elde etme yöntemleri artık yetersiz kalmaktadır[377]. Bu bağlamda dijital verilerin öneminin arttığını görmekteyiz. Günümüzde akıllı telefonlar, akıllı saatler ve akıllı ev sistemleri gibi çeşitli veri taşıyıcıları birçok veriyi kaydetmekte ve bunlar soruşturma makamları için önemli deliller haline gelmektedir[378]. Bu nedenle elektronik delilin sadece bilgisayar, bilgisayar programları ve kütüklerinden değil, içinde bilişim teknolojisi barındıran birçok farklı veri taşıyıcısından elde edilebileceği vurgulanmaktadır[379]. Nihayet, veri taşıyıcılarının da CMK m. 134 kapsamına girdiği ve bu surette dijital verilere ilişkin aramanın, kopyalamanın ve elkoymanın mümkün olduğu kabul edilmelidir[380].

Söz konusu tedbirin uygulanması hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilmesi gereken karara bağlıdır. Cumhuriyet savcısının karar vermesi halinde, bu kararın yirmi dört saat içinde hâkim onayına sunulması gerekir ve hâkim kararını en geç yirmi dört saat içinde vermelidir. Eğer

[375] Kassebohm in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, §43 Strafrecht im Bereich der Informationstechnologien Rn. 426.
[376] Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, s. 640.
[377] Kunter, Nurullah/ Feridun Yenisey/Ayşe Nuhoğlu: Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18.Bası, İstanbul, Beta Yayınevi, 2010, s. 1092.
[378] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 542.
[379] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 544.
[380] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 543.

sürenin dolması söz konusu olursa ya da hâkim aksine bir karar verirse, alınan kopyaların ve çözümü yapılan metinlerin derhal imha edilmesi hüküm altına alınmıştır.

Bununla birlikte genel arama ve elkoyma yöntemlerine başvurulması suretiyle, şüphelinin bilgisayarı üzerinde gerçekleştirilecek tedbirlerin uygulanması sonucunda birçok temel hak ve özgürlüğe müdahalenin söz konusu olacağı ifade edilmektedir. Zira genel arama tedbirinin şartları gerçekleşmiş olsa da bu bilgisayar üzerinde bir arama yapmak için şartların gerçekleşmiş olması anlamına gelmemektedir. Neticede genel arama kararına dayalı bilgisayar üzerinde arama yapılması ölçülülük ilkesine aykırılık olarak değerlendirilmektedir[381].

Ayrıca asıl amaç, bilgisayar ve bilgisayar kütüklerine elkoymaksızın sistemde arama yapıp gerekli verilere ulaşmak olup, bunların sadece kopyasının alınmasıdır[382]. Böylelikle Avrupa İnsan Hakları Mahkemesi kararlarına da uygun davranılmış olunur. Nitekim Avrupa İnsan Hakları Mahkemesi bir kararında bilgisayarın uzun süre muhafaza edilmesini Avrupa İnsan Hakları Sözleşmesi'nin ihlali olarak kabul etmiştir[383]. Bu nedenle bilişim sistemlerine elkonulması, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması şartıyla gerçekleştirilebilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan sistemlerin gecikmeksizin iade edilmesi gerektiği hüküm altına alınmıştır.

Ancak uygulamada arama işleminin bilişim sisteminin bulunduğu yerden ziyade, elkoyma tedbirinin uygulanması suretiyle kolluk görevlileri tarafından kendi merkezlerinde yapıldığı ileri sürülmektedir. Bunun neticesinde istisna olması gereken elkoyma tedbiri hatalı şekilde kural haline getirilmektedir[384].

Bilişim sistemlerinin manipüle edildiği iddialarının önüne geçmek, soruşturmanın güvenirliği ve tarafsızlığını korumak amacıyla[385], bilgisayar veya bilgisayar kütüklerine elkonulduğunda sistemdeki tüm verilerin yedeklemesi yapılması gerekmektedir. Bunun sonucunda yedeklemenin bir kopyası oluşturulur,

[381] Öztürk/Kazancı/Güleç, s. 192.
[382] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 562; Ünver/Hakeri, Ceza Muhakemesi Hukuku, s. 439.
[383] AİHM SIMIRNOV/Rusya kararı, 71362/01, No. 98. Söz konusu karada ceza davasına kanıt olarak eklenen hukukçunun bilgisayarının uzun süre boyunca muhafazası Avrupa İnsan Hakları Sözleşmesinin ihlali olarak kabul edilmiştir.
[384] Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, s. 646.
[385] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s.564; Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, s. 644

şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilir. Ayrıca bu sırada müdafiin mutlaka hazır bulundurulmasında fayda vardır. Böylece şüpheli veya sanığın haklarını gözetecek dengeleyici bir usuli tedbir alınmış olacaktır.

Bunun ötesinde, bilişim sistemlerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği, kopyası alınan verilerin ise kâğıda yazdırılarak, bu hususun tutanağa kaydedilmesi gerektiği düzenlenmiştir. Ancak dijitalleşmenin beraberinde getirdiği teknolojik gelişmeler dikkate alındığında, bu hükmün uygulanmasının zor ve yanlış olduğu ileri sürülmektedir. Kopyası alınan verilerin kâğıda yazdırılmasının özellikle büyük hacimli dijital veri ve dosyalar söz konusu olduğunda, mümkün olmayacağı haklı şekilde vurgulanmaktadır[386].

Bilişim sistemlerine doğrudan uygulanan bu tedbir ile kişilerin temel hak ve özgürlerine yoğun bir müdahale söz konusu olup, kişilerin özel hayatı, hayatın gizli alanı ve kişisel verilerin gizliliği etkilenmektedir[387].

Hükümde soruşturma evresinden ve şüpheliden bahsedilmesine rağmen bilişim sistemlerinde aramaya, kopyalamaya ve elkoymaya kovuşturma evresinde de başvurulabileceği savunulmaktadır[388]. Bunun gerekçesi olarak, maddi gerçeğin ortaya çıkmasında re'sen araştırma yükümlülüğü bulunan hâkimin yargılama devam ederken bu tedbire başvurabilmesi gerektiği ileri sürülmektedir[389].

Online arama ile mukayesesi bakımından, yukarıda da belirttiğimiz gibi online aramanın gizli bir soruşturma tedbiri olarak düzenlenmesi soruşturma makamlarına bilişim sistemlerinin doğrudan aranması, verilerin kopyalanması ve el konulması ile kıyaslandığında taktiksel avantajlar sağlamaktadır. Nitekim online aramanın temel amacı, veri taşıyıcıları ve bilgi teknolojisi sistemleri üzerindeki şifreleme tekniklerini aşmaktır. Bilişim sistemlerinin açık bir şekilde aranıp ve bunlara el konulması halinde, içindeki veriler eğer kriptografik teknikler ile şifrelenmişse, şifrelerin çözümü oldukça zor hatta bazen imkansızdır[390].

Buna ek olarak, online arama tedbiri sistemin sürekli izlenmesine olanak tanır. Müdahale uzunca bir süre devam edebilir ve böylelikle yazılımın bilişim sisteminde bulunduğu süre boyunca "gerçek zamanlı" unsurlara sahip olan bir gözetim gerçekleşir. Bunun sonucunda geleneksel bir arama tedbirine kıyasla çok daha fazla

[386] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s.565.
[387] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s.562.
[388] Şahin/Göktürk, Ceza Muhakemesi Hukuku, s. 373 ;
[389] Gökcen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 496.
[390] Sinn, Stellungnahme, S. 2

bilgi elde edilip, çok sayıda veriye ulaşılabilir, tüm kullanım davranışları izlenebilir[391] ve kapsamlı kişilik profilleri oluşturulabilir[392].

d. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi araya bir vasıta sokulmak suretiyle iletişimin tespiti, dinlenmesi ve kayda alınması olarak düzenlenmiştir. Bu bağlamda öncelikle iletişim ve telekomünikasyon kavramlarının kapsama alanını belirlemek gerekir. Öncelikle ifade edilmelidir ki CMK'da telekomünikasyon, iletişim, iletişimin denetlenmesi, tespiti, dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi kavramları tanımlanmamıştır.

Türk Dil Kurumu iletişimi, "*duygu, düşünce veya bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması; bildirişim, haberleşme, komünikasyon*", teknik anlamıyla ise "*telefon, telgraf, televizyon, radyo vb. araçlardan yararlanarak yürütülen bilgi alışverişi; bildirişim, haberleşme, muhabere, komünikasyon*" olarak açıklamıştır.

Sosyal varlıklar olan insanlar, yaşamlarını çevreleriyle iletişim kurarak sürdürürler ve birbirlerini ancak iletişim yoluyla anlayabilirler. Genel olarak iletişim, bir göndericinin bir alıcıya bir şey hakkında sözlü veya yazılı bir mesaj gönderdiği, bu mesajın alıcı tarafından analiz edildiği ve duygu, düşünce ve fikirleri içeren anlamların ortak simgeler kullanılarak iletildiği süreç olarak tanımlanabilir.[393]

İletişimin, yüz yüze olan ve olmayan iletişim olmak üzere iki türü bulunmaktadır. Yüz yüze iletişim, insanların iletici görevi gören araçları kullanmadan birebir gerçekleştirdikleri iletişim türüdür. Buna karşılık duygu, düşünce ve bilgilerin telefon, televizyon, posta, basın, radyo vb. araçlar kullanılarak karşı tarafa iletilmesine yüz yüze olmayan iletişim denir. Telekomünikasyon yoluyla yapılan iletişim tedbiri bakımından, iletişim araya bir vasıta sokularak gerçekleştirildiğinden, yüz yüze olmayan iletişim söz konusudur.

Türk Dil Kurumuna göre telekomünikasyon, *"Haber, yazı, resim, sembol veya her çeşit bilginin tel, radyo, optik vb. elektromanyetik sistemlerle iletilmesi, bunların yayımı veya alınması; uz iletişimdir"*[394].

---

[391] Meyer-Gossner/Schmitt, §100b, Rn. 1.
[392] BVerfG 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833 ff; Grossmann, GA 2018, 433.
[393] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 142.
[394] Telekomünikasyon ne demek TDK Sözlük Anlamı (sozluk.gov.tr), Erişim tarihi: 01.06.2024:

Telekomünikasyon kavramının, Türkçe olmayan "communication" kelimesinin önüne elektronik, elektromanyetik gibi anlamlara gelen "tele" ekinin getirilmesiyle oluşturulmuş, "elektronik-elektromanyetik iletişim" anlamına geldiği belirtilmektedir[395]. Bununla birlikte, haber, yazı, resim, sembol veya her çeşit bilginin tel, radyo, optik vb. elektromanyetik sistemlerle iletilmesi, bunların yayımı veya alınması anlamları taşıdığı ifade edilir[396].

Bu tanımların neticesinde bir iletişimin telekomünikasyon olarak değerlendirilebilmesi için her türlü görüntü, ses veya sembolün elektromanyetik bir sistemle karşı tarafa aktarılması şartı gerektiği söylenebilir. Ayrıca yapılan tanımların oldukça geniş kapsamlı olduğu; nerede, nasıl üretilmiş, işlenmiş ya da depolanmış olursa olsun, her türlü işaret, ses, sembol, görüntü ve diğer elektrik sinyallere dönüştürülebilen her türlü verinin iletilmesi, gönderilmesi, alınması telekomünikasyon faaliyetinin konusunu oluşturacağı vurgulanmaktadır[397].

Sonuç olarak, insanların günlük hayatlarında sıkça kullandıkları telefon, faks, teleks, telsiz, televizyon ve radyo yayınları ile internet, telekomünikasyon teriminin kapsamına girmektedir. Bununla birlikte bir iletişim faaliyetinin telekomünikasyon olarak nitelendirilmesi için anında karşılıklı bir iletişimin kurulması şartı da aranmamaktadır. Bu çerçevede örneğin elektronik posta gönderiminde tek taraflı bir iletimin gerçekleştiği, ancak bu durumun iletinin gönderiliş şekli ve niteliği sebebiyle telekomünikasyon olarak kabul edilmesini engellemediği, bunun telekomünikasyon yoluyla yapılıp yapılmadığının belirleyici ölçüt teşkil ettiği ileri sürülmektedir[398].

Bununla birlikte, kanun koyucunun iletişimde kullanılan denetlemeye tabi belirli vasıtaları saymak yerine, "telekomünikasyon yoluyla yapılan iletişim" diyerek, teknolojik cihazlardan gelecekte ortaya çıkabilecekleri de kapsamayı hedeflediğini ifade edebiliriz. Bunun sonucunda, internet ve bilgisayar kullanılarak yapılan iletişim (SMS, MMS, E-mail vb.) de bu kapsamda ele alınabileceği kabul edilmektedir[399].

Telekomünikasyon yoluyla yapılan iletişim, suçun önlenmesi amacıyla denetlenebileceği gibi, işlenmiş olan suçların soruşturma ve kovuşturma evresinde delil elde etmek için de denetlenebilir. 2005 yılında 5397 sayılı kanunun yürürlüğe

[395] Ekici, Şerafettin, Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon (Elektronik İletişim) Hukuku, İstanbul, Vedat Kitapçılık, 2006, s. 3
[396] Ünver/Hakeri, s. 441.
[397] Ekici, s. 4.
[398] Ünver/Hakeri, s. 442; Ekici, s. 4,5.
[399] Şen, "E-Posta Takibi", Terazi Hukuk Dergisi, s.88-89.

girmesiyle birlikte, adli ve önleme amaçlı telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirleri arasında bir ayrım yapılmış; önleme amaçlı denetim PVSK, JTK ve MİT Kanunu kapsamında yasal dayanağa kavuşmuştur.

(1) Önleme Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi

Günümüzde teknolojik gelişmelerin suç artışına sebep olması nedeniyle, devletler suç ile mücadelede yeni yöntemler kullanmak zorunda kalıp, bunlardan bazıları henüz suç işlenmeden müdahalede bulunarak bir suçun önlenmesine hizmet etmektedirler. Bu tedbirlerin suç işlenmeden önce uygulanabilmesi için bireysel yararın yanı sıra toplumsal bir yararın da bulunması olması gerekir. Herhangi bir suçun cezalandırılmasının toplumsal bir yararı olduğu kabul edilmekle birlikte, bazı suçların işlenmesinden kaynaklanan toplumsal zarar daha ciddidir. Bu ciddi zarar riskini önlemek için yasa koyucu, bireyin belirli hak ve özgürlüklerine, özellikle de haberleşme özgürlüğüne müdahale edebilir. Bu doğrultuda, "ön alan soruşturmaları" olarak adlandırılan bir zaman diliminde doğacak tehlikeyi en başından savuşturma ve istihbari bilgi toplama amacına götürür[400]. Ön alan soruşturmalarında etkin bir önleme tedbiri olarak da şüphesiz iletişimin denetlenmesi tedbirinin yer aldığı ifade edilmelidir[401].

Önleme Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi bakımından mevcut yasal düzenlemeler[402] şu şekildedir: "2559 sayılı Polis Vazife ve Salahiyet Kanununda İletişimin Denetlenmesi", "2803 Sayılı Jandarma Teşkilat Görev ve Yetkileri Kanununda İletişimin Denetlenmesi", "2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda İletişimin Denetlenmesi" ve "Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanununda İletişimin Denetlenmesi".

Bu adı geçen tüm önleme amaçlı iletişimin denetlenmesi tedbirlerine başvurulmasının sebebi henüz suç işlenmeden müdahalede bulunarak, kamu düzeninin bozulmasına ve bireylerin zarar görmesine engel olmaktır. Bu tedbir, devletin bireyler ve toplum için güvenlik ve huzur sağlamasıyla meşrulaştırılmaktadır. Esas olarak idari nitelikte olan önleme amaçlı iletişimin denetlenmesi gizli uygulanan bir tedbirdir ve

[400] Kızılırmak, s. 32.
[401] Taşkın, Mustafa, Adli ve İstihbari Amaçlı İletişimin Denetlenmesi, 4.baskı, Ankara: Seçkin Yayınları, 2013, s. 189.
[402] Öztürk/Eker Kazancı/ Soyer Güleç, s. 230 vd.

istihbari amaca hizmet eder[403]. Ayrıca yukarıda anılan kanunlar çerçevesinde yürütülen önleme ve istihbari faaliyetlerde elde edilen deliller bakımından, bunların başka amaçlar dışında kullanılmasını engellemek için güvencelerin getirildiği de vurgulanmalıdır.

(2) Adli Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi

Adli amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi tedbiri CMK 135. madde[404] ve devamında düzenleme altına alınmıştır. CMK m. 135'te

---

[403] Bulduk, Seyfi, Telekomünikasyon Yoluyla Yapılan İletişimin Adli ve Önleme Amaçlı Olarak Denetlenmesi. 1.baskı. Ankara; Adalet Yayınevi, 2015, s. 170.

[404] İletişimin tespiti, dinlenmesi ve kayda alınması: CMK Madde 135 –
(1) (Değişik: 21/2/2014–6526/12 md.) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır.36 (Mülga son iki cümle: 24/11/2016-6763/26 md.)
(2) (Ek: 21/2/2014–6526/12 md.) Talepte bulunulurken hakkında bu madde uyarınca tedbir kararı verilecek hattın veya iletişim aracının sahibini ve biliniyorsa kullanıcısını gösterir belge veya rapor eklenir.
(3) Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir.
(4) Birinci fıkra hükmüne göre verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu, tedbirin türü, kapsamı ve süresi belirtilir. Tedbir kararı en çok iki ay için verilebilir; bu süre, bir ay daha uzatılabilir. (Ek cümle: 25/5/2005 – 5353/17 md.) Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim yukarıdaki sürelere ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere uzatılmasına karar verebilir.
(5) Şüpheli veya sanığın yakalanabilmesi için, mobil telefonun yeri, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebilir. Bu hususa ilişkin olarak verilen kararda, mobil telefon numarası ve tespit işleminin süresi belirtilir. Tespit işlemi en çok iki ay için yapılabilir; bu süre, bir ay daha uzatılabilir.
(6) (Ek: 2/12/2014-6572/42 md.) Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti, soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır. Kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi belirtilir. (Ek cümleler: 24/11/2016-6763/26 md.) Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtlar derhâl imha edilir.
(7) Bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur.
(8) Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir: a) Türk Ceza Kanununda yer alan; 1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80) ile organ veya doku ticareti (madde 91), 2. Kasten öldürme (madde 81, 82, 83), 3. İşkence (madde 94, 95), 4. Cinsel saldırı (birinci fıkra hariç, madde 102), 5. Çocukların cinsel istismarı (madde 103), 6. (Ek: 21/2/2014 – 6526/12 md.) Nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149) ile nitelikli dolandırıcılık (madde 158), 7. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), 8. Parada sahtecilik (madde 197), 9. (Mülga: 21/2/2014 – 6526/12 md.; Yeniden düzenleme: 24/11/2016-6763/26 md.) Suç işlemek amacıyla örgüt

iletişimin denetlenebilmesi için gerekli koşulların neler olduğu, hangi suçlar ve hangi kişiler açısından iletişimin denetlenmesi tedbirine başvurulabileceği, m. 136 'da şüpheli veya sanığa yüklenen suç dolayısıyla müdafiin iletişimin denetlenmesine ilişkin sınırlama, m. 137' de kararların yerine getirilmesine ilişkin koşullar, iletişimin içeriklerinin yok edilmesi, m. 138' de ise iletişimin denetlenmesi sırasında tesadüfen ele geçen delillere ilişkin hareket şekilleri hüküm altına alınmıştır.

Yapılan iletişimin CMK m. 135 kapsamında değerlendirilebilmesi için, kişilerin söz konusu iletişimi telefon, faks, bilgisayar ve benzeri bir vasıta kullanmak suretiyle gerçekleştirmesi zorunludur. Aksi takdirde, bu tür araçlar kullanılmaksızın doğrudan yüz yüze gerçekleşen iletişim CMK m. 139 ve 140'da ele alınmış olan "Gizli Soruşturmacı ve Teknik Araçlarla İzleme" tedbirlerinin kapsamına girebilir[405].

CMK m. 135 gereği telekomünikasyon yoluyla yapılan iletişimin denetlenmesi farklı yöntemlerle yapılabilmekte olup, bunlar iletişimin tespiti, dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi ve mobil telefonun yerinin tespiti olarak hüküm altına alınmıştır.

Bu koruma tedbirine başvurulabilmesinin temel koşullarından biri, maddede belirtilmiş suç kataloğudur. İletişimin denetlenmesi yöntemleri bakımından farklılıklar söz konusu olup, iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi bakımından suç kataloğu öngörülmüş olup, tedbir sadece bu suçlar için uygulanabilir. Bu suçların belirli bir ağırlığa sahip olduğu ve işleniş biçimleri nedeniyle, iletişimin denetlenmesi tedbirine en çok ihtiyaç duyulacak suçlar olarak belirlendiği söylenmektedir[406]. Burada özellikle belirtilmesi gereken iki husus var. Bunlardan biri, bu katalog suçları dışındaki suçlarla ilgili olarak iletişimin dinlenmesinin, kayda alınmasının ve sinyal bilgilerinin değerlendirilmesinin mümkün

---

kurma (madde 220, fikra üç), 10. (Ek: 25/5/2005 – 5353/17 md.) Fuhuş (madde 227), 11. İhaleye fesat karıştırma (madde 235), 12. (Ek: 24/11/2016-6763/26 md.) Tefecilik (madde 241), 13. Rüşvet (madde 252), 14. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282), 15. (Değişik: 2/12/2014-6572/42 md.) Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302) , 16. (Ek: 2/12/2014-6572/42 md.) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316), 17. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları. b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları. c) (Ek: 25/5/2005 – 5353/17 md.) Bankalar Kanununun 22 nci maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,39 d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar. e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.
(9) Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz."

[405] Kaymaz, s.57.

[406] Ünver/Hakeri, s. 445.

olmadığıdır. Diğer husus ise telekomünikasyon yoluyla iletişiminin tespiti ve bununla birlikte telefonunun yerinin tespiti bakımından suç kataloğunun dikkate alınması zorunluluğun bulunmaması, herhangi bir suçta dahi bu tedbirin uygulanabilmesidir[407].

Bununla birlikte telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirinin uygulanması "bir suç dolayısıyla" ceza soruşturulması yapılması şartına bağlanmıştır. Bu çerçevede ceza muhakemesi hukuku bakımından bu yetkinin delil elde etmek amacıyla halen işlenmekte olan bir suçun kovuşturmasıyla sınırlı olduğu ifade edilmektedir[408].

Ayrıca CMK m. 135 gereği *"suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* ile *"başka türlü delil elde etme imkanının da bulunmaması"* aranmaktadır. Kuvvetli şüphe sebeplerinin varlığı, basit bir başlangıç şüphesinden daha yoğun ancak yeterli veya kuvvetli şüphe derecesine ulaşma gerekliliği bulunmayan şüphe olarak tanımlanabilir[409].

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin hukuki niteliği bakımından öğretide farklı görüşler bulunmaktadır. Bir görüşe göre koruma tedbiri olarak değil, delil elde etme amacıyla başvurulan bir araştırma vasıtasıdır[410]. Diğer bir görüş ise kanunda düzenlenmiş diğer koruma tedbirlerinden farklı olarak gizli gerçekleştirilmesi ve işlenmiş ve işlenmekte olan suçlara yönelik delil elde etme amacıyla başvurulması nedeniyle, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirinin hukuki niteliğini gizli bir soruşturma tedbiri olarak benimsemiştir[411]. Farklı bir başka görüşe göre ise tedbir önleyici veya adli niteliğine göre değerlendirilmektedir. Buna göre adli niteliği itibariyle, işlenmiş bir suçun aydınlatılması için delil elde etme amacından dolayı koruma tedbiri olarak sınıflandırılmakta olup, önleyici niteliği haiz ise delile götüren vasıta olarak adlandırılmaktadır[412]. Başka bir görüşe göre, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri "modern koruma tedbiri" olarak kategorize edilip, aslında postada el koyma tedbirinin bir türü olarak kabul edilmektedir[413]. Öğretideki bu farklı görüşlere rağmen, kanun koyucunun telekomünikasyon yoluyla iletişimin

[407] Ünver/Hakeri, s.446.
[408] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 556.
[409] Gökçen/Balcı/Alşahin/Çakır, s. 514.
[410] Centel/Zafer, s. 514.
[411] Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s. 373.
[412] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 508.
[413] Kunter/Yenisey/Nuhoğlu, s.37.

denetlenmesi tedbirini, 5271 sayılı Ceza Muhakemesi Kanununun Birinci Kitabının Dördüncü Kısmında "Koruma Tedbirleri" başlığı altında düzenlediği ifade edilmelidir.

Diğer koruma tedbirleri gibi telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri de temel hak ve özgürlüklere ciddi şekilde müdahale etmektedir. Burada özellikle Anayasamızın 22. maddesiyle düzenlenme altına alının kişilerin hem haberleşme hakkını hem de haberleşmenin gizliğini kapsayan "haberleşme hürriyeti" etkilenmektedir[414]. Koruma tedbiri niteliği sebebiyle, yasada düzenlenme, zorunlu durumlarda uygulanma, geçici, araç, orantılı, görünüşte haklı olma, ikinci derecede uygulanabilirlik, bir karara dayanma olarak sıralayabileceğimiz koruma tedbirlerinin ortak özelliklerinin telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri için de geçerli olduğunu ifade edebiliriz.

Haberleşme özgürlüğüne ağır bir müdahale teşkil etmesi sebebiyle, bu tedbir kural olarak hâkim kararıyla, gecikmesinde sakınca bulunan hallerde ise Cumhuriyet Savcısı kararı ile uygulanabilir. Bu durumda Cumhuriyet Savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim kararını en geç yirmi dört saat içinde verir. Aksi durumda, kayıtların derhal silinmesi gerekir[415].

Online arama ile mukayese edildiğinde, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri de gizli gerçekleştirilen bir tedbir olmakla beraber, kapsadığı veriler daha sınırlıdır ve devam eden iletişim sürecine yöneliktir. Dolayısıyla telekomünikasyon yoluyla yapılan iletişimin denetimi yalnızca devam eden iletişimin izlenmesini ve kaydedilmesini içerir. Buna karşılık online arama gerek kullanılan yöntem gerekse başvurulan amaç bakımından farklılık arz eder. Online arama gereği casus yazılım olarak tanımlanabilen teknik araç vasıtasıyla tedbire maruz kalan kişinin bilgi teknoloji sistemine sızılarak sistemde kayıtlı tüm verilerine erişim sağlanabilmektedir[416].

Online aramaya yönelik anayasal müdahalenin kapsamının, geleneksel telekomünikasyon yoluyla yapılan iletişimin denetlenmesine kıyasla birçok açıdan çok daha ciddi olduğu vurgulanmalıdır. Bunun nedeni, online aramanın gizli bir şekilde ve uzun bir süre boyunca gerçekleştirilebilmesi olup, bu surette sistemin sürekli izlenebilmesidir[417].

---

[414] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 507.
[415] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 553.
[416] Knierim/Oehmichen/Beck/Geisler, §100b, Rn. 59.
[417] MüKoStPO/Rückert StPO §100b Rn.2.

e. Alman CMK'da Düzenlenmiş Kaynak Telekomünikasyon Denetimi ("Quellen-Telekommunikationsüberwachung")

Kaynak telekomünikasyon denetimi olarak Türkçe'ye tercüme edilebilecek olan[418] *"Quellen-Telekommunikationsüberwachung"* online arama tedbiri ile 2017 yılında Alman Ceza Muhakemesi Kanunu'nun 100a maddesinin 1. fıkrasının 2. ve 3. cümlesinde düzenlenerek [419] yürürlüğe girmiştir.

Kaynak telekomünikasyon denetimi ile özel olarak geliştirilmiş casus yazılım kullanmak suretiyle yabancı bir bilgi teknoloji sistemine gizlice sızılarak iletişim izlenip kaydedilebilmektedir[420]. Yukarıda açıkladığımız geleneksel tedbir olan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ile de telekomünikasyon ağına girilip iletişim tespit edilebilir, dinlenebilir ve kaydolunabilir. Ancak eğer iletişim şifrelenmiş ise geleneksel tedbir elverişli olmayıp, amaca hizmet etmez.

Günümüzde iletişimin büyük bir kısmı İnternet Protokolü (IP) tabanlı gerçekleştiğinden ve çok sayıda "IP üzerinden ses (VoIP)" ve messenger hizmetleri iletişim içeriğini şifrelediğinden, soruşturma makamlarına telekomünikasyon ağında izleme ve kayıt yaparken genelde şifrelenmiş veriler aktarılmaktadır. Bu verilerin şifresinin çözülmesi mevcut bilgi işlem kapasiteleri ve kullanılan algoritmalar sebebiyle ya hiç mümkün değildir ya da zaman alıcı ve yüksek maliyetlidir[421].

Dolayısıyla kaynak telekomünikasyon denetimi, örneğin *"WhattsApp"* veya *"Telegram"* gibi *"messenger hizmetleri"* kullanımında akıllı telefonlar aracılığıyla iletişimin giderek daha şifreli hale gelmesi sorununa bir çözüm sunarak, modern teknolojinin gereğini yerine getirmeyi amaçlamaktadır[422]. Bu doğrultuda şifreli iletişimin gerçekleştiği durumda, deyim yerindeyse "kaynaktaki" verilerin okunmasını mümkün kılmaktadır. Bu amaçla, hakkında tedbir uygulanan kişinin akıllı telefon veya bilgisayar gibi cihazına bir yazılım yüklenip, bu yazılım sayesinde iletişim içeriğine "kaynağında" erişilir. Bunun sonucunda iletişim içeriğine ya göndericinin sisteminde şifrelenmeden önce ya da alıcı tarafından şifresi çözüldükten sonra erişilir ve soruşturma makamlarına iletilir[423].

---

[418] Köker, Nilüfer, Çeviri: Prof. Dr. Prof. h.c. Arndt Sinn, "Kaynak Telekomünikasyon Denetimi ve Online Arama Yoluyla Yeni Gizli Soruşturma Tedbirleri", Fasikül Aylık Hukuk Dergisi, Haziran, 2019.
[419] StPO §100 a Absatz 1 Satz 2 und 3, § 100a StPO - Einzelnorm (gesetze-im-internet.de), Erişim tarihi: 01.06.2024:
[420] Sinn, Stellungnahme zum Gesetzesentwurf BT-Drucksache 18/11272, s. 4.
[421] BT-Drucksache 18/12785, s. 48.
[422] Momsen/Bruckmann, Soziale Netzwerke als Ort der Kriminalitaet, KriPoZ 1/2019, S. 22.
[423] BT-Drucksache 18/12785, s. 48, 49.

Geçmişte "Access Provider" olarak adlandırılan erişim sağlayıcı vasıtasıyla arayüzler aracılığıyla devam eden iletişim süreçlerine erişim sağlanmasının nispeten daha kolay olduğu, bu sayede telefon konuşmalarının dinlenilmesinin veya SMS olarak bilinen kısa mesajların kaydedilmesinin mümkün olduğu ifade edilmektedir[424]. Ancak günümüzde "uçtan uça şifreleme" yöntemiyle[425] göndericiden alıcıya kadar tüm iletişim yolunun şifrelendiği ve bu sebeple şifrelenmiş iletişim içeriklerinin soruşturma makamları için büyük zorluk teşkil ettiği belirtilmektedir[426].

Kaynak telekomünikasyon denetiminin geleneksel telekomünikasyon denetimiyle ortak özelliği, aynı amaca hizmet etmeleridir. Her iki denetim yolu, iki veya daha fazla kişi arasında telefon, ses, video veya kısa mesaj yoluyla yapılan iletişimin içeriğinin soruşturma amacıyla kullanılmasını amaçlar. Bu nedenle her ikisi de aynı iletişim verilerini hedeflemektedir. Ancak, telekomünikasyona erişim yöntemi farklıdır. Kaynak telekomünikasyon denetimi, örneğin Telekom gibi erişim sağlayıcı ile yapılan telefon görüşmesine, yani iletim yoluna müdahale etmez. Bunun yerine, iletişimi kuran cihaza nüfuz edip, sistemi casusluğa maruz bırakır[427].

İstenmeyen bir yan sonuç olarak, kaynak telekomünikasyon denetiminin, devlet yetkililerine geleneksel telekomünikasyon gözetiminden daha fazla erişim imkânı sağladığı belirtilmektedir[428]. Tedbirin amacı bu olmasa bile, soruşturmacılar teknik olarak sadece devam eden iletişim süreçlerine değil, aynı zamanda veri deposundaki çok daha kapsamlı, son derece hassas veri kayıtlarına da erişebilmektedir. Bir akıllı telefona bir bütün olarak erişimi olan herkes, örneğin sadece bir mesajlaşma programındaki mesajları okumakla kalmaz, aynı zamanda mesaj arşivinde arama yapabilir, veri deposundaki özel görüntülere ve kameraya erişebilir veya hareket profilleri oluşturmak için GPS verilerini kaydedebilir[429].

Kaynak telekomünikasyon denetimini online arama tedbiri ile mukayese ettiğimizde, dışarıdan bakıldığında, her ikisinin bilgi teknoloji sistemlerine gizli erişim sağladıklarından çok farklı olmadıkları düşünülebilir. Zira her iki tedbirde de devlet ağ bağlantıları üzerinden bir bilgi teknoloji sistemine yazılım vasıtasıyla sızmakta ve onu kendi çıkarlarına kullanmaktadır. Dolayısıyla her iki yöntem de sistemi manipüle

[424] Pohlmann/ Riedel, DuD 2018, 37 (39).
[425] BT-Drucksache 18/12785, s. 51.
[426] Martini/Fröhlingsdorf, Catch me if you can: Quellen-Tekeommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020, s. 1; Kruse/Grzesiek, s. 336.
[427] BVerfGE 120, 274 (308) = NJW 2008, 822 (825) Rn. 188.
[428] Stadler, MMR 2012, 18 (19).
[429] Martini/Fröhlingsdorf, s. 3.

ederek sistemin bütünlüğünü etkilemektedir[430]. Bu nedenle kaynak telekomünikasyon tedbiri "ufak çaplı bir online arama" olarak da adlandırılmaktadır[431].

Ancak, online arama tedbiri ile bir bilgi teknoloji sisteminin tüm kişisel veri tabanına erişilir, bir kişinin tüm kullanım davranışı izlenebilir[432] ve bu nedenle hakkında tedbir uygulanan kişinin kişiliği hakkında çok daha derin bilgiler sağlanabilir[433]. Bunun aksine kaynak telekomünikasyon tedbiri daha dar kapsamlı olup, kullanılan yazılım kaynağa sızarak yalnızca devam eden iletişim sürecinden veri toplamayı amaçlar. Hedef sistemde kaydedilen verilerin devam eden güncel iletişim olarak gerçekleşmediği hallerde, bu verilerin aktarımı mümkün değildir[434].

Kaynak telekomünikasyon denetimi tedbiri ile gerçekleşen müdahalenin yoğunluğu online arama ile karşılaştırıldığında, online arama tedbirinin erişilen verilerin kapsamı nedeniyle temel hak ve özgürlükleri çok daha yoğun bir şekilde etkilediği açıkça anlaşılır[435].

[430] Buermeyer/Baecker, HRRS 2009, 433 (437).
[431] BT-Drucksache 18/12785, 50; Kruse/Grzesiek, s. 337.
[432] BT-Drucksache 18/12785, s. 54.
[433] Knierim/Oehmichen, Kapitel 20: Quellen-TKÜ und Online Durchsuchung, Rn. 59.
[434] Kruse/Grzesiek, s. 336.
[435] Bratke, die Quellen-Telekommunikationsüberwachung im Strafverfahren, 2013, S. 53.

İKİNCİ BÖLÜM
ALMAN HUKUK SİSTEMİNDE ONLİNE ARAMANIN TARİHİ GELİŞİMİ VE MEVCUT YASAL DÜZENLEMELER

I. TARİHİ GELİŞİM

A. Genel Olarak

Yirmi birinci yüzyılın başında, bilgisayarların özel ve iş hayatının her alanında yaygın olarak kullanılması, geleneksel soruşturma yöntemlerinin değiştirilmesi ihtiyacını doğurmuştur.

Bununla birlikte dünyanın her yerinde artan terör saldırıları ve özellikle 11 Eylül 2001 saldırılarından sonra, uluslararası terörizm tehdidinin bir sonucu olarak, internet tabanlı müdahale ve terörle mücadele yöntemlerinin geliştirilmesine olan ilgi artmıştır.

Ağustos 2006'da Almanya'da bölgesel trenlere yönelik yapılan bombalı çanta saldırıları siyasi tartışmaları alevlendirmiştir[436]. Bunun sonucunda, döneminin iç işleri bakanı tarafından teklif edilen *"İç Güvenliği Güçlendirme Programı (PSIS)"*, Alman Federal Meclisi Bütçe Komisyonu tarafınca 2006 yılında kabul edilmiştir[437]. Program hem önleyici hem de baskıcı alanlarda online arama imkânı sağlamaktadır[438]. Böylelikle cezai soruşturma amacıyla, bilgisayarlar üzerinde yargılamalarla ilgili içeriklerin uzaktan aranmasına resmi olarak imkân tanınmıştır.

---

[436] Kohlmann, s. 21.
[437] *"Programm zur Stärkung der Inneren Sicherheit (PSIS)"*, BT-Drs. 16/3492, 21.11.06.
[438] BT-Drs. 16/3492, 21.11.06., s. 2.

Online arama tedbiri, Federal Kriminal Dairesi Kanunu'nun 20k maddesi[439] uyarınca bir tehdidin varlığına bağlanarak açıklığa kavuşturulan önleyici alanda uygulamaya konulmuştur. Federal ve eyalet polis güçlerini destekleyen merkezi bir kurum olan Federal Kriminal Daire, suçla mücadelede polis yöntemlerini ve çalışma şekillerini araştırmak ve buna bağlı olarak ceza takibi için yeni teknik prosedürlerin uygunluğunu test etmek ve değerlendirmekle sorumludur[440].

İç Güvenliği Güçlendirme Programının başlıca amaçlarından biri, internet arama ve soruşturma olanaklarını genişletmek ve böylece federal ve eyalet güvenlik makamları arasındaki iş birliğini yoğunlaştırmaktır[441]. Bu sunulan programın kolluk düzeyinde de memnuniyetle karşılandığı, özellikle terörizm, organize suç, insan ve silah kaçakçılığı alanlarına yönelik ilerleme olarak değerlendirildiği ifade edilebilir[442].

Çalışmanın bu bölümünde online aramanın Alman Hukuk sistemindeki Federal mahkemelerin verdiği kararlar çerçevesinde tarihi gelişimi ve yasama süreci incelenecektir.

B. Federal Almanya Yargıtayı Şubat 2006 Tarihli Kararı

21 Şubat 2006 tarihinde Federal Almanya Yargıtayı bir federal mahkeme olarak ilk kez online arama tedbirinin geleneksel arama tedbirini yasal dayanak göstermek suretiyle adli amaçla uygulanmasına izin vermiştir[443]. Bu çerçevede yetkili yargıtay soruşturma hâkimi tedbiri yasal olarak değerlendirip, sadece bir defaya mahsus olmak üzere online erişim kararı vermekle kalmamış, aynı zamanda hedef sistemdeki tüm veriler elde edilene kadar tekrarlanan erişimlere de izin vermiştir[444]. Karara gerekçe olarak, bunun zaten başlamış olan ve bir mahkeme kararı kapsamına giren tek tip bir arama operasyonunun yasal olarak bağımlı bir uzantısı olduğunu ifade etmiştir[445]. Bu bağlamda, geleneksel arama tedbirinin yetkilendirme temelinin, belirli bir sınırlandırılabilir alan veya nesnede saklı olan bir şeyin devlet organları tarafından hedefli ve amaçlı bir şekilde aranmasını içerdiğini ve bu nedenle elektronik olarak

[439] Federal Kriminal Dairesi Kanununun (BKA-Gesetz) 20k maddesi 24.05.2018 tarihi itibariyle geçerliliğini kaybedip, yerine BKA-Gesetz 49. madde düzenlenmiştir.
[440] Kohlmann, s. 23.
[441] BT-Drs. 16/3492, 21.11.06., s. 2.
[442] Leipold, Klaus, Die Online_Durchsuchung, NJW Spezial, 2007, 135 (135).
[443] BGH, StV 2007, 60 (60).
[444] BGH, StV 2007, 60 (60).
[445] BGH, HRRS 2007, Nr. 468, Rn. 26.

depolanan verilerin aranmasına yönelik de olduğunu belirtilmektedir[446]. Ayrıca, arama yetkisinden aleniyet ilkesinin çıkarılamayacağı ve bu nedenle de tedbirin gizli uygulanmasına engel söz konusu olmadığı ileri sürülmektedir[447].

C. Federal Almanya Yargıtayı Ocak 2007 Tarihli Kararı

31 Ocak 2007 tarihli kararında ise Federal Yargıtay, geleneksel arama tedbirinin online aramanın gerçekleştirilmesi için yasal dayanak olarak kullanılamayacağını[448], tedbirin temel hak ve özgürlüklere neden olduğu ciddi müdahaleyi haklı gösteremeyeceğini, bu surette gerçekleştirilen tedbirlerin yasal kabul edilemeyeceğini açıklamıştır[449]. Dolayısıyla Federal Yargıtay'ın daireleri arasında online aramanın uygulanabilirliğine yönelik görüş ayrılığı yaşandığı ifade edilebilir.

Yargıtay yürürlükteki kanunu dikkate alarak, bilgisayarların gizli bir şekilde aranmasının, ne soruşturma makamlarına verilen genel soruşturma yetkisi ile ne de Ceza Muhakemesi Kanunu hükümleri ile gerekçelendirilemeyeceğini ifade etmiştir[450]. Bununla birlikte online aramanın kişisel bir hak olarak kategorize edilen ve Anayasa ile korunan bilgi edinme konusunda kendi kaderini tayin etme hakkına *("Recht auf informationelle Selbstbestimmung")* ciddi bir ihlal teşkil ettiğini belirtmiştir. Federal yüksek mahkeme aleniyet ilkesinin ve fiziksel müdahalenin geleneksel aramada dikkate alınması gerektiğini vurgulamış ve bu tedbirin gizli ve online uygulamasının geleneksel arama bağlamında uygulanamayacağını açıklığa kavuşturmuştur. Aleniyet ilkesine titizlikle uyulması gerektiği, bu ilkenin amacının tedbirin, hakkında tedbir uygulanan kalan kişinin bilgisi dahilinde ve tanıkların huzurunda yapılmasını sağlamak olduğu[451] ve soruşturma makamlarının takdirine bırakılamayacağı vurgulanmaktadır[452].

Yargıtayın 2007 yılında bu yönde karar vermesi, Kasım 2006 da başsavcının federal yargıtay soruşturma hakimine online arama emrinin çıkarılmasına yönelik

---

[446] BGH, StV 2007, 60 (60).

[447] BGH, HRRS 2007, Nr. 468, Rn. 9.

[448] Federal Yargıtayın 3. Ceza Dairesi Alman CMK 102, 110 maddelerini online arama için yasal dayanak olarak kabul etmeyip, Alman CMK 105/2 cümle 1, 106/1 ve 107/1 maddeleri gereği arama tedbirinin yalnızca açık bir şekilde gerçekleştirilebileceğini kabul etmektedir.

[449] BGH, MMR 2007, 237 (238).

[450] BFG, FD-Strafrecht 2007, 210345.

[451] BGH, MMR 2007, 237 (237).

[452]Kemper, Martin, Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZRP 2007, 105 (107); BGH, NJW, 2007, 930 (930).

yaptığı başvuru ve hâkimin bu başvuruyu reddetmesiyle ilgilidir[453]. Başsavcının başvurusu, şüpheli tarafından kullanılan dizüstü bilgisayarın, özellikle sabit diskte ve RAM'de depolanan verilerin gizli bir şekilde aranmasına ve bunlara el konulmasına; bunlar için özel olarak tasarlanmış, şüphelinin bilgisayarının belleğinde bulunan verileri kopyalamak ve incelenmek üzere soruşturma makamlarına gönderilmesi için bir yazılımın şüpheliye gönderilmesini kapsamaktadır[454]. Soruşturma hâkimi ise bilgi edinme hakkına yönelik bu ciddi müdahalenin yasal dayanağının bulunmadığını, Alman hukuk sisteminde online aramanın uygulanamayacağını belirterek başvuruyu reddetmiştir[455]. Bu karara başsavcılık tarafından itiraz edilmiş olup, Federal Yargıtayın 3. Ceza Dairesi ise itirazı karar bağlamak zorunda kalmıştır ve 31 Ocak 2007 tarihinde soruşturma hakimine yetki vermiştir.

D. 20 Aralık 2006 tarihli Kuzey Ren-Vestfalya Anayasayı Koruma Yasası

20 Aralık 2006 tarihinde Kuzey Ren-Vestfalya Anayasayı Koruma Yasası'nda[456] önleme amaçlı online arama düzenlenerek online arama ilk kez yasal olarak meşruiyet kazanmıştır. Buna göre Kuzey Ren-Vestfalya Anayasayı Koruma Yasası'nın 5/2-11 maddesi anayasayı korumayla görevli birimlere iki tür soruşturma tedbirini uygulama imkânı sağlamaktadır. Birinci alternatif gereği internet içeriklerinin gizli olarak takip edilmesi ve aydınlığa kavuşturulması, ikinci alternatif gereği ise bilgi teknoloji sistemlerine gizli olarak erişimin sağlanması mümkün kılınmıştır.

Yeni düzenlemeyle birlikte, teknik araçların kullanımı da dahil olmak üzere bilgi teknolojisi sistemlerine gizli erişimin yanı sıra, özellikle iletişim tesislerine gizli katılım gibi internetin gizli izlenmesine ve internet içeriklerinin "başka surette gizli keşfine" olanak tanınmıştır. İnternet içeriklerinin gizli keşfi, internet iletişiminin teknik olarak amaçlanan araçlarla izlenmesi anlamına gelir[457].

Ayrıca sohbetlere, açık artırmalara ve paylaşım sitelerine katılım, domain sahiplerinin belirlenmesi, ana sayfalara erişimin doğrulanması, gizli web sitelerinin keşfedilmesi ve kaydedilen bilgisayar verilerine erişim sağlanmıştır[458]. Bununla

[453] BGH BeckRS 2007, 00295.
[454] BGH, MMR 2007, 237 (237).
[455] BGH-Ermittlungsrichter, Beschluss vom 25.11.2006 – 1 BGs 184/2006, Nichtabhilfebeschluss auf die Beschwerde der Generalanwältin am 28.11.2006 (1 BGs 186/2006).
[456] Verfassungsschutzgesetz (VSG NRW) söz konusu madde 5/2 No. 11 VSG NRW'dir.
[457] BVerfG, Urt. v. 27.2.2008, Rn. 4.
[458] NRW LTag-Drs. 14/2211, s. 4.

birlikte erişim korumalı bilgilere, yani şifrelenmiş bilgilere de erişilmesi mümkündür[459].

Tedbirler, yazışma, posta veya telekomünikasyon gizliliğinin ihlalini teşkil ettiği veya eylemin niteliği ve ciddiyeti nedeniyle bu tür bir ihlale eşdeğer olduğu ölçüde, yalnızca Federal Anayasa'nın 10. maddesi ile düzenlenmiş telekomünikasyonun gizliliği temel hakkı gerekliliklerine tabi olarak kabul edilebilir[460].

E. 27.02.2008 tarihli Federal Almanya Anayasa Mahkemesinin Kuzey Ren Vestfalya Kararı

1. Hukuki Olayın Özeti

27.02.2008 tarihinde Federal Almanya Anayasası önleme amaçlı online arama tedbiri hakkında karar vermiştir[461]. Karar 20 Aralık 2006 tarihinde Kuzey Ren-Vestfalya Anayasayı Koruma Yasası'nda yürürlüğe giren önleme amaçlı online arama düzenlemesine karşı yapılan iki tane bireysel başvuruya dayanmaktadır.

Federal Anayasa Mahkemesi kararında, Kuzey Ren-Vestfalya Anayasayı Koruma Yasası ile internet içeriklerinin gizli olarak takip edilmesi ve aydınlığa kavuşturulması ile bilgi teknoloji sistemlerine gizli olarak erişimin sağlanması için getirilen tedbirlerin yasallığı konusunda net bir tutum sergileyip yetki temellerinin Federal Almanya Anayasası ile uyumlu olmadıklarına, bu nedenle hükümsüz olduklarına karar vermiştir[462].

Tedbirlerin son derece müdahaleci yapısı nedeniyle, konut dokunulmazlığı, haberleşmenin gizliliği ve kişiliğin korunması haklarının koruması kapsamına giremeyeceğinden, federal anayasa mahkemesi Anayasa'nın 1'inci maddesinin 1'inci fıkrası ve 2'nci maddesinin 1'inci fıkrası ile koruma altına alınan genel kişilik hakkının yansıması olan bilgi teknolojisi temel hakkı *("IT-Grundrecht")* olarak da bilinen bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün garanti altına alınması hakkını *("Recht auf Gewaehrleistung der Vertraulichkeit und Integritaet informationstechnischer Systeme")* geliştirmiştir[463].

---

[459] BVerfG, Urt. v. 27.2.2008, Rn. 6.
[460] Kaufmann, Noogie C., BGH lehnt Online-Durchsuchungen ab und NRW schafft statthaftes Gesetz, MMR 2/2007, XII.
[461] BVerfG, Urteil des Ersten Senats vom 27.02.2008, 1 BvR 370/07; BVerfG NJW 2008, 822 vd.
[462] BVerfG, NJW 2008, 822 (824).
[463] BVerfG NJW 2008, 822 (824).

Bu yeni geliştirilmiş bilgi teknolojisi temel hakkının etkilenmesi, müdahale yetkisinin tek başına veya teknik ağlarında veri sahibinin kişisel verilerini belli bir ölçüde içerebilecek sistemleri kapsayarak, veri sahibinin kişisel verilerine devlet tarafından erişim sağlanması ve bu surette bir kişinin hayatının önemli kısımları hakkında bilgi edinilmesi ve hatta kişiliği hakkında bir profil oluşturulabilmesi durumunda söz konusu olur. Federal Anayasa mahkemesinin kararına göre, bu temel hakkın koruma kapsamına ilgili işlev yelpazesine sahip oldukları ve çeşitli türlerde kişisel verilerin depolanmasına izin verdikleri ölçüde ister özel ister profesyonel olarak kullanılsın özellikle kişisel bilgisayarlar ve aynı zamanda cep telefonları veya elektronik günlükler girmektedir[464].

Diğer temel haklar, özellikle telekomünikasyonun gizliliği, konut dokunulmazlığı ve yine genel kişilik hakkının yansıması olarak bilinen özel hayatın gizliliği ve bilgi edinme konusunda kendi kaderini tayin etme hakları, Anayasa mahkemesinin görüşüne göre, bilgi teknolojisinin gelişmesinden kaynaklanan koruma ihtiyacını yeterince karşılamamaktadır. Bu temel hakların, bilgi teknolojisi sistemlerinin kullanımıyla kısmen ilgili oldukları ve bu nedenle kişisel gelişim için bu tür sistemlerin kullanımının artan öneminin hakkını veremeyecekleri ifade edilir[465].

Bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün garanti altına alınması hakkına değinmeden önce, konut dokunulmazlığı, haberleşmenin gizliliği ve genel kişilik hakkının yansıması olarak özel hayatın gizliliğin korunması ile bilgi edinme konusunda kendi kaderini tayin etme haklarının koruma kapsamına online arama tedbiriyle hangi ölçüde müdahale edildiği Federal Anayasa Mahkemesi kararı ışığında irdelenecektir.

2. Tedbirden Etkilenen Temel Haklar Ekseninden Kararın Gerekçesinin Hukuki Temelleri

Federal Anayasa Mahkemesi'nin 27.02.2008 tarihli Kuzey Ren Vestfalya kararında online arama tedbirinin en ağır müdahalede bulunduğu haklar bakımından yapmış olduğu inceleme ve bu detaylı incelemesi sonucu mevcut haklar açısından yapılan tartışmaların yetersizliğini tespit edişi dikkat çekicidir. Mahkeme, tüm bu tartışmalar sonucunda genel kişilik hakkının yansıması olarak bir yeni kavram daha

[464] BVerfG, Urt. v. 27.2.2008, Rn. 203.
[465] BVerfG, Urt. v. 27.2.2008, Rn. 174.

ortaya koymuştur. Aşağıda mevcut haklar bakımından yapılacak değerlendirmelerin yetersizliği konusundaki açıklamaları takiben, Mahkeme tarafından genel kişilik hakkının günün koşullarına uyarlanması şeklinde tezahür eden yeni kavramlara dair bir inceleme yapılacaktır.

a. Haberleşmenin Gizliliği Boyutuyla İnceleme

Alman Anayasası'nın 10. maddesi her türlü özel iletişimin gizliliğini korur. Buna telekomünikasyon yoluyla bireysel alıcılara fiziksel olmayan bilgi aktarımı da dahildir[466] ve böylelikle kişiliğin özgür gelişiminin bir ifadesi olarak mahremiyet güvence altına alınır[467]. Bu aynı zamanda telekomünikasyonun içeriğinin ve koşullarının, yani telekomünikasyonun hangi kişiler veya telekomünikasyon sistemleri arasında gerçekleştiğinin ne zaman ve ne sıklıkta yapılmaya çalışıldığının korunmasını da içerir[468]. Telekomünikasyon gizliliğinin koruma kapsamı örneğin e-postaları da içeren internet iletişim hizmetlerini de kapsar[469].

Bir yetkilendirme temelinin, bilgisayar ağında devam eden telekomünikasyonun içeriğinin ve koşullarının toplandığı veya ilgili verilerin değerlendirildiği bir devlet tedbiriyle sınırlı olduğu ölçüde, müdahalenin yalnızca Federal Almanya Anayasası'nın 10. maddesi gereği düzenlenmiş olan haberleşmenin gizliliği temel hakkına göre ölçülmesi gerektiği vurgulanır[470].

Bu temel hakkın koruma kapsamı, tedbirin teknik olarak iletim yoluna mı yoksa telekomünikasyon cihazına mı uygulandığına bakılmaksızın etkilenir[471]. Ancak Federal Anayasa Mahkemesine göre Anayasa'nın 10. maddesi uyarınca temel hakkın korunması, abonenin verilere gizli erişime karşı kendi koruyucu önlemlerini alabilmesi koşuluyla, bir iletişim sürecinin tamamlanmasından sonra bir iletişim abonesinin etki alanında depolanan telekomünikasyon içeriğini ve koşullarını kapsamaz[472]. Zira bu durumda, 10. maddenin önlemeyi amaçladığı uzaktan iletişimin kendine özgü riskleri artık bulunmayacaktır.

Telekomünikasyon gizliliğinin öngördüğü koruma, bir devlet kurumunun bir bilgi teknolojisi sisteminin kullanımını izlemesi veya sistemin depolama ortamını

[466] BVerfGE 67, 157 (172); BVerfGE 106, 28 (35 vd.)
[467] BVerfGE 85, 386 (396).
[468] BverfGE 67, 157 (172); BVerfGE 85, 386 (396).
[469] BVerfGE 113, 348 (383); LG Hanau, NJW 1999, 3647.
[470] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 184.
[471] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 184.
[472] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 185.

araması durumunda da sağlanmaz[473]. Bu bakımdan, bilgi teknolojisi sistemlerinin gizliliğinin ve bütünlüğünün korunması şeklinde genel kişilik hakkı tarafından kapatılması gereken bir koruma boşluğu bulunmaktadır[474].

Eğer karmaşık bir bilgi teknolojisi sistemine telekomünikasyonun izlenmesi amacıyla teknik olarak sızılırsa, bu sızma ile sistemin tamamının izlenmesi için eşiğin aşıldığı kabul edilir. Ortaya çıkan tehdit, sadece devam eden telekomünikasyonun izlenmesiyle ilişkili olanın çok ötesine geçer. Özellikle, kişisel bilgisayarda saklanan ve sistemin telekomünikasyon kullanımıyla ilgili olmayan verilere de erişilebildiğinden, Federal Anayasa mahkemesi online aramanın telekomünikasyona sızmanın çok ötesine geçtiğini kabul ederek, bu tedbirin Anayasa'nın 10. maddesinin koruma kapsamına girmediğine hükmetmiştir[475]. Sonuç olarak online arama tedbirinin devam eden telekomünikasyon faaliyetleriyle sınırlı olmamasından dolayı haberleşmenin gizliliği temel hakkı çerçevesinde bir koruma sağlanması yetersiz kalmaktadır[476].

b. Konut Dokunulmazlığı Boyutuyla İnceleme

Federal Anayasa'nın 13. maddesi ile korunan konut, mahremiyet alanı ve insan varlığının merkezi olarak kabul edilir[477]. Bu çerçevede bireyin kişiliğini devlet müdahalesi olmaksızın geliştirebileceği temel bir yaşam alanı olarak konutun mahremiyeti korunur. Bu bağlamda konut, kamunun erişimine açık olmayan ve özel yaşam için kullanılan alan olarak anlaşılmaktadır[478].

Federal Anayasa mahkemesi, konut dokunulmazlığı korumasının, yalnızca konuta fiziksel bir müdahaleye karşı savunma ile sınırlı olmadığını, devlet yetkililerinin korunan alanın dışından doğal olarak algılanamayacak olan ev içindeki süreçlere dair fikir edinmek için özel araçlar kullanılan tedbirlerin de Anayasa'nın 13. maddesine ihlal niteliği taşıdıklarını kabul etmektedir[479].

Ancak federal mahkeme, konut dokunulmazlığı güvencesinin de bilgi teknolojisi sistemlerine erişime karşı korumada boşluklar bıraktığını[480], Anayasa'nın 13. maddesinin, erişimin türüne bakılmaksızın, sistemin bir konutta bulunması

[473] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 186.
[474] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 187.
[475] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 188.
[476] Palm/Roy, NJW 1997, 1904 f.
[477] BVerfGE 18, 121 (131 vd.); BVerfGE 32, 54 (75).
[478] Manssen, Staatsrecht II Grundrechte, München 2007, Rn. 704.
[479] BVerfGE 109, 279 (309, 327).
[480] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 191.

durumunda dahi, bireylere bilgi teknolojisi sistemlerine sızılmasına karşı genel bir koruma sağlamadığını vurgulamaktadır[481].

Bunun nedeni olarak, yetkisiz erişimin konumdan bağımsız olarak gerçekleşebiliyor olması, dolayısıyla mekânsal korumanın özellikle laptoplar, cep telefonları veya kişisel dijital asistanlar gibi mobil bilgi teknolojisi sistemleri bakımından bilgi teknolojisi sistemine yönelik spesifik tehdidi önleyememesi belirtilir[482]. Bu durum, bir konutta bulunmanın bu tür izinsiz erişimlere karşı koruma sağlayamayacağı anlamına gelir, zira coğrafi konum, internet bağlantısı olduğu sürece bilgi teknoloji sistemlerine sızmaya karşı herhangi bir koruma sağlayamaz.

Bununla birlikte, bilgi teknoloji sistemine sızılırken bir bilgi teknoloji ağının kullanması söz konusu olduğu durumlarda, konutun sınırlandırılmasıyla aktarılan mekânsal mahremiyetin etkilenmediği ifade edilir. Ayrıca birçok durumda, sistemin yerinin soruşturma tedbiri için önemsiz olacağı ve çoğu zaman yetkili makam tarafından bile tanınmayacağı belirtilir[483]. Ancak soruşturma makamlarının bilgi teknolojisi sistemini fiziksel olarak manipüle etmek amacıyla konut olarak korunan bir alana girmeleri halinde, konut dokunulmazlığı temel hakkı şüphesiz ihlal edilmiş olur[484].

Bu nedenlerle Federal Anayasa Mahkemesi, konut dokunulmazlığı temel hakkının, online arama bağlamında devlet erişimine karşı koruma sağlamadığını, koruma kapsamının sadece temel yaşam alanında kişiliğin geliştirilmesi kapsamındaki menfaatlere yönelik olduğunu kabul etmektedir.

Federal Anayasa Mahkemesi 03.03.2004 tarihli "büyük ölçekli gizli dinleme müdahalesi" olarak çevrilebilen “Grosser Lauschangriff” adlı kararının[485] aksine, 13. maddenin koruma kapsamının online arama bakımından uygulanamayacağı görüşündedir. Teknik araçlar kullanılarak kamuya açık olmayan konuşmaların gizlice dinlenmesi ve kaydedilmesi anlamına gelen bu tedbir bakımından Federal Almanya Anayasa Mahkemesi, Anayasanın 13. maddesinin koruma kapsamını teknik gelişmeler ışığında geniş yorumlamıştır[486]. Bu bağlamda konut dokunulmazlığı hakkının

[481] Beulke/Meininghaus, StV 2007, S. 63 (64); Gercke, CR 2007, S. 245 (250); Schlegel, GA 2007, S. 648 (654 vd.)
[482] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 194.
[483] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 194.
[484] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 193.
[485] BVerfG, Urteil vom 03.03.2004 – 1 BvR 2378/98
[486] Buermeyer, Ulf, „Die „Online-Durchsuchung“ Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme“, HRRS, 8/2007, S. 332.

günümüz koşullarında sadece fiziksel saldırıya karşı koruyucu bir etkiye sahip olmadığı, bununla birlikte konutun teknik araçlarla izlenmesinin de buna dahil olması gerektiği vurgulanmıştır[487]. Ancak "büyük ölçekli gizli dinleme müdahalesinden" farklı olarak, online arama ile ilgili kişinin mekânsal bölümlendirmeye dayalı özel yaşam alanına müdahale edilmemektedir. Nitekim, online aramada bilgisayarın bulunduğu konum önemsizdir.

c. Genel kişilik hakkından doğan haklar

(1) Genel kişilik hakkının bir yansıması olarak özel hayatın gizliğinin korunması

Federal Almanya Anayasası'nın 2'nci maddesinin 1'inci fıkrası ile 1'inci maddesinin 1'inci fıkrası gereği genel kişilik hakkının yansıması olarak özel hayatın gizliliği korunmaktadır. Mahremiyetin korunması şeklindeki genel kişilik hakkı, bireye istenmeyen erişimden uzak kalması gereken mekânsal ve konusal olarak tanımlanmış bir alanı garanti eder[488]. Ancak, bir bilgi teknolojisi sisteminin kullanıcısının korunma ihtiyacının, mahremiyetine yönelik olarak tanımlanabilecek verilerle sınırlı olmadığı, bunun verilerin üretildiği ve diğer verilerle ilişkilendirildiği içeriğe de bağlı olduğu vurgulanır.

Sonuç olarak, sisteme sızmanın sadece kaçınılmaz olarak özel verilerin elde edilmesine yol açmadığı, aynı zamanda tüm verilere erişim sağlandığı ve bunun sonucunda sistem kullanıcısı hakkında kapsamlı bir profil çizilebileceği belirtilir[489]. Bu nedenlerle Federal Anayasa Mahkemesi, Almanya Anayasasının 2/1 ile 1/1 maddeleri ile güvence altına alınan özel hayatın gizliliğinin korunmasının, online aramanın getirdiği tehlikeleri tam olarak karşılayamayacağını ileri sürmüştür.

(2.) Bilgilerin kaderini belirleme hakkı

Federal Almanya Anayasası en son 1983 yılında *"nüfus sayımı"* kararında[490], modern veri işlemenin mevcut ve gelecekteki koşulları altında özel koruma gerektirdiğini belirterek, veri koruma ile ilgili bir temel hak oluşturmuştur: *"bilgilerin*

[487] BVerfG, Urteil vom 03.03.2004, Rn.105.
[488] BVerfGE 27, 344 (350 vd.); BVerfGE 44, 353 (372 f.).
[489] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 197.
[490] Volkszaehlungsurteil des Bundesverfassungsgerichts, BVerfGE 65, 1 vd.

kaderini belirleme hakkı" (Informationelle Selbstbestimmung). 80'li yıllarda bu koruma ihtiyacı, Alman vatandaşlarının bilgisayar ortamında kayıt altına alınmasıyla ilgiliydi.

Kararda, gelişen bilgi teknolojileri nedeniyle hızla şeffaflaşan bireyin karşı karşıya olduğu tehlike detaylı olarak analiz edilmiş, bu tehlikeye karşı anayasal korumanın temelleri belirtilmiş ve Almanya'daki Federal Veri Koruma Yasası'nda yer alan güvencelerin anayasal gereklilikler ışığında güçlendirilmesi amaçlanmıştır[491].

Bilgilerin kaderini belirleme hakkı, özel hayatın gizliliğinin korunmasından daha geniş kapsamlı olup, bireylere, kişisel verilerinin nasıl ifşa edileceğine ve kullanılacağına dair kendilerince karar verme hakkını garanti eder[492]. Bu çerçevede anayasal korumanın gerek davranış özgürlüğünü gerekse mahremiyetin korunmasını kapsadığı ve kişiliğin tehlikeye girmesiyle başladığı ifade edilir. Koruma kapsamında bulunan verilerin doğası gereği hassas olan ve bu nedenle temel haklar tarafından korunan bilgilerle sınırlı olmadığı belirtilir. Kendi içinde çok az bilgi barındıran kişisel verilerin kullanımı bile, erişimin amacına ve mevcut işleme ve bağlantı seçeneklerine bağlı olarak, ilgili kişinin mahremiyeti ve davranış özgürlüğü üzerinde müdahaleci bir etkiye sahip olabilir[493].

Bilgilerin kaderini belirleme hakkı ile önlenmesi gereken kişiliğe yönelik tehditler, devletin ve uygulanabilir olduğu durumlarda özel aktörlerin kişisel verileri toplayabileceği, işleyebileceği ve kullanabileceği birçok yöntemden kaynaklanmaktadır[494].

Özellikle elektronik veri işleme, bu tür bilgilerden daha fazla bilgi üretmek ve böylece hem ilgili kişinin temel haklarla korunan gizlilik çıkarlarına zarar verebilecek hem de davranış özgürlüğüne müdahale edebilecek sonuçlar çıkarmak için kullanılabilir[495].

Federal Anayasa Mahkemesi aynı zamanda genel kişilik hakkından türetilen bu temel hakkın bireyin kendi verileri üzerinde tam yetkiye sahip olduğu anlamına gelmediğini, ancak devletin de bu verilere kısıtlama olmaksızın erişememesi gerektiğini ifade etmiştir. Bunun nedeni olarak, kişisel bilgilerin, sosyal topluluğa

[491] BVerfGE 65, 1 vd.
[492] BVerfG NJW 2008, 822 (826).
[493] BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03, NJW 2007, S. 2464 (2466).
[494] BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Oktober 2006 - 1 BvR 2027/02 -, JZ 2007, S. 576
495 BVerfGE 65, 1 (42); 113, 29 (45 f.); BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 -, NJW 2007, S. 2464 (2466).

dahil olmaları nedeniyle münhasıran bireyi ilgilendirmemesi, daha ziyade, bu topluluktaki diğer kişilere de tahsis edilebilen sosyal gerçekliğin bir yansımasını temsil ettiğini açıklamıştır[496]. Bu nedenle bireyler, öncelikli kamu yararı için *bilgilerin kaderini belirleme hakkı*na getirilen kısıtlamaları kabul etmelidir[497].

Federal Anayasa Mahkemesi, kendi kaderini tayin hakkının, bireylerin kişiliklerini geliştirmek için bilgi teknolojisi sistemlerinin kullanımına bağımlı olmalarından ve bunu yaparken sisteme kişisel verileri emanet etmelerinden veya kaçınılmaz olarak bunları sadece kullanarak sağlamalarından kaynaklanan kişiliğe yönelik tehditleri tam olarak karşılamadığını vurgulamaktadır. Böyle bir sisteme erişim sağlayan üçüncü kişilerin başka bir tedbire ihtiyaç duymadan geniş veri tabanlarına kolaylıkla erişim sağlayabileceğini, bunun da bilgi edinme konusunda kendi kaderini tayin etme hakkı ile korunan bireysel veri elde etmenin çok ötesine geçtiğini iler sürer[498]. Zira kendi kaderini tayin hakkı, bireylerin verilerinin nasıl ifşa edileceğine ve kullanılacağına kendilerinin karar verme hakkını güvence altına alırken[499], sadece münferit kişisel verilere erişime karşı seçici bir koruma sağlar[500]. Ancak online arama ile sistemde depolanan tüm veri tabanına erişilir. Bu durum Federal Anayasa Mahkemesi'nin görüşüne göre, kişiliğe ilişkin bir imaj yaratma olasılığı nedeniyle kişiliğe yönelik tehdidin artmasına yol açıp, kendi kaderini tayin etme hakkının sağladığı koruma düzeyini aşmaktadır.

Nitekim bilgi teknolojisi sistemlerinin karmaşıklığı nedeniyle, kullanıcı sistemi kullanırken hangi kişisel verilerin elde edildiğini fark edemez ve dolayısıyla verilerin kim veya kimler tarafından kullanıldığını da değerlendiremez. Bu durum veri sahibinin aslında kendi kaderini tayin etme hakkını kullanabilecek durumda olmadığı anlamına gelir.

(2) Bilgi Teknolojisi Sistemlerinin Gizliliğini ve Bütünlüğünü Sağlama Hakkı

Federal Anayasa Mahkemesi 2008 kararıyla kişiliğin korunması hakkından[501] hareketle, bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünü sağlama hakkını

[496] BVerfG, NJW 1984, 419 (422).
[497] BVerfG, NJW 1984, 419 (422).
[498] Urteil vom 27. Februar 2008 - 1 BvR 370/07, 200.
[499] BVerfGE 65, 1 (43).
[500] Pretz, Mona, FreiLaw 2/2016, s. 131.
[501] Kişiliğin korunması hakkı Federal Almanya Anayasasının 2/1 ve 1/1 maddeleri uyarınca düzenlenmiştir

(bilgi teknolojisi temel hakkını) geliştirmiştir[502]. Bu bilgi teknolojisi temel hakkının, bilimsel ve teknolojik ilerleme ile değişen yaşam koşullarından kaynaklanabilecek tehditlere karşı boşluk doldurucu bir işleve sahip olduğu ifade edilmektedir[503].

Anayasa mahkemesi, ağa bağlı bilgi teknolojisi sistemlerinin giderek yaygınlaşmasının bireylerin kişiliklerini geliştirmeleri için yeni fırsatların yanında yeni tehditler de yarattığını belirterek, korumanın kapsamının dijital mahremiyet olarak somutlaştırılması gerektiğini vurgulamıştır.

Federal Anayasa Mahkemesi, bilgi teknoloji temel hakkının sınırsız bir şekilde güvence altına alınmadığını gerek önleyici gerekse adli amaçla müdahalelerin meşru olabileceğini açıklamıştır. Bu doğrultuda mahkeme, tehlikenin önlenmesinin sınırlarını yüksek tutmuş ve katı koşullara bağlamıştır. Kararda, *"bir bilgi teknolojisi sistemine, sistemin kullanımının izlenebileceği ve depolama ortamının okunabileceği şekilde gizlice sızılmasına, anayasa hukuku kapsamında, ancak ağır basan önemli bir hukuki menfaate yönelik somut bir tehlike olduğuna dair gerçek belirtiler varsa izin verilebilir. Ağır basan önemli bir menfaat kişinin yaşamı, bedeni ve özgürlüğü ya da devletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu mallarıdır. Buna kamu hizmetlerinin temel parçalarının işlevselliğini güvence altına alan tedarik tesisleri de dahildir. Önemli bir tehdidin bulunmadığı durumlarda, bireylerin diğer meşru menfaatlerinin veya genel kamuoyunun korunması için burada olduğu gibi, ilgili kişinin kişiliğinin kapsamlı bir şekilde soruşturma makamı tarafından izlenmesi genel olarak ölçülü değildir"* şeklinde açıklanmıştır[504]. Bu formülasyon ile Federal Anayasa mahkemesi tehlikenin önlenmesi çerçevesinde yasal menfaatlerin önceliğine ilişkin olası kaygıları ortadan kaldırmış ve böylece online arama ile izin verilen azami sınırı tanımlamıştır. Ayrıca tehlikenin yakın gelecekte gerçekleşeceği henüz yeterli bir olasılıkla tespit edilemese dahi, belirli olguların münferit davada belirli kişiler tarafından ağır basan hukuki menfaate yönelik bir tehlikeye işaret etmesi koşuluyla, tedbirin meşru sayılabileceğine hükmedilmiştir.

Çalışmanın devamında bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün sağlanması hakkı, koruma alanı ve sınırları bakımından incelenecektir.

[502] BVerfG NJW 2008, 822 (824).
[503] BVerfG NJW 2008, 822 (824), Kudlich, JA 2008, 475 vd.
[504] BVerfG, Urteil vom 27.02.2008, Rn. 247.

(a) Koruma Alanı

Koruma kapsamı, tek başına veya teknik ağlarında, veri sahibinin kişisel verilerini, sisteme erişimin bir kişinin hayatının önemli kısımları hakkında bir fikir edinmeyi veya hatta kişiliği hakkında geniş kapsamlı bir profil elde etmeyi mümkün kılacak ölçüde ve çeşitlilikte içerebilen bilgi teknoloji sistemlerini içerir[505].

Bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün sağlanması hakkı, iki tür korumayı amaçlar[506]. Birincisi kullanıcının koruma kapsamındaki bir bilgi teknoloji sistemi tarafından üretilen, işlenen ve saklanan verilerin gizli kalmasını sağlama konusundaki menfaatinin korunmasıdır[507].

İkincisi ise bilgi teknolojisi sisteminin bütünlüğünün korunmasıdır. Bilgi teknoloji sistemine hizmetlerinin, işlevlerinin ve depolama içeriğinin üçüncü taraflarca kullanılabileceği şekilde erişilmesi halinde, sistemin bütünlüğüne müdahale edildiği kabul edilir. Zira bu durumda sistemin izlenmesi veya manipüle edilmesi için belirleyici teknik engel aşılmış olur[508].

Bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün sağlanması temel hakkının korunması, sistemdeki verilerin tamamen veya kısmen gözetlenebildiği "gizli erişimi" içerir[509]. Söz konusu verilerin çalışma belleğinde (RAM) ya da hedef sistemde geçici veya kalıcı olarak saklanıp saklanmadığı önemli değildir[510].

Ayrıca bilgi teknolojisi sistemine erişimin kolay veya ancak ciddi bir çaba ile mümkün olup olmadığına bakılmaksızın koruma sağlanmaktadır[511]. Ancak, hakkında tedbir uygulanan kişi, bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğü temel hakkının korunmasını ancak hedef sistemi "kendi sistemi olarak kullanması" ve bu nedenle tek başına veya sistemi kullanma yetkisine sahip diğer kişilerle birlikte sistem üzerinde kendi kararına sahip olduğunu varsayması halinde talep edebilir[512].

Bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün sağlanması temel hakkı bir erişim seçeneği sunulmadan önce de bu erişim seçeneğinin belirli bir veri toplama yoluyla kullanılması gerekmeksizin bilgi teknoloji sistemlerini korur. Bu bakımdan bilgi teknolojisi temel hakkı, işlevsel olarak, sadece veri toplama ve veri işlemeye karşı

[505] BVerfG, Urteil vom 27.02.2008, Rn. 203.
[506] MüKoStPO/Rückert StPO § 100b, Rn. 5.
[507] BVerfG, Urteil vom 27.02.2008, Rn. 204.
[508] BVerfG, Urteil vom 27.02.2008, Rn. 204.
[509] Hauck in Löwe/Rosenberg, §100b Rn. 17.
[510] BVerfG, Urteil vom 27.02.2008, Rn. 205.
[511] BVerfG, Urteil vom 27.02.2008, Rn. 2056; MüKoStPO/Rückert StPO § 100b, Rn. 8.
[512] BVerfG, Urteil vom 27.02.2008, Rn. 2056; MüKoStPO/Rückert StPO § 100b, Rn. 8.

koruma sağlayan bilgi edinme konusunda kendi kaderini tayin etme hakkının ötesine geçer. Online arama, teknik araçların, yani casus yazılımının kullanımı yoluyla bilgi teknoloji sistemine erişim olasılığını açarak, söz konusu bilgi teknoloji temel hakkına müdahale etmektedir[513].

(b) Sınırları

Bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü sağlama temel hakkı sınırsız değildir. Bu temel hakka müdahale edilebilir ve müdahaleler gerek önleyici gerekse adli amaçla gerekçelendirilebilir. Bireyler, temel haklarına yönelik kısıtlamaları ancak anayasal bir yasal dayanağı olması halinde kabul etmelidirler[514], zira temel hakları sınırlayan tüm devlet tedbirleri, yetkilendirme için resmi bir yasal dayanak gerektirir ("Vorbehalt des Gesetzes") [515].

Yetkilendirme temeli bazı gereklilikleri yerine getirmelidir. Bu çerçevede öncelikle açıklık ve belirlilik gerekliliğini karşılamalı ve devamında ölçülülük ilkesine uygun olmalıdır. Bu, temel haklara yönelik bir müdahalenin meşru bir amaca hizmet etmesini ve bu amaca yönelik bir araç olarak uygun, gerekli ve orantılı olmasını gerektirir. Son olarak, çekirdek alanın korunmasına ilişkin hükümlere uyulmalıdır. Ayrıca insan onurunun dokunulmazlığı ilkesine yakınlığı sebebiyle, Federal Anayasa mahkemesi bilgi teknolojisi temel hakkına yapılan müdahalelere karşı ek güvencelerin sağlanmasını şart koşmuştur[516].

i. Açıklık ve Belirlilik kriterlerine uygunluk

Öncelikle yetkilendirme temelinin açık ve belirli olması gerekir. Belirlilik şartı, demokratik olarak meşrulaştırılmış parlamenter yasama organının, temel haklara yönelik müdahaleler ve bunların kapsamı konusunda temel kararları kendisinin vermesini, hükümet ve idarenin yasada eylem için yol gösterici ve sınırlayıcı ölçütler bulmasını ve mahkemelerin hukuki denetim yapabilmesini sağlamayı amaçlamaktadır[517].

Ayrıca, normun açıklığı ve belirliliği, ilgili kişinin hukuki durumu fark edebilmesini ve olası sıkı tedbirlere hazırlıklı olmasını sağlar[518]. Yasa koyucu, müdahalenin nedenini, amacını ve sınırlarını yeterince spesifik, kesin ve normatif bir

[513] MüKoStPO/Rückert StPO § 100b, Rn. 6.
[514] BVerfG, Urteil vom 27.02.2008, Rn. 207; Hauck in Löwe/Rosenberg, §100b Rn. 19.
[515] Pretz, Freilaw 2/2016, S. 132.
[516] Bantlin, JuS 2019, s. 772.
[517] BVerfG, Urteil vom 27.02.2008, Rn. 209.
[518] BVerfGE 110, 33 (52 vd.); BVerfGE113, 348 (375 vd.).

şekilde tanımlamalıdır[519]. Dolayısıyla vatandaşların davranışlarını [520]yönlendirebilmeleri için nelere hazırlıklı olmaları gerektiği açık olmalıdır.

Online arama bakımından hangi somut biçimlerinin temel haklara müdahale teşkil ettiğini ve bunların hangi koşullarda mümkün olabileceğini kanun koyucu müdahalenin ciddiyeti ve yeniliğini göz önünde bulundurarak düzenlemelidir. Ancak burada kanun koyucu "*bu tür tedbirler bir müdahale teşkil ettiği veya nitelikleri ve ciddiyetleri bakımından böyle bir müdahaleye eşdeğer olduğu ölçüde*" ifadesiyle genel formülasyonlar kullanmıştır[521]. Federal Anayasa mahkemesi bu nedenle açıklık ve belirlilik ilkelerine uyulmadığını ifade etmiştir.

ii. Ölçülülük ilkesine uygunluk

Yetkilendirme temeli ölçülük ilkesine de uygun olmalıdır. Bu çerçevede, gerçekleşen müdahalenin meşru bir amaca hizmet etmesi ve bu amaca yönelik bir araç olarak uygun, gerekli ve orantılı olması gerekir[522].

Barış ve düzen için anayasal bir güç olarak devletin güvenliği ve halkın yaşam, beden ve özgürlüğüne yönelik tehditlere karşı güvenliği, diğer üstün değerlerle eşit derecede anayasal değerlerdir[523]. Elektronik veya dijital iletişim araçlarının kullanımının artması ve bunların hayatın neredeyse tüm alanlarına nüfuz etmesi, Anayasa Koruma Teşkilatının görevlerini etkin bir şekilde ifa etmesini imkânsız hale getirmektedir. Zira modern bilişim teknolojisi aynı zamanda aşırılık yanlısı ve terörist örgütlere temas kurmak ve sürdürmek, suç eylemlerini planlamak, hazırlamak ve gerçekleştirmek için çok sayıda fırsat sunmaktadır[524].

Anayasayı Koruma Yasası ile getirilen yetkilendirme temeli ile anayasayı koruma teşkilatının, özellikle internet iletişimiyle bağlantılı olanlar olmak üzere yeni tehditler karşısında terörizmle etkin bir şekilde mücadele etmesini sağlama amacı[525] meşru bir amaçtır[526].

Aynı zamanda bilgi teknoloji sistemlerine gizli erişim sağlayan yetkilendirme temeli terörizmle etkin bir şekilde mücadele etme amacına uygundur. Zira bu

[519] BVerfGE 100, 313 (359 f.), (372); BVerfGE 110, 33 (53); BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 , NJW 2007, S. 2464 (2466).
[520] Bantlin, JuS 2019, s. 772.
[521] BVerfG, Urteil vom 27.02.2008, Rn. 213 vd.
[522] Epping, Grundrechte, 7. Auflage 2017, Rn. 48 vd.
[523] BVerfGE 49, 24 (56f.); BVerfGE 115, 320 (346).
[524] Hauck in Löwe-Rosenberg, §100b, Rn. 26.
[525] NRW-LT-Drucksache 14/2211, 1.
[526] BVerfG, Urteil vom 27.02.2008, Rn. 219.

yetkilendirme temeliyle tehdit durumlarını açıklığa kavuşturmak için Anayasa Koruma teşkilatının olanakları genişletilmiştir[527]. Yasa koyucu uygunluğu değerlendirirken ciddi bir hareket alanına sahiptir ve burada bu alanın aşıldığı tespit edilmemiştir[528].

Bununla birlikte bilgi teknolojisi sistemlerine gizli erişim, yetkilendirme temelinin meşru amacına ulaşması bakımından da gereklidir. Kanun koyucu, takdir yetkisi kapsamında, bu tür sistemlerde mevcut olan verileri elde etmek için eşit derecede etkili ancak daha az müdahaleci bir yol olmadığını varsayma hakkına sahiptir[529]. Kural olarak, Anayasa Koruma Yasasında öngörülmeyen hedef sistemin açık bir şekilde aranması, gizli erişimden daha hafif bir araç olarak kabul edilir[530]. Bununla birlikte, anayasayı koruma teşkilatı, görevi kapsamında bir bilgi teknolojisi sisteminin depolama ortamında saklanan dosyaları, şifrelenmiş veriler de dahil olmak üzere incelemek, uzun bir süre boyunca değişiklikleri izlemek veya sistemin kullanımını kapsamlı bir şekilde izlemek için yeterli nedene sahipse, bu istihbarat hedeflerine ulaşmak için daha hafif bir yol görünmemektedir[531].

Ancak Federal Anayasa Mahkemesi ölçülülük şartının yerine getirilmediğine hükmetmiştir. Ölçülülük ilkesi, müdahalenin ağırlığının, genel bir değerlendirmede müdahaleyi haklı kılan nedenlerin ağırlığıyla orantısız olmamasını gerektirir[532]. Bu çerçevede yasa koyucu, temel haklara yapılan bir müdahale ile kısıtlanan bireysel menfaati, müdahalenin hizmet ettiği genel menfaatlere makul bir şekilde tahsis etmelidir[533]. Online arama, tedbire maruz kalan kişinin tüm veri tabanına erişmeyi mümkün kıldığı için ciddi bir müdahale teşkil etmektedir. Bu verilere dayanarak, davranış ve iletişim profillerinin oluşturulması da dahil olmak üzere, ilgili kişinin kişiliği hakkında geniş kapsamlı sonuçlar çıkarılabilir[534]. Özellikle uzun süreli izlemenin de mümkün olduğu ifade edilmelidir.

Federal Anayasa Mahkemesi'nin kararına göre, online arama yoluyla ciddi bir müdahalenin, ancak yetki temelinin müdahaleyi somut olayda ağır basan önemli bir hukuki menfaate yönelik yakın bir tehlikeye işaret eden belirli olgulara bağlı kılması

[527] BVerfGE 77, 84 (106); BVerfGE 90, 145 (173).
[528] BVerfG, Urteil vom 27.02.2008, Rn. 221.
[529] BVerfG, Urteil vom 27.02.2008, Rn. 224.
[530] Hornung, DuD 2007, 575 (580).
[531] BVerfG, Urteil vom 27.02.2008, Rn. 225.
[532] BVErfGE 90, 145 (173); BVerfGE 109, 279 (349 vd.).
[533] BVerfG, Urteil vom 27.02.2008, Rn. 227.
[534] BVerfG, Urteil vom 27.02.2008, Rn. 237.

halinde uygundur. Ağır basan önemli bir menfaat kişinin hayatı, vücut bütünlüğü ve özgürlüğüdür. Ayrıca kamu menfaatleri de eğer bunların tehdit altında olması devletin temelleri veya varlığını ya da insanların varlığının temellerini etkiliyorsa ağır basan önemli menfaat olarak kabul edilir[535].

Gerçeğe dayalı belirtilerin gerekliliği, varsayımların veya genel deneyimin tek başına erişimi haklı çıkarmak için yeterli olmadığı anlamına geldiği, bunun yerine, bir risk öngörüsünü destekleyen belirli olguların ortaya konması gerektiği ifade edilir[536]. Bu öngörünün, belirli bir tehlikenin ortaya çıkmasıyla ilgili olması gerektiği belirtilir[537]. Belirli olguların, somut olayda ağır basan bir hukuki menfaate yönelik yakın bir tehlikeye işaret etmesi halinde, tehlikenin yakın gelecekte gerçekleşmesi henüz yeterince muhtemel olmasa dahi, bilgi teknolojisi sistemine erişim haklı görülebilir. Bir yandan, olgular, olayın en azından somut nitelikte olduğu ve zaman içinde öngörülebilir olduğu sonucuna varılmasına izin vermelidir. Diğer yandan olgular, izleme tedbirinin büyük ölçüde belirli kişilerle sınırlandırılabilmesi için kimlikleri hakkında en azından yeterince bilgi sahibi olunan belirli kişilerin olaya dahil olacağı sonucuna varılmasına olanak tanımalıdır[538].

Ayrıca, temel haklara ciddi bir müdahale oluşturması sebebiyle bilgi teknolojisi sistemine gizli erişim yetkisi, tedbire maruz kalan kişinin menfaatlerinin koruması amacıyla uygun usulî tedbirlerle desteklenip güvence altına alınmalıdır[539]. Bu çerçevede bağımsız bir organ tarafından önleyici bir denetim yapılmasının anayasal bir gereklilik olduğu vurgulanmaktadır. Zira aksi takdirde, tedbire maruz kalan kişi korumasız kalacaktır. Bununla birlikte, yasa koyucuya, örneğin denetim organına ve kullanılacak prosedüre karar verme konusunda genellikle takdir yetkisi tanınmaktadır. Ancak bilgi teknoloji sistemine gizli erişim gibi temel haklara özellikle ciddi bir müdahale söz konusu olduğu hallerde, kapsam, tedbirin her zaman bir mahkeme kararına tabi olması gerektiği ölçüde daraltılır[540].

Anayasa koruma yasasının ilgili hükümlerine göre, istihbarat servisi kaynaklarının anayasayı koruma teşkilatı tarafından kullanılmasının tek ön koşulu, anayasaya aykırı girişimler hakkında bu yolla bilgi edinilebileceği varsayımına

[535] BVerfG, Urteil vom 27.02.2008, Rn. 247 vd.
[536] BVerfGE 110, 33 (61); BVerfGE 113, 348 (378); Gusy, Christoph, Gefahraufklaerung zum Schutz der öffentlichen Sicherheit und Ordnung, JA, 2011, s. 647.
[537] BVerfG, Urteil vom 27.02.2008, Rn. 249 vd.
[538] BVerfG, Urteil vom 27.02.2008, Rn. 251.
[539] BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 -, NJW 2007, S. 2464 (2471).
[540] BVerfG, Urteil vom 27.02.2008, Rn. 259.

yönelik olgusal göstergelerdir. Federal Anayasa Mahkemesi için bu hem saldırının fiili koşulları hem de korunması gereken yasal menfaatlerin ağırlığı açısından, müdahale için yeterli bir maddi eşik değildir. Bununla birlikte Federal Anayasa mahkemesi, bağımsız bir organ tarafından önceden inceleme yapılmasına ilişkin bir hükmün de bulunmadığını ileri sürer[541].

Ayrıca Federal Anayasa Mahkemesi, insan onurunun dokunulmazlığı ilkesinden kaynaklanan özel hayatın mutlak koruma altındaki çekirdek alanına[542] müdahaleyi önlemek için yeterli yasal önlemlerin alınmadığını da ifade eder. Özel yaşamın çekirdek alanında kişiliğin gelişimi, duygu ve hisler gibi içsel süreçlerin yanı sıra son derece kişisel nitelikteki düşünce, görüş ve deneyimlerin devlet yetkililerinin bunu izleyeceği korkusu olmaksızın ifade edilmesi olasılığını içerir[543]. Bir bilgi teknolojisi sistemine gizli erişim bağlamında, harekete geçen soruşturma yetkililerin çekirdek alana dahil edilebilecek kişisel verileri elde etme riski bulunmaktadır. Örneğin, tedbire maruz kalan kişi sistemi günlük veya özel film veya ses belgeleri gibi son derece kişisel içerikli dosyalar oluşturmak ve saklamak için kullanabilir[544]. Ancak bu kişisel verilerin mutlak korunması söz konusudur. Bu nedenle çekirdek alanın korunması için düzenlemeler getirilmeli ve bunlar çekirdek alanla ilgili verilerin toplanmasını engellemelidir[545].

Hakkında tedbir uygulanan kişinin bilgi teknoloji sistemine gizli bir şekilde erişim sağlanacaksa, bu durum özel hayatın çekirdek alanını korumak bakımından özel yasal önlemlerin alınması gerektiği anlamına gelir[546]. Zira erişimin gizli olması nedeniyle, soruşturmaya konu olan kişinin, soruşturma tedbiri öncesinde veya sırasında, soruşturmayı yürüten yetkililerin kendi özel hayatının çekirdek alanına saygı göstermesini sağlama imkanı bulunmamaktadır. Kontrolün tamamen kaybedildiği bu durum, uygun usulî önlemler yoluyla çekirdek alanın ihlal edilmesi riskine karşı koruma sağlayan özel düzenlemelerle karşılanmalıdır[547].

Özel hayatın çekirdek alanını etkileyebilecek bir gözetim tedbiri için yasal izin, mümkün olduğunca çekirdek alanla ilgili verilerin toplanmamasını sağlamalıdır. Bir bilgi teknolojisi sistemine gizli erişim durumunda olduğu gibi, bilginin çekirdek alanla

[541] BVerfG, Urteil vom 27.02.2008, Rn. 264.
[542] BVerfGE 6, 32 (41), BVerfGE 27, 1 (6); BVerfGE 32, 373 (378).
[543] BVerfGE 109, 279 (314).
[544] BVerfG, Urteil vom 27.02.2008, Rn. 272.
[545] MüKoStPO/Rückert §100b, Rn. 11.
[546] BVerfG, Urteil vom 27.02.2008, Rn. 273.
[547] BVerfG, Urteil vom 27.02.2008, Rn. 275.

ilgisini değerlendirmeden önce elde edilmesi kaçınılmazsa, değerlendirme aşamasında uygun koruma sağlanmalıdır. Özellikle, çekirdek alanla ilgili bulunan ve toplanan her türlü veri derhal silinmeli ve kullanımı engellenmelidir[548].

Ancak Federal Anayasa Mahkemesi Anayasa Koruma Yasasının ilgili düzenlemelerinin çekirdek alanının korunmasına yönelik şartların da karşılanmadığını vurgular[549]. Bu nedenlerle Federal Anayasa mahkemesi Anayasa koruma yasasının söz konusu düzenlemelerini ölçülülük ilkesine ve özel hayatın mutlak koruma altındaki çekirdek alanına aykırı olarak değerlendirip, bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün garanti altına alınması hakkına ciddi bir müdahale teşkil ettiğini kabul ederek, ilgili düzenlemelerin hükümsüzlüğüne karar vermiştir.

Federal Anayasa Mahkemesi'nin kararı önleyici alana ilişkin bir düzenleme hakkında verilmiş olsa da bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün garanti altına alınması hakkının adli amaçla da geçerli olması için evrensel geçerliliğe sahip olduğu kabul edilir[550]. Yeni geliştirilen ve temel hak olarak kabul edilen bu bilgi teknolojisi hakkına müdahalenin adli amaçlar için meşru olabileceği, ancak potansiyel müdahalenin ciddiyetinin müdahale için normatif olarak açık ve spesifik temeller gerektirdiği vurgulanmıştır[551].

Federal Anayasa Mahkemesinin dönüm noktası niteliğindeki 2008 tarihli kararı ile yasa koyucuya bilgi teknolojisi sistemlerine müdahaleler için anayasal çerçevenin sağlanmış olduğunu ve *"kişiliğin korunması hakkını*[552]*"* buna göre tanımlamış olduğunu görmekteyiz. Dolayısıyla bu karar ile yasal bir yetkilendirme temelinin ve online aramanın kodifiye edilmesinin önünün açıldığını ifade edebiliriz.

Son olarak belirtilmelidir ki Federal Anayasa Mahkemesi'nin kararı gerek davacılar gerekse davalılar tarafından övgüyle karşılanmıştır. Birçok kişi kararın gözetim devletinin daha da genişlemesinin reddi olarak değerlendirilmesi gerektiğini vurgulamıştır[553]. Bununla birlikte bilgi teknolojisi sistemlerinin bütünlüğünün ve gizliliğinin sağlanmasına yönelik yeni temel hakkın tesis edilmesi de modern bilgi

[548] BVerfGE 109, 279 (318); BVErfGE 113, 348 (391 f.).
[549] BVerfG, Urteil vom 27.02.2008, Rn. 284.
[550] BVerfG NJW 2008, 822 (827);
Bode, Verdeckte strafprozessuale Ermittlungsmassnahmen, 2012, s. 99.
[551] Sieber/Brodowski, Handbuch- Multimedia-Recht, 58. EL, Maerz 2022, Strafprozessrecht, VI. Online-Durchsuchung, Rn.155.
[552] Allgemeines Persönlichkeitsrecht nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.
[553] Eski içişleri bakanı Gerhart Baum'un röportajı için bkz. Onlinedurchsuchung:"Ein Stück Rechtsgeschichte" | ZEIT ONLINE, Erişim tarihi: 01.06.2024:

teknolojisinin kişiliğe yönelik yeni tehdit türlerini ele alması bakımından olumlu bir şekilde karşılanmıştır[554].

Kararla ilgili dikkat çekici husus bilgi teknolojisi sistemlerinin korunmasının güvence altına alınmasıyla birlikte, sistemdeki verilerin korunmasının yanı sıra sistemin kendisinin de korunmasıdır. Burada odak noktası izinsiz giriş yapan kişinin fiili faaliyeti değil, izinsiz girişin neden olduğu kontrol kaybıdır. Sistemin bütünlüğünün kasıtlı ve gizli bir şekilde ihlal edilmesi aynı zamanda kişinin bütünlüğünün de ihlal edilmesi anlamına gelmektedir. Sonuç olarak, kişinin korunması, özerkliği, özgürlüğü ve onuru gibi temel değerler ihlal edilmiş olur.

Bu nedenle Federal Anayasa Mahkemesinin kararını bizde olumlu değerlendirmekteyiz. Zira Federal Anayasa Mahkemesi, devletin bilgi teknolojisi sistemlerine gizli müdahalesinin ciddiyetini vurgulamakta ve bu tür sistemlerin yoğun kullanımı ve buna bağlı olarak hassas kişisel verilerin çokluğu, Federal Anayasa Mahkemesi'ni özel hayatın korunmasını temel haklar çerçevesinde farklılaştırmaya sevk etmektedir.

F. 27.05.2008 tarihli Federal Kriminal Polis Dairesi Uluslararası Terörizm Tehlikelerine Karşı Savunma Kanunu

27 Mayıs 2008 tarihinde Federal Meclis, Federal Kriminal Polis Dairesi'nin uluslararası terörizm tehlikelerine karşı savunma yapmasını öngören yasayı kabul ederek, Federal Anayasa Mahkemesi'nin belirlediği şartlara uygun olarak, bilgi teknolojisi sistemlerine gizli müdahale de dahil olmak üzere, ilk kez önleyici yetkiler vermiştir[555].

Uluslararası terörizm tehlikelerine karşı Federal Kriminal Dairesi Kanunu'nun 20k maddesi[556] uyarınca alınan tedbir, henüz telekomünikasyonun konusu olmayan, telekomünikasyonun konusu olmaktan çıkan ya da telekomünikasyona yönelik olmayan verilerin elde edilmesini amaçlamaktadır[557].

---

[554] Schramm, Marc / Jansen, Kathrin, Die Online-Durchsuchung im Lichte der Rechtsprechung, s. 7, Erişim: https://www.uni-muenster.de/Jura.tkr/oer/wp-content/uploads/2010/06/Jur.Info_Nr1-2008-Online-Durchsuchung_im_Lichte_der_Rspr.pdf, Erişim tarihi: 01.06.2024.
[555] BT-Drucksache 16/9588.
[556] Federal Kriminal Dairesi Kanunu'nun (BKAG) 20k maddesi artık yürürlükte olmayıp, yerine BKAG 49 düzenlenmiştir.
[557] BT-Drucksache 16/9588.

G. 20.04.2016 Tarihli Federal Almanya Anayasa Mahkemesinin Federal Kriminal Dairesi Kanunu'nun (BKA-Gesetz) Yasallığına İlişkin Kararı

20 Nisan 2016 tarihinde Federal Anayasa Mahkemesi Federal Kriminal Dairesi Kanunu'nun yasallığına ilişkin kararını açıklamıştır[558].

Kararın esaslarında, "*Federal Kriminal Dairesi'ne, uluslararası terörizm tehdidini önlemek amacıyla gizli izleme tedbirleri (konut izlemesi, online arama, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, telekomünikasyon trafiği veri toplanması ve özel veri toplanması araçlarıyla konut dışında izleme) uygulama yetkisi verilmesinin, ilke olarak Anayasa'nın temel haklarıyla uyumlu olduğu"* belirtilmiştir[559].

Federal Kriminal Dairesi Kanunu'nun 20k maddesi uyarınca, Federal Kriminal Dairesi, veri sahibi tarafından kullanılan bilgi teknolojisi sistemlerine müdahale etmek için teknik araçlar kullanabilir ve veri sahibinin bilgisi olmadan bu sistemlerden veri elde edebilir ve böylelikle davranışların takibini mümkün kılar[560].

Federal Anayasa Mahkemesi, Federal Kriminal Dairesi Kanunun 20k maddesinin bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü güvence altına alma temel hakkına müdahale teşkil ettiğini ve bu müdahalenin anayasal gerekliliklere uygun bir şekilde gerçekleştiğini tespit etmiştir[561]. Bu doğrultuda bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü güvence altına alma temel hakkının, verilere gizli erişime ve özellikle bilgisayarları ve diğer bilgi teknolojisi sistemlerini manipüle etmek ve okumak için kullanılan online aramaya karşı koruma sağladığını, ayrıca meşru bir gizlilik beklentisiyle harici sunucularda saklanan kişisel verileri de koruduğunu ifade etmektedir[562]. Federal Anayasa Mahkemesi, bu verilerin özellikle bağlantılarından kaynaklanan son derece kişisel doğası nedeniyle, bu temel hakka müdahalenin ağır olarak değerlendirildiğini, ağırlığı bakımından konutun dokunulmazlığı temel hakkına karşı yapılan müdahale ile karşılaştırılabileceğini belirtmektedir[563].

---

[558] BVerfG NJW 2016, 1781 vd.; BVerfG, 20.04.2016 – 1 BvR 969/09.
[559] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09.
[560] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 209; Kruse/Grzesiek, s. 343.
[561] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 211.
[562] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 210.
[563] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 210.

Ancak, bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü garanti altına alma hakkına yönelik müdahaleler katı koşullara tabidir[564]. Federal Anayasa Mahkemesi'nin 2008 yılında aldığı karar doğrultusunda, Federal Anayasa mahkemesi somut olayda ağır basan bir hukuki menfaate yönelik belirli bir tehdidin olgusal göstergelerine ilişkin sıkı şartların arandığının, Federal Kriminal Dairesi Kanunun 20k maddesinin ise bu gerekliliği de karşıladığının belirtilmektedir[565].

Buna göre, bir kişinin hayatı, bedeni veya özgürlüğüne ya da devletin temellerini veya varlığını veya insanların varlığının temellerini etkileyen bu tür kamu mallarına yönelik bir tehlikenin varlığı aranmaktadır. 20k maddesinin birinci fıkrası gereği, Federal Kriminal Dairesi ilgili kişinin bilgisi olmadan bir kişinin yaşamı, bedeni ve özgürlüğüne ya da devletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu mallarına yönelik tehlike bulunduğuna dair somut olguların var olması halinde, bilgi teknolojisi sistemlerine teknik araçlarla müdahale edilip, sistemden verilere erişilebilir. Ayrıca belirli olguların öngörülebilir bir zaman diliminde, en azından somutlaştırılmış bir şekilde öngörülebilir bir süre içinde bu belirtilmiş olan hukuki değerlere zarar verilebilmesi halinde ve bir kişinin bireysel davranışının belirtilmiş olan hukuki değerlere somut olarak zarar verebilme olasılığının bulunması halinde tedbire başvurulabilir. 2008 tarihli Anayasa mahkemesinin somut olayda ağır basan bir hukuki menfaate yönelik belirli bir tehdidin olgusal göstergelerine ilişkin sıkı şartlarının 20k maddesi tarafından uyumlu bir şekilde uygulandığını ifade edebiliriz[566].

Bunun ötesinde, Anayasa Mahkemesi gizli erişime izin veren tedbirlerin ölçülük ilkesini dikkate alarak uygulanmasının, *"özel hayatın derinliklerine uzanan yetkilerin, yeterince önemli yasal menfaatlerin korunması veya savunulmasıyla bağlantılı olması gerektiğini"* vurgulamıştır. Bu bağlamda Federal Anayasa Mahkemesi, gizli erişim nedeniyle bilişim sisteminde meydana gelen değişikliklerin üçüncü şahıslar tarafından kullanılmasının önlenmesi ve tedbir sona erdikten sonra mümkün olduğunca değişiklikleri geri döndürmek amacıyla en aza indirilmesi gerektiğini belirtmiş, 20k maddesinin bu gerekliliklerini yerine getirmesi sebebiyle

[564] BVerfGE 120, 274 (322 vd., 326 vd.).
[565] Kruse/Grzesiek, s. 344; BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 212.
[566] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 213.

anayasaya uygun olduğunu ve genel olarak ölçülülük ilkesine de uygun olduğunu kabul etmiştir[567].

Ancak Federal Anayasa Mahkemesi 20k maddesinin özel hayatın çekirdek alanını korunmak için yeterli olmadığı ve bu nedenle anayasaya aykırı olduğuna hükmetmiştir. Bu çerçevede Federal Anayasa mahkemesi, bilgi teknolojisi sistemlerine gizli erişimin tipik olarak son derece gizli verilerin elde edilmesi riskini beraberinde getirdiğinden ve bu nedenle özellikle özel hayatın çekirdek alana yakın olduğundan, bu özel alanın korunması bakımından yasal önlemlerin alınması gerektiğini vurgulamaktadır[568].

Federal Anayasa mahkemesi özel hayatın çekirdek alanının korunması bakımından "iki aşamalı koruma mekanizması" geliştirmiş olup, yasa koyucuyu özel hayatın çekirdek alanını koruyacak düzenlemeleri bu doğrultuda tasarlamakla yükümlü kılmıştır[569].

Bunun sonucunda ilk aşamada, özel yaşamın çekirdek alanının etkilenebileceğine dair somut göstergelerin bulunması halinde, yasa koyucu çekirdek alanla ilgili verilerin elde edilmemesini sağlamaya çalışmalıdır. Bu bağlamda özellikle bilgi teknolojisi güvenlik önlemleri kullanılmalıdır.[570]

Çekirdek alana ilişkin verilerin veri toplama öncesinde veya sırasında ayrıştırılamaması halinde, yüksek düzeyde kişisel verilerin bu süreçte elde edilmesi ihtimalinin bulunması halinde, bilgi teknolojisi sistemine erişime izin verilir. Bu durumda ikinci aşamanın önemi vurgulanır. Zira ikinci aşamada, değerlendirme ve kullanım aşamasındaki güvenceler vasıtasıyla veri sahiplerinin koruma ihtiyaçlarının dikkate alınması ve bu tür bir erişimin etkilerinin en aza indirilmeye çalışılması gerektiği belirtilir[571]. Federal Kriminal Dairesi tarafından erişilmeden ve kullanılmadan önce temel alanla ilgili bilgileri filtreleyen bağımsız bir organ tarafından yapılan bir denetim burada belirleyici bir öneme sahiptir[572]. Dolayısıyla bağımsız bir organ tarafından yapılacak bir incelemeyle, çekirdek alanla ilgili bilgilerin ifşa edilmemesi amaçlanmaktadır.

[567] BVerfG NJW 2016, 1781 ff; BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 215.
[568] BVerfGE 120, 274 (335 vd.).
[569] BVerfG NJW 2008, 822 (834).
[570] BVerfGE 120, 274 (338).
[571] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 220.
[572] BVerfGE 120, 274 (338 f.).

Federal Anayasa Mahkemesi 20 k maddesinin bu gereklilikleri yalnızca kısmen karşıladığını belirtmiştir. Bu çerçevede veri elde etme aşamasının anayasa uygun şekilde düzenlenmiş olduğu, özel hayatın çekirdek alanıyla ilgili bilgilerin elde edilmesinden kaçınmak için teknik imkanların kullanıldığı ifade edebiliriz. Özellikle bilişim sisteminde meydana gelen değişikliklerin üçüncü şahıslar tarafından kullanılmasının önlenmesi ve tedbir sona erdikten sonra mümkün olduğunca değişiklikleri geri döndürmek amacıyla en aza indirilmesi için güvenceler sağlanmıştır[573].

Ancak ikinci aşama bakımından, çekirdek alanın korunmasının yeterli önlemlerden yoksun olduğu ileri sürülmektedir[574]. Burada bağımsız bir organ tarafından yapılması gereken denetimin 20 k uyarınca Federal Kriminal Dairesi bünyesinde çalışan bir veri koruma yetkilisi ile iki Federal Kriminal Dairesi yetkilisi tarafından yapılması düzenlenmiştir[575]. Fakat bağımsız bir organ tarafından yapılan taramanın temel amacının, çekirdek alanla ilgili verilerin mümkünse güvenlik makamlarına ifşa edilmeyecek kadar erken bir aşamada filtrelenmesi olduğu ifade edilmektedir. Bu denetimin esasen güvenlikle ilgili görevlerle görevlendirilmemiş harici kişiler tarafından yapılması gerektiği, Federal Kriminal Dairesi yetkililerinin katılımının mümkün olabileceği, ancak denetimle ilgili asıl uygulama ve karar verme sorumluluğun Federal Kriminal Dairesinden bağımsız yetkililerin elinde olması gerektiği vurgulanmaktadır[576].

Ayrıca verilerin silindiğine dair tutanakların saklanması için öngörülen sürenin de çok kısa olmasının anayasaya aykırılık teşkil ettiği belirtilmektedir[577]. Zira bu durumda tedbire maruz kalan kişinin verilerin kullanımına ilişkin denetiminin imkânsız hale getirilmesi eleştirilmektedir[578].

Sonuç olarak Federal Anayasa Mahkemesi, Federal Kriminal Dairesi Kanunu'nun 20 k maddesinin özel hayatın çekirdek alanını yeterli düzeyde korumaması ve verilerin silinmesini raporlayan tutanakların yeterli süre saklanmaması sebebiyle anayasaya aykırı olduğuna hükmetmiştir.

[573] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 222.
[574] Baum/Schantz, ZRP 2008, 137 (138).
[575] Roggan, NJW 2009, 257 (261).
[576] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 224.
[577] BVerfG Urteil v. 20.04.2016 – 1 BvR 966/09, Rn. 226.
[578] Baum/Scantz, ZRP 2008, 137 (138).

Bu karar çerçevesinde Federal Anayasa Mahkemesi, Federal Kriminal Dairesi Kanununun uyumsuz ilan edilen hükümlerinin 30 Haziran 2018 tarihine kadar ya da buna uygun yeni bir düzenleme yapılana kadar geçerli olacağına dair bir süre belirlemiştir. Bunun üzerine "Genel Veri Koruma Yönetmeliğine" ve yeni" Federal Veri Koruma Kanunu'na" uyum sağlamak amacıyla yapılan değişikliklere ek olarak, bilgi teknolojisi sistemlerine gizli erişim de tekrar düzenlenmiştir. Federal Kriminal Dairesi Kanununda yapılan bu kapsamlı düzenlemeler 1 Temmuz 2017 yılında yürürlüğe girmiştir[579].

H. Bavyera eyaleti adli amaçlı online arama yasa tasarısı

Bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü garanti etme temel hakkının Federal Anayasa Mahkemesi tarafından kişiliğin korunması hakkının yansıması olarak geliştirilmesi üzerine Bavyera eyaleti ilk kez adli amaçlı online arama tedbirinin uygulanması için bir yasa taslağı hazırlamıştır[580]. Bu doğrultuda 27 Mayıs 2008 tarihinde bilgi teknolojisi sistemlerine gizli erişimi meşrulaştırmayı amaçlayan Ceza Muhakemeleri Usulü Kanunu'nda değişiklik öngören bir yasa tasarısı Federal Konsey'e sunulmuştur.

Yasanın gerekçesinde, soruşturma makamlarının çalışmalarının artarak yeni teknolojiler tarafından belirlendiği ve internetin, teknolojilerin minyatür haline gelmesinin, bellek hacminin ve bilgi işleme ile bilgi yayma hızının sınırsız bir şekilde artmasının suç failleri tarafından kullanıldığı vurgulanmaktadır[581].

Taslak öncelikle komplocu suç şebekeleriyle, özellikle de İslamcı aşırıcılıkla, çocukların cinsel istismarı ve çocuk pornografisi dağıtımıyla mücadeleyi amaçlıyor. Zamanının Bavyera İçişleri Bakanının, önerilen yasa tasarısı hakkında, "teröristler en son iletişim teknolojilerini kullanırken, Anayasa Koruma Dairesi on yıl öncesinin teknolojik seviyesinde kalamaz, terör tehlikelerinin ve buna bağlı tehditlerin incelenmesi ve masum insanların hayatlarının ve sağlıklarının korunması gereklidir[582]" sözlerini kullanmıştır. Bu çerçevede öncelikli amaç, soruşturmaları tehlikeye atmadan failleri ve suç yapılarını ortaya çıkarmaktır[583].

[579] 01.07.2017 tarihli BKA-Gesetz:
[580] BRat-Drucksache 365/08.
[581] BRat-Drucksache 365/08, s.5.
[582] Bayerischer Gesetzesentwurf zur Online-Durchsuchung - Golem.de, Erişim tarihi: 01.06.2024:
[583] BRat-Drucksache 365/08, s.5.

Eyalet yasama organı, tehlikenin önlenmesi bağlamında yüksek müdahale gerekliliklerini dikkate almak suretiyle, online arama yapmak için kendi suç kataloğunu oluşturmuştur. Federal Anayasa mahkemesi 27 Şubat 2008 tarihli kararında, önleyici alanda temel haklara müdahale yapılabilmesi için yüksek eşiklerin söz konusu olduğunu, suç kataloğun belirtilen yasal menfaatlerle ilgili olması ve dar bir şekilde tanımlanması gerektiğini belirtmiştir. Ancak bu katı koşullara rağmen yasa tasarısının Federal Anayasa mahkemesinin öngördüğü suçlar dışında da kataloğa suçlar eklediğinde görmekteyiz.[584]

Ayrıca, bilgi teknoloji sistemlerine erişim verilerinin elde edilmesi veya depolanan verilere erişilmesinden farklı olarak, bilgi teknoloji sistemlerini tanımlamak ve konumlarını belirlemek üzere teknik araçlar kullanma yetkisi getirilmiştir. Bu hükmün, özel tanımlayıcıları ve konumları soruşturma makamları tarafından bilinmeyen bilgi teknolojisi sistemlerinin ağır suçların işlenmesinde giderek daha fazla kullanılması sebebiyle bilgi teknolojisi alanındaki gelişmeler ışığında gerekli olduğu ifade edilmiştir[585].

Bunun ötesinde hedef sistemi kullanmak veya donanım ve yazılım bileşenlerinin kurulumu için gizlice arama yapmak amacıyla konuta girilmesi gibi geniş kapsamlı "ilave tedbirlerin" de yetki temeli kapsamına alınması istenmiştir[586].

Sonuç olarak, hukuk ve içişleri komisyonlarının tavsiyelerinin aksine, Federal Konsey 4 Temmuz 2008'de adli amaçlı online aramaya yönelik yasa tasarısını Federal Meclise sunmama kararı almıştır[587]. Oturumun ilgili tutanağında herhangi bir gerekçenin belirtilmediğini görmekteyiz.

I. Adli amaçlı online arama tedbirinin federal düzeydeki yasama süreci

22 Şubat 2017 tarihinde federal hükümet "Ceza Muhakemesinin Daha Etkin ve Uygulanabilir Düzenlenmesi Hakkında Kanun"[588] ve "Alman Ceza Kanunu, Genç Mahkemeleri Kanunu, Ceza Muhakemeleri Usulü Kanunu ve diğer kanunlarda

[584] BRat-Drucksache 365/08, s.10.
[585] BRat-Drucksache 365/08, s.12.
[586] BRat-Drucksache 365/08, s.14.
[587] Bundesrat – 846. Sitzung – 4. Juli 2008, Plenarprotokoll846 (bundestag.de) s. 209, Erişim tarihi: 01.06.2024:
[588] BTag-Drucksache 18/11277.

değişiklik yapmak üzere Federal Meclis'e iki yasa tasarısı sunmuştur[589]. Ancak her iki yasa tasarısı da online arama ile ilgili herhangi bir düzenleme içermemekteydi.

9 Mart 2017 tarihinde Federal Meclis her iki tasarıya ilişkin ilk müzakeresini gerçekleştirmiş ve tasarıları komisyonlara havale etmiştir[590].

15 Mayıs 2017 tarihinde Alman hükümeti CDU, CSU ve SPD parlamento grupları tarafından hazırlanan bir "değişiklik önerisi taslağı" sunmuş[591], 20 Haziran 2017 tarihinde bu taslak "Hukuk İşleri ve Tüketiciyi Koruma Komisyonu" aracılığıyla tasarıya dahil edilmiştir[592]. Söz konusu değişiklik önerisi taslağı, kaynak telekomünikasyon denetiminin ve online aramanın eklenmesini içermektedir. Online arama bakımından tamamen yeniden tasarlanmış ve "Alman CMK m. 100c gereği konutun teknik araçlarla akustik olarak dinlenmesinden" uyarlanan bir suç kataloğu dahil edilmiş şekilde yeni bir madde önerilmiştir.

Hukuk İşleri ve Tüketici Koruma Komisyonunu söz konusu değişiklikleri yasa tasarısına dahil etmesinden hemen iki gün sonra, 22 Haziran 2017 tarihinde Federal meclis ikinci müzakeresini gerçekleştirmiş ve Komisyonu'nun taslağı büyük çoğunlukla kabul edilmiştir[593]. 7 Temmuz 2017 tarihinde Federal Konseyin tasarıya onayını vermesiyle birlikte[594], 17 Ağustos 2017 tarihli Ceza Muhakemesinin Daha Etkin ve Uygulanabilir Düzenlenmesi Hakkında Kanun ile 24 Ağustos 2017 tarihinde online arama tedbiri Ceza Muhakemesi Kanununun 100b maddesi uyarınca yürürlüğe girmiştir.

İfade edilmelidir ki, teknik karmaşıklık ve özellikle de temel haklara yönelik öngörülen müdahalelerin yoğunluğu göz önünde bulundurulduğunda, 100b maddesinin kabul edildiği yasama süreci şaşırtıcı derecede kısa sürmüş ve parlamentoda temel hakların çok az dikkate alındığı bir süreç gerçekleşmiştir[595]. Tüm yasama sürecinin toplam dört buçuk ay sürdüğünü ve sonuç itibariyle gerek online arama tedbirinin gerekse kaynak telekomünikasyon denetiminin müdahaleci kimliklerinin kamuoyunda tartışılmadan Ceza Muhakemesi Kanununa adli amaçla

[589] BTag-Drucksache 18/11272.
[590] BT-Protokoll, 9.3.2017 S. 22 no.142 ve s. 22 no.183.
[591] Ausschuss-Drucksache 18(6)334, 15.05.2017.
[592] BT-Drucksache 18/12785, 20.06.2017.
[593] BT-Protokoll, 22.06.2017, s. 24 no. 585 vd.
[594] BR-Protokoll, 07.07.2017, s356.
[595] MüKoStPO/Rückert StPO §100b Rn. 16.

dahil edildikleri eleştirilmektedir[596]. Yasanın kabul edilme biçimine ve içeriğine yönelik sert eleştiriler yasa tasarısı hakkında alınan bilirkişi raporlarında ve Alman Barolar Birliği Ceza Hukuku Komitesi'nin açıklamalarında da yer almaktadır[597].

Özellikle de Hukuk İşleri ve Tüketiciyi Koruma Komisyonunun önemli ancak göze çarpmayan yasa değişikliklerinin arkasına gizlenerek, ilk yasa tasarısında yer almayan iki önemli müdahale tedbirini kanun haline getirmesinin tabiri caizse "buruk bir tat" bıraktığı ifade edilmektedir[598].

II. YASAL DÜZENLEMELER

A. Genel Olarak

Çalışmamızın tarihi gelişimi bölümünde gerek önleme alanında gerekse baskılayıcı alanda Alman Hukuk sisteminde online arama tedbirine yönelik çeşitli düzenlemeler yapıldığını belirttik. Çalışmamızın devamında öncelikle önleme alanındaki yürürlükte olan düzenlemeler incelenecek olup, bu incelemeyi adli amaçla online düzenlemesi takip edecektir.

B. Önleme Amaçlı Online Arama Düzenlemeleri

Almanya Cumhuriyetinin Federal yapısı sebebiyle gerek federal gerekse federe düzeyde önleme amaçlı online arama düzenlemelerine rastlamak mümkündür.

Federe devletler suçların önlenmesi de dahil olmak üzere tehlikenin önlenmesinden sorumludur. Aynı zamanda Federal Kriminal Dairesinin uluslararası terörizm tehlikesini önlemekle sınırlı olan önleyici kolluk sorumluluğu bulunmaktadır.

Buna özellikle internetin kullanımından kaynaklanan bazı tehlikelerin önlenmesi için ihtiyaç duyulmuştur. Zira modern bir iletişim ve bilgi teknolojisi olarak internet, önemli kamu güvenliği değerlerine yönelik tehditlerin ortaya çıkmasını

[596] Kochheim, KriPoZ 2/2018, s. 61; Yasanın kabul edilme biçimine ve içeriğine yönelik sert eleştiriler ayrıca yasa tasarısı hk. Alınan bilirkişi raporlarına ve Alman Barolar Birliği Ceza Hukuku Komitesi'nin açıklamalarına da yansımıştır.
[597] Özellikle Prof. Dr. Arndt Sinn'in, Dr. Ulf Buermeyer'in ve Linus Neumann'ın bu yönde eleştirileri için bkz: Deutscher Bundestag - Stellungnahmen der Sachverständigen, Erişim tarihi: 01.06.2024:
[598] Kochheim, KriPoZ 2/2018, s. 61.

kolaylaştırmaktadır. Bu durum örneğin aşırı İslamcı propagandanın yayılması, terörist saldırısı tehdidi ve World Wide Web'in organize suçlar tarafından bir araç olarak kullanılması için geçerlidir. Benzer durum çocukların cinsel istismarına yönelik hazırlık eylemleri ve kapalı internet forumlarında çocuk pornografisinin yayınlanması ve satışı için de söz konusudur. Bu tehlikeler, iletişim süreçlerinin bilgi teknolojisi sistemleri ve kriptolojik yöntemler kullanılarak telefon bağlantıları üzerinden giderek daha fazla gerçekleştiriliyor olması nedeniyle daha da artmaktadır[599].

1. Federal Kriminal Dairesi Kanunu *("Bundeskriminalamtsgesetz")* [600]

Federal Almanya Anayasası'nın 73. maddesinin 1. fıkrasının 9a bendi [601]uyarınca Federal devlet, uluslararası terörizm tehdidine karşı Federal Kriminal Dairesi için münhasır yasama yetkisine sahiptir. Bu yetki, sınır ötesi bir tehdidin söz konusu olduğu, bir eyalet polis makamının yetkisinin tanınmadığı veya en yüksek eyalet makamının devralınmasını talep ettiği durumlarda kullanılır.

27 Şubat 2008 tarihli Federal Almanya Anayasa mahkemesinin kararına müteakip Federal Kriminal Dairesi Kanunu reforme edilmiş ve 25 Aralık 2008 tarihinde yürürlüğe girmiştir[602]. Mevcut yasama döneminin en önemli güvenlik kanunu olarak nitelendirilen Federal Kriminal Dairesi Kanunu ile Federal Kriminal Dairesine terörle mücadelede ilk kez önleyici kolluk yetkileri verilmiştir[603].

Federal Anayasa mahkemesinin online arama tedbirinin belirli koşullar yerine getirilerek bir yetkilendirme temeliyle mevzuatlarda yer alabileceğine hükmetmesinin üzerine, online arama Federal Kriminal Dairesi Kanunu'nun 20k maddesinde düzenleme altına alınmıştır. Lakin çalışmamızın tarihi gelişim bölümünde de belirttiğimiz üzere, Federal Anayasa Mahkemesi 20 Nisan 2016 tarihli kararında 20k maddesi çerçevesinde Federal Kriminal Dairesinin bilişim sistemlerine gizli erişim yetkisinin prensipte Anayasa ile uyumlu olduğuna, ancak 20k maddesinin özel hayatın çekirdek alanının korunmasını yeterli ölçüde dikkate almaması sebebiyle anayasaya aykırı olduğuna hükmetmiştir. Anayasa mahkemesinin bu kararı üzerine, Federal

[599] Soine, Eingriffe in informationstechnische Systeme nach dem Polizairecht des Bundes und Laender, NVwZ 2012, 1585.
[600] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtsgesetz – BKA-Gesetz)
[601] Art. 73 § 1 Abs. 1 Nr. 9a GG.
[602] BGB I, 3083.
[603] Roggan, Fredrik, Das neue BKA-Gesetz, NJW 2009, 257; Baum/Schantz, die Novelle des BKA-Gesetzes, ZRP 2008, 137.

Kriminal Dairesi Kanununda kapsamlı değişiklikler yapılmış ve 1 Temmuz 2017 yılında yürürlüğe girmiştir[604].

Bunun sonucunda bilgi teknoloji sistemlerine gizli erişim Federal Kriminal Dairesi Kanunu'nun uluslararası terörizmle mücadeleyi düzenleyen bölümün altında 49. Maddede düzenlenmiştir[605]. Bu hüküm, Federal Kriminal Dairesinin uluslararası mücadelede yetkisinin bir parçası olarak bilgi teknoloji sistemlerine müdahale etmek için teknik araçlar kullanılmasına imkân tanımaktadır. Hükmün son derece müdahaleci bir soruşturma tedbiri ve katı maddi ve usuli gerekliliklere tabi olduğu vurgulanmaktadır[606]. Sekiz fıkradan oluşan oldukça ayrıntılı bir düzenleme yapıldığını ve kısmen Federal Almanya Anayasası Kararının metninden faydalanıldığını ifade edebiliriz.

Federal Kriminal Dairesi Kanunu'nun 49. Maddesi gereği bilgi teknolojisi sistemlerine gizli erişim Federal Anayasa Mahkemesinin içtihadı uyarınca "konutun izlenmesi" temel hakkına benzer ancak diğer gizli gözetim tedbirlerin ötesine geçer bir şekilde temel haklarla yakından ilgili olduğu belirtilmektedir[607].

49. maddenin birinci fıkrası gereği, Federal Kriminal Dairesi ilgili kişinin bilgisi olmadan bir kişinin yaşamı, bedeni ve özgürlüğüne ya da devletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu mallarına yönelik tehlike bulunduğuna dair somut olguların var olması halinde, bilgi teknolojisi sistemlerine teknik araçlarla müdahale edilip, sistemden verilere erişilebilir. Ayrıca belirli olguların öngörülebilir bir zaman diliminde, en azından somutlaştırılmış bir şekilde öngörülebilir bir süre içinde bu belirtilmiş olan hukuki değerlere zarar verilebilmesi halinde ve bir kişinin bireysel davranışının belirtilmiş olan hukuki değerlere somut olarak zarar verebilme olasılığının bulunması halinde tedbire başvurulabilir.

Bununla birlikte tedbir Federal Kriminal Dairesi Kanunu'nun 5. madde kapsamındaki "Uluslararası terör tehlikesine karşı savunma" yükümlülüğünün yerine getirilmesi için gerekli olması ve aksi takdirde anlamsız veya çok daha zor olması durumunda uygulanabileceği düzenlenmiştir.

---

[604] 01.07.2017 tarihli BKA-Gesetz
[605] Federlal Kriminal Dairesi Kanunu'nun 49 maddesi: § 49 BKAG - Bireysel standart (gesetze-im-internet.de), Erişim tarihi: 01.06.2024:
[606] NK-BKAG/Naumann BKAG § 49 Rn. 1.
[607] BVerfG Urt. v. 20.4.2016 – 1 BvR 966/09 ua –, BVerfGE 141, 220 (298 f., Rn. 192).

Her hayata, bedene veya özgürlüğe karşı bulunan tehlikenin online arama kararına başvurulabilmesi için yeterli olmadığını belirtmek gerekir. İnsanın hayatını ve beden bütünlüğünü ilgilendiren tehlikeler bakımından, örneğin terörist faaliyetleriyle ilgili olan belirli sağlık riskleri online arama kararı için gerekçe gösterilebilir[608].

Tehlike tanımı bakımından birinci fıkrada kanun koyucunun müdahale eşiği olarak "müdahaleyi haklı kılan belirli olgulardan" bahsettiğini görmekteyiz. Bunun neticesinde, somut bir tehlikenin varlığının ön koşul olarak düzenlenmediğini ifade edebiliriz.

Buna göre, tehlikenin yakın gelecekte gerçekleşeceğinin yeterli olasılıkla tespit edilemediği durumlarda, olguların somut olayda ağır basan bir hukuki menfaate yönelik yakın bir tehlikeye işaret etmesi halinde bilgi teknolojisi sistemine erişim haklı görülebilir. Bir yandan olgular, olayın en azından somut nitelikte olduğu ve zaman içinde öngörülebilir olduğu sonucuna varılmasına imkân vermelidir. Diğer yandan olgular, kimliği hakkında en azından gözetim tedbirini gerektirecek ölçüde bilgi sahibi olunan belirli kişilerin dahil olacağına ve tedbire büyük ölçüde bu kişilerle sınırlı olarak başvurulabileceğine işaret etmelidir. Dolayısıyla henüz bir zararın meydana gelme gerekliliği aranmayıp, bir tehlikenin varlığı için azaltılmış bir olasılık ölçütü benimsenmiştir[609]. Bu doğrultuda bilinen olgulardan yola çıkarak bir tehlikenin varlığının mümkün görünüp görünmemesi açısından bir öngörüde bulunmak mümkün olmalıdır[610].

49. maddenin ikinci fıkrası gereği, bilgi teknolojisi sisteminde yalnızca veri toplama için gerekli olan değişikliklerin yapılabileceği ve tedbirin sonunda yapılan değişikliklerin, teknik olarak mümkün olduğunca otomatik olarak geri alınacağı düzenlenmiştir. Ayrıca kullanılan araçların en son teknolojiye uygun olarak yetkisiz kullanıma karşı korunması, kopyalanan verilerin değiştirilmeye, yetkisiz silinmeye ve son teknolojiye yetkisiz erişime karşı korunması gerektiği hüküm altına alınmıştır.

Tedbirin uygulanabilecek kişiler bakımından ise 49. Maddenin üçüncü fıkrasında düzenleme getirilmiştir. Bu tedbir yalnızca Federal Kolluk Kanunu'nun 17. veya 18. maddesi uyarınca sorumlu olan bir kişiye karşı uygulanabilir. Bu, söz konusu tedbirin yalnızca tehlikeye neden olan veya on dört yaşından küçükse onu

[608] NK-BKAG/Naumann BKAG § 49 Rn. 27.
[609] NK-BKAG/Naumann BKAG § 49 Rn. 30.
[610] Bantlin JuS 2019, 669 (673).

denetlemekle yükümlü olan bir kişiye karşı uygulanabileceği anlamına gelmektedir. Ayrıca tedbir, tehlikeye neden olan başka bir kişiyi görevi yerine getirmesi için yetkilendiren bir kişiye[611] karşı da yöneltilebilir. Bunun dışında bu tedbir fiili güç sahibi, mal sahibi veya diğer yetkili kişilere karşı da online arama kararı verilebilir. Tehlikenin bir hayvan veya nesneden kaynaklanması halinde[612], nesnenin mülkiyetinden feragat etmiş olan kişiler de tedbire maruz kalabilir. Bu nedenle bilgi teknolojisi sistemlerinin sahiplerine veya işletmecilerine[613] karşı da bu tedbirin uygulanmasının mümkün olabileceği, bu nedenle tedbirin uygulanabileceği kişi kapsamının Federal Anayasa Mahkemesinin kararında olduğu kadar dar olmadığı ve bu sebeple de ölçülülük ilkesini etkilediği eleştirilerek ifade edilmektedir[614]. Federal Anayasa Mahkemesi'nin kararına göre, bilgi teknolojisi sistemlerinin sahipleri veya işletmecilerinin tedbirden doğrudan etkilenebilecek kişiler arasında değil, yalnızca diğer üçüncü taraflar arasında yer aldığı vurgulanmaktadır[615].

49. maddenin dördüncü fıkrasında tedbir kararının sadece Federal Kriminal Dairesi Başkanının veya temsilcisinin talebi üzerine mahkeme tarafından verilebileceği düzenlenmiştir. Beşinci fıkrada ise tedbire yönelik talebin neleri içermesi gerektiği düzenleme altına alınmıştır. Bunlar;

1. Tedbirin uygulanacağı kişinin mümkün olduğunca ismi ve adresi ile,
2. Veri toplamaya müdahale edilecek bilgi teknolojisi sisteminin mümkün olduğunca açık bir şekilde tanımlanması,
3. Tedbirin niteliği, kapsamı ve süresi;
4. Somut olay ile
5. Gerekçe.

49. maddenin altıncı fıkrasında tedbir kararının yazılı olarak verilmesi gerektiği düzenlenmiştir. Bununla birlikte, tedbirin en fazla üç ay ile sınırlı olacağı, ancak gerekli duyulduğu ve tedbirin koşullarının devam etmesi halinde, üç aydan fazla olmayan bir uzatmaya izin verilebileceği hüküm altına alınmıştır.

Devamında, 49. Maddenin yedinci fıkrasında yalnızca özel hayatın çekirdek alanını ilgilendiren bilgilerin sağlanacağına yönelik somut olguların bulunması halinde, tedbirin uygulanamayacağı, mümkün olduğunca, özel hayatın temel alanına

[611] Federal Kolluk Kanunu'nun 17. Maddesi gereği.
[612] Federal Kolluk Kanunu'nun 18. Maddesi gereği.
[613] Soine, NVwZ 2012, S. 1588.
[614] Baum/Schnatz, ZRP 2008, s. 140.
[615] Baum/Schnatz, ZRP 2008, s. 140.

ilişkin verilerin toplanmamasının teknik olarak sağlanması gerektiği düzenlenmiştir. Özel hayatın çekirdek alanını ilgilendiren verilerin elde edilmesi durumunda bunlar derhal mahkemeye sunulmalıdır. Elde edilen verilerin kullanılıp kullanılamayacağına ya da silinip silinemeyeceğine karar verme sorumluluğu kararı veren mahkemeye aittir. Özel hayatın çekirdek alanını ilgilendiren veriler kullanılamaz ve derhal silinmelidir.

Ayrıca verilerin elde edilmesi ve silinmesiyle ilgili adımların belgelenmesi gerekmekte olup, bu belgelerin sadece veri koruma denetimi amacıyla kullanılabilir. Tedbire maruz kalan kişi ve diğer bağlantılı kişilerin tedbirle ilgili bildirilmesinden altı ay sonra veya bildirim yapılamayacağın nihai olarak mahkeme tarafından onaylanmasından altı ay sonra belgelendirme (tutanaklar) silinebilir. Veri koruma denetiminin tamamlanmadığı hallerde, belgelerin denetim tamamlanana kadar saklanmalıdır.

Federal Kriminal Dairesi Kanunu'nun önceki 20 k düzenlemesinde gerek özel hayatın çekirdek alanı gerekse silme kayıtlarının saklanması için öngörülen düzenlemelerin Federal Anayasa Mahkemesi tarafından yetersiz olarak değerlendirilmişti. Bu bağlamda 49. Madde ile getirilen düzenlemelerin Federal Anayasa Mahkemesi Kararlarıyla uyumlu olduğunu ifade edebiliriz.

49. maddenin sekizinci ve son fıkrası uyarınca, gecikmesi sakınca bulunan hallerde, Federal Kriminal Dairesi Başkanı veya temsilcisi Federal Kriminal Dairesi Veri Koruma Görevlisine danışarak bulguların kullanımına karar verebilir. Bu durumda mahkeme kararı ivedilikle talep edilmelidir.

2. Anayasanın Korunması Hakkında Kanunun Uyarlanmasına İlişkin Kanun (" Gesetz zur Anpassung des Verfassungsschutzrechts")

9 Temmuz 2021 tarihinde, Alman istihbarat servislerine telekomünikasyonu izleme konusunda geniş yetkiler veren "Anayasanın Korunması Hakkında Kanunun Uyarlanmasına İlişkin Kanun" yürürlüğe girmiştir[616]. Bu Kanun ile Federal Almanya Anayasa Koruma Kanununda, Güvenlik Soruşturma Kanununda[617], Askeri Karşı-İstihbarat Servisi Kanununda[618], Federal İstihbarat Servisi Kanununda[619] ve Mektup,

[616] BT-Drucksache 19/30477.
[617] Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz).
[618] Gesetz über den militärischen Abschirmdienst (MAD-Gesetz).
[619] Gesetz über den Bundesnachrichtendienst (BND-Gesetz).

Posta ve Telekomünikasyon Gizliliğinin Sınırlandırılması Hakkında Kanunda[620] bazı değişiklikler yapılmıştır.

Federal İçişleri Bakanlığı, değişiklikler öngören bu Kanunu, federal hükümet tarafından aşırı sağcılık ve ırkçılıkla mücadele için benimsenen yasal politika tedbirlerinin merkezi bir ayağı olarak tanımlamaktadır[621].

Bu kapsamda getirilmiş olan esaslı değişiklikler şu şekilde özetlenebilir. Kaynak telekomünikasyon denetimine ilişkin bir düzenleme getirilmiş olup, telekomünikasyon gözetiminin uygulanması dijital dünyada değişen kullanım koşullarına uyarlanmıştır. Aşırılık yanlısı bireylerin izlenmesi, Anayasayı Koruma Dairesinin yürüttüğü erken uyarı işlevine entegre edilmiştir. Bu sayede, daha içe dönük bir radikalleşme seyri izleyen bireysel suçluların fail profiline daha iyi ve her şeyden önce erken odaklanılması amaçlanmaktadır. Askeri Karşı İstihbarat Servisi'nin anayasayı koruma makamlarının istihbarat bilgi sistemine entegre edilmesi için yasal bir zemin oluşturulmuştur. Bu sayede, aşırı sağcı şebekelerin soruşturulmasında Anayasayı Koruma Teşkilatı ile Askeri Karşı İstihbarat Servisi arasındaki iş birliğinin geliştirilmesi amaçlanmaktadır[622].

Telekomünikasyonun izlenmesi bakımından getirilen düzenleme, *"Kararın verildiği zamandan itibaren devam eden telekomünikasyonun izlenmesi ve kaydedilmesi, özellikle şifrelenmemiş biçimde izleme ve kaydetmeyi mümkün kılmak için gerekli olması halinde, veri sahibi tarafından kullanılan bir bilgi teknolojisi sistemine müdahale edilecek şekilde de gerçekleştirilebilir. Kararın verildiği andan itibaren veri sahibinin bilgi teknoloji sisteminde saklanan iletişimin içeriği ve koşulları, kamuya açık telekomünikasyon ağında devam eden iletim süreci sırasında şifrelenmiş biçimde de izlenmesi ve kaydedilmesi mümkün olması durumunda da izlenebilir ve kaydedilebilir[623]".*

Sonuç olarak, istihbarat servislerine telekomünikasyonun izlenmesi bakımından, geniş yetkilerin getirilmiş olduğunu belirtebiliriz. Özellikle de şifrelenmiş iletişimin söz konusu olduğu hallerde, şifreyi çözmek için yazılımın kullanılması öngörülmüş. Bu bağlamda doğrudan Kaynak-Telekomünikasyon tedbiri ile getirilmiş düzenlemelerin uygulanabileceğini ifade edebiliriz. Ancak Kaynak-

[620] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz).
[621] BMI - Gesetzgebungsverfahren - Gesetz zur Anpassung des Verfassungsschutzrechts (bund.de), Erişim tarihi: 01.06.2024:
[622] BT-Drucksache 19/30477.
[623] Askeri Karşı-İstihbarat Servisi Kanununun 11/1a maddesinde düzenlenmiştir.

Telekomünikasyon tedbirinin online arama tedbirinden faklı olduğunu da çalışmamızın ilk bölümünde ifade etmiştik.

Bu nedenle Anayasanın Korunması Hakkında Kanunun Uyarlanmasına İlişkin Kanunun online arama bakımından bir düzenleme içermediğini ileri sürebiliriz.

3. Federal Almanya Anayasa Koruma Kanunu *("Bundesverfassungsschutzgesetz")* [624]

20 Aralık 1990 tarihinde düzenlenmiş olan Federal Almanya Anayasa Koruma Kanunu'nun 1. Maddesi gereği Anayasanın korunması, özgür demokratik düzenin, Federal Devletin ve eyaletlerin varlığının ve güvenliğinin korunmasına hizmet eder. Federal Devlet ve eyaletler, Anayasanın korunması ile ilgili konularda iş birliği yapmakla yükümlüdürler.

Kanunun 3. Maddesinde Anayasa Koruma kurumlarının görevleri düzenlenmiştir. Bu bağlamda Federal ve federe devleti anayasayı koruma kurumlarının görevi özellikle demokratik düzeni ilgilendiren tehditler, güvenliği tehlikeye atan faaliyetler veya yabancı bir güç adına bu Kanun kapsamındaki gizli servis faaliyetleri, bu Kanunun uygulama alanına giren ve uluslararası anlayış fikrine, özellikle de insanların barış içinde bir arada yaşamasına karşı olan girişimler konusunda başta olgusal ve kişisel bilgi olmak üzere genel olarak bilgi, istihbarat ve belge toplamak ve analiz etmektir.

Alman Federal Anayasayı Koruma Teşkilatının yetkileri Kanunun 8 maddesinde düzenleneme altına alınmıştır. Buna göre, Federal Anayasayı Koruma Teşkilatı, Federal Veri Koruma Yasası'nın ilgili hükümleri veya bu yasadaki özel hükümler aksini öngörmediği sürece, kişisel veriler de dahil olmak üzere görevlerini yerine getirmek için gerekli bilgileri işleyebilir. Veri sahibinin rızası olması halinde de işleme yetkisi bulunmaktadır. Federal Anayasayı Koruma Teşkilatı'ndan kişisel verilerin iletilmesi için yapılan bir talep, yalnızca talebin sağlanması için gerekli olan kişisel verileri içerebilir. Veri sahibinin korunmaya değer menfaatleri ancak kaçınılmaz ölçüde zarar görebilir. Bunun ötesinde Federal Anayasayı Koruma Teşkilatı, gizlice bilgi toplamak için gizli danışmanlar ve muhbirler, gözetleme, video ve ses kayıtları,

[624] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG) BVerfSchG - Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (gesetze-im-internet.de), Erişim tarihi: 01.06.2024.

kamuflaj kağıtları ve kamuflajlı kimlik plakaları gibi yöntemler, nesneler ve araçlar kullanabilir. Bireysel haklara ancak özel yetkiler çerçevesinde müdahale edilebilir.

Bu yetkileri incelediğimizde, online aramaya yönelik herhangi bir yetkilendirme bulunmadığını görmekteyiz. Ancak ifade edilmelidir ki, Mart 2019' da Federal İçişleri Bakanlığı tarafından "Anayasanın Korunmasına İlişkin Yasanın Uyumlaştırılması Hakkında Yasa Tasarısı" internete düşmüştür[625]. Yasa tasarısının içerdiği önemli bir düzenleme ise, Federal Anayasayı Koruma Teşkilatının online arama yapabilmesi için gizlice ilgili kişinin konutuna girip bilgi teknoloji sistemine yazılım sızdırmaya yöneliktir. Bu yasa tasarısıyla ilgili bazı milletvekillerin ve AfD parti grubunun İçişleri Bakanlığına yönelttiği sorulara[626], Federal hükümetin bilgi talebine istinaden verdiği cevabı; kuvvetler ayrılığı ilkesinin, parlamento tarafından denetlenemeyen bir inisiyatif, istişare ve eylem alanını içeren temel bir yürütme sorumluluğu alanına yol açmasını, federal hükümetin kural olarak kendisinin münhasır yetkisi dahilinde olan konular hakkında parlamentonun bilgi taleplerini yerine getirmekle yükümlü olmadığını, Parlamento'nun denetim yetkisinin sadece halihazırda sonuçlandırılmış süreçleri kapsadığını ve devam eden müzakerelere müdahale etme yetkisini içermediğini bu nedenle de bilgi vermeyeceği şeklinde olmuştur[627]. Bu yasa tasarısı büyük yankı uyandırmıştır, zira kolluk kuvvetleri tarafından doğrudan adli amaçlı veya tehlikeyi önleme amaçlı yapılmasına izin verilmeyen tedbir yetkisinin, Federal Anayasa Mahkemesi'nin anlayışına göre[628] güvenlik otoritesi olarak bile kabul edilmemesi gereken bir kuruma verilmesi çok eleştirilmiştir[629]. Tüm eleştiriler üzerine önerilen yasa tasarısı hakkında Federal Parlamentoda görüşülmekten vazgeçilmiştir[630].

[625] Meister/Biselli, Wir veröffentlichen den Gesetzentwurf: Seehofer will Staatstrojaner für den Verfassungsschutz (netzpolitik.org), Erişim tarihi: 01.06.2024.
[626] BT-Drucksache 19/14602 ("Kleine Anfrage")
[627] BT-Drucksache 19/15219.
[628] BVerfGE 133, 277 (327).
[629] Roggan, Die Überwachung von IT-Systemen und das Wohnungsrundrecht, Vorgaenge Nr. 227, Polizei und Technik, 11/2019, s. 147 vd.
[630] Behring, Einbrechen für Staatstrojaner: Verfassungsschutz soll mehr Befugnisse erhalten als bisher gedacht (netzpolitik.org), Erişim tarihi: 01.06.2024; Roggan, Die Überwachung von IT-Systemen und das Wohnungsrundrecht, Vorgaenge Nr. 227, Polizei und Technik, 11/2019, s. 147 vd.

4. Eyaletlerin Anayasalarını Koruma Kanunları *("Landesverfassungsschutzgesetze")*

Kuzey Ren-Vestfalya Eyaleti Anayasayı Koruma Yasası öncü bir rol oynamıştır. Çalışmamızda belirttiğimiz gibi, Kuzey Ren-Vestfalya Anayasayı Koruma Yasasında internet içeriklerinin gizli olarak takip edilmesi ve aydınlığa kavuşturulması ile bilgi teknoloji sistemlerine gizli olarak erişimin sağlanması yönünde 20 Aralık 2006 tarihinde tedbirler düzenleme altına alınmış olup, Federal Almanya Anayasa mahkemesi ilgili düzenlemelerin Anayasa ile uyumlu olmadıklarına, bu nedenle hükümsüz olduklarına karar vermiştir. Yürürlükte olan Kuzey Ren-Vestfalya Eyaleti Anayasayı Koruma Yasası m. 5/2 No. 11 gereği, kamuya açık olmayan iletişim içeriğinin izlenmesine izin verilmiş olup, ancak online arama bakımından herhangi bir yetkinin tanınmadığı açıkça hüküm altına alınmıştır[631].

Hessen eyaletinde 14 Kasım 2017 tarihinde "Anayasa Koruma Teşkilatının yeni yapılanmasına ilişkin yasa tasarısı" açıklanmıştır. Bu tasarıda terör suçları ve bunların oluşturduğu büyük tehlike ve tehditlere işaret edilip, iyi işleyen bir "güvenlik mimarisine" ihtiyaç duyulduğu ifade edilmektedir. Bu doğrultuda tasarının 7. Maddesinde "konutun izlenmesi için teknik araçların kullanımı" ile 8. Maddesinde "bilgi teknolojisi sistemlerine gizli erişim" öngörülmüştür[632]. Ancak bu yasa tasarısı kabul edilmemiştir.

12 Haziran 2018 tarihinde kapsamlı bir reforma uğrayan Bavyera Anayasayı Koruma Kanunu uyarınca Bavyera Eyaleti Anayasayı Koruma Dairesi, bilgi teknolojisi sistemlerine gizlice erişme yetkisine sahip olmuştur[633].

Bu yetki Bavyera Anayasayı Koruma Kanunu'nun 10. Maddesinde düzenleme altına alınmış olup, buna göre, yasal bir menfaate yönelik belirli bir tehdidi önlemek amacıyla, teknik araçlar kullanarak, veri sahibinin meşru gizlilik beklentisi içinde kendi olarak kullandığı ve kendi belirlediği tasarrufuna tabi olan bilgi teknolojisi sistemlerine yalnızca erişim verilerini ve işlenmiş verileri elde etmek veya bu tedbirlere hazırlık olarak belirli tanımlayıcıları ve bilgi teknolojisi sisteminin yerini belirlemek için gizlice erişilebilir.

---

[631] SGV § 5 (Fn 19) Befugnisse | RECHT.NRW.DE, Erişim tarihi: 01.06.2024.
[632] Hessischer Landtag-Drucksache 19/5412.
[633]Bayerisches Verfassungsschutzgesetz (BayVSG) Bürgerservice - BayVSG: Bayerisches Verfassungsschutzgesetz (BayVSG) Vom 12. Juli 2016 (GVBl. S. 145) BayRS 12-1-I (Art. 1–34) (gesetze-bayern.de), Erişim tarihi: 01.06.2024.

Bavyera Anayasası Koruma Kanunu'nun online arama bakımından Federal Anayasa Mahkemesi'nin 2016 tarihli kararının özellikle dikkate alındığı ifade edilmektedir. Bu bağlamda Federal Anayasa Mahkemesi Kararının sadece Federal Kriminal Dairesinin yetkilerine yönelik olmuş olsa da gerekliliklerin diğer güvenlik makamlarına, özellikle de istihbarat servislerinin çalışmaları için yasal zemine aktarılmasının uygun olarak değerlendirildiği belirtilmektedir. Zira gizli bilgi toplamanın, istihbarat faaliyetlerinin doğasında olduğu vurgulanmaktadır. Hatta bazı münferit durumlarda, gizliliğin temel haklara yönelik oluşturduğu özel tehditin, istihbarat servisleri tarafından veri elde edilmesi halinde, kolluk makamları tarafından alınan gizli tedbirlere kıyasla daha yüksek olabileceği ileri sürülmektedir[634].

Sonuç olarak günümüzde sadece Bavyera eyaletinin Anayasayı Koruma Kanunu'nda online arama tedbirine yönelik bir düzenleme bulunduğunu ifade edebiliriz.

5. Eyaletlerin Kolluk Kanunları ("Polizeigesetze der Bundesländer")

Öncelikle "Federal Kolluk Kanunu'nda" (Bundespolizeigesetz) bilgi teknoloji sistemlerine gizli erişim için herhangi bir düzenleme yapılmadığını ifade etmek isteriz. Kolluk Kanunları bakımından eyalet düzeyinde düzenlemeler yapılmış, eyaletlerin Kolluk Kanunlarında 2018 itibariyle kanunların değiştirilmesi yönünde yoğun [635]çalışmalar yürütülmeye başlamıştır. Bu çerçevede online arama tedbiri en tartışmalı yetkilerden biri olarak dikkat çekmiştir. İfade edilmelidir ki, Federal Almanya Anayasası'nın 27 Şubat 2008 ve 20 Nisan 2016 tarihli kararları eyalet mevzuatı için de belirleyicidir. Federal Anaysa Mahkemesi kolluk hukukunun yeni veya değişsen tehlike veya tehdit senaryolarına uyarlanabileceğini açıklamıştır[636]. Ancak mahkeme aynı zamanda bireyi devletin gizli erişiminden korumayı amaçlayan bilgi teknolojisi sistemlerinin gizliliğinin ve bütünlüğünün garanti altına alınmasına ilişkin temel hakkı genel kişilik hakkından türetmiştir. Tehlikeyi önlemek için bu temel hakka yönelik müdahaleler söz konusu olduğunda, ilgili kişi sadece anayasal bir yasal temele dayanan haklarına yönelik kısıtlamaları kabul etmelidir[637].

---

[634] Reform des Bayerischen VErfassungsschutzgesetzes 2018, BayLfD: 5. Verfassungsschutz (datenschutz-bayern.de), Erişim tarihi: 01.06.2024.
[635] Neue Polizeigesetze, überall – eine Bestandsaufnahme» LabourNet Germany, Erişim tarihi: 01.06.2024; Übersicht über die Änderungen der Polizeigesetze in den einzelnen Bundesländern | Amnesty International, Erişim tarihi: 01.06.2024.
[636] BVerfGE 115, 320 = NJW 2006, 1939 (1946) = NVwZ 2006, 1156.
[637] BVerfGE 120, 274 = NJW 2008, 822 (824).

Her eyaletin kolluk veya benzeri Kanunu'nda online arama tedbiri henüz düzenlenmemiş olup, 16 eyaletten sadece 5 eyalette bu tedbirin hüküm altına alınmış olduğunu belirtebiliriz.

Bunlar Bavyera Polis Vazifeleri Kanunu, Hessen Kamu Güvenliği ve Düzeni Hakkında Kanun, Mecklenburg-Vorpommern Kamu Güvenliği ve Düzeni Hakkında Kanunu, Aşağı Saksonya Polis ve Zabıta Teşkilatı Kanunu, Kuzey Ren Vestfalya Polis Kanunu ile Renanya-Palatina Polis ve Zabıta Teşkilatı Kanunu.

a. Bavyera Polis Vazifeleri Kanunu (Polizeiaufgabengesetz-PAG)[638]

Bavyera eyaletinin Polis Vazifeleri Kanunu'nun "Veri toplama için özel yetki ve önlemler" başlığı altında 45. Madde de bilgi teknoloji sistemlerine gizli erişim düzenleme altına alınmıştır[639].

Buna göre, kolluk erişim verilerini ve depolanan verileri toplamak amacıyla hâkim kararıyla bilgi teknolojisi sistemlerine gizlice erişmek için teknik araçlar kullanabilir.

Burada tedbire maruz kalan kişi tehlikeden veya muhtemel bir tehlikeden sorumlu olan kişidir ve bu tedbir federal hükümetin veya bir eyaletin varlığına veya güvenliğine, yaşama, sağlığa veya özgürlüğe veya kamu mallarına yönelik, insanların varlığının temelini etkileyen bir tehlikenin veya yakın bir tehlikenin önlenmesi için gerekli olduğu ölçüde uygulanabilmektedir. Bununla birlikte, belirli olguların tedbire maruz kalan kişinin başka kişilerin bilgi teknolojisi sistemlerini kullandığı veya kullanmış olduğu ve dolayısıyla bu kişilerin tehlike durumuyla muhtemelen bağlantılı olduğu varsayımı haklı kıldığı ölçüde, diğer kişilerin de bilgi teknoloji sistemlerine gizlice erişilebilir.

Bu tedbir, veri sahibi tarafından kullanılan bilgi teknolojisi sisteminden fiziksel olarak ayrı olan bilgi teknolojisi sistemlerini ve depolama ortamlarını da kapsayacak şekilde genişletilebilir. Ancak bu yalnızca doğrudan inceleme altındaki bilgi teknolojisi sisteminden erişilebildikleri veya veri sahibinin verilerini depolamak için kullanıldıkları takdirde geçerlidir. Bu tedbirler ancak bir polis vazifesinin yerine getirilmesi aksi takdirde anlamsız ya da çok daha zor olacaksa uygulanabilir. Ayrıca

[638] Art. 45 PAG - Verdeckter Zugriff auf informationstechnische Systeme.
[639] Bavyera Polis Vazifeleri Kanunu 45. Madde: Bürgerservice - PAG: Art. 45 Verdeckter Zugriff auf informationstechnische Systeme (gesetze-bayern.de) Erişim tarihi: 01.06.2024.

üçüncü tarafların kaçınılmaz olarak etkilenmesi durumunda da bu tedbirlerin gerçekleştirilebileceği hüküm altına alınmıştır. Kullanılan araçların, teknolojinin en son durumuna uygun olarak yetkisiz kullanıma karşı korunma altına alınması gerektiği de düzenlenmiştir. Bunun ötesinde tedbir kararının şekline, içeriğine ve süresine, tedbirin sonlandırılmasıyla elde edilen verilerin silinmesine ve raporlama yükümlülüğü gibi birçok hususun düzenlendiğini belirtebiliriz.

b. Hessen Kamu Güvenliği ve Düzeni Hakkında Kanun (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung-HSOG) [640]

Online arama Hessen eyaletinde Kamu Güvenliği ve Düzeni Hakkında Kanun'un 15c maddesinde "bilgi teknoloji sistemlerine gizli erişim" başlığı altında düzenlenmiştir[641].

Buna göre polis otoriteleri, bir kişinin hayatı, bedeni veya özgürlüğüne ya da federal devletin veya bir eyaletin temellerini veya varlığını veya insan varlığının temellerini etkileyen bir kamu malına yönelik acil bir tehlikeyi önlemek için gerekli olması halinde, veri sahibi tarafından kullanılan bilgi teknolojisi sistemlerine müdahale etmek için teknik araçlar kullanabilir ve veri sahibinin bilgisi olmadan bunlardan veri elde edebilir.

Tedbirin uygulanabileceği kişiler bakımından, tedbirin bilgi teknolojisi sitemini kullanan kişiler dışında, terör suçlarının önlenmesi için gerekli olduğu ölçüde belirli olguların kişiler üzerinde öngörülebilir bir süre içinde, en azından belirli bir şekilde, kayda değer öneme sahip bir suç işleyecekleri varsayımını haklı çıkarması ve bu suçun önlenmesi için gerekli olması halinde, bu kişilere de uygulanabilmektedir. Ayrıca bireysel davranışlarının öngörülebilir bir süre içinde bir terör suçunun işleneceğine dair somut bir olasılık doğurması ve bu suçun önlenmesinin gerekli olması halinde, tedbir bu kişilere de uygulanabilir.

Tedbir, diğer kişilerin bilgi teknolojisi sistemlerine ancak, yukarıda bahsi geçen kişilerden birinin soruşturmayla ilgili bilgileri kaydettiği ve bunun gerekli olduğu varsayımını haklı kılan olguların bulunması halinde gerçekleştirilebilir. Ayrıca tedbir, diğer kişilerin kaçınılmaz olarak etkilenmesi halinde de uygulanabilir.

---

[640] § 15c HSOG - Verdeckter Eingriff in informationstechnische Systeme.

[641] Hessen Kamu Güvenliği ve Düzeni Hakkında Kanunun 15c maddesi: https://www.rv.hessenrecht.hessen.de/perma?j=SOG_HE_!_15c, Erişim tarihi: 01.06.2024:

Özel hayatın çekirdek alanının korunmasına yönelik te düzenleme getirilmiş, mümkün olduğunca, özel hayatın çekirdek alanına ilişkin verilerin elde edilmemesi için teknik olarak güvencelerin sağlanması gerektiği belirtilmiştir.

c. Mecklenburg-Vorpommern Kamu Güvenliği ve Düzeni Hakkında Kanunu (Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern-SOG M-V)[642]

Mecklenburg-Vorpommern eyaletinin Kamu Güvenliği ve Düzeni Hakkında Kanunun 33c maddesinde "bilgi teknolojisi sistemlerine müdahale etmek için teknik araçların kullanımı" düzenleme altına alınmıştır[643].

Buna göre, bir kişinin hayatı, bedeni veya özgürlüğüne karşı veya federal devletin ya da bir eyaletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu mallarına yönelik bir tehlike bulunması halinde, kolluk veri sahibi tarafından kullanılan bilgi teknolojisi sistemlerine müdahale etmek ve veri elde etmek için gizli teknik araçlar kullanabilir. Tedbirin yalnızca bir tehlikeden sorumlu olan bir kişiye yönelik uygulanabileceği gibi, başka kişilere de ancak olguların az önce ifade ettiğimiz korunan değerler bağlamında etkilenen bir kişinin soruşturmayla ilgili bilgileri bilgi teknolojisi sisteminde sakladığı varsayımını haklı çıkarması durumunda uygulanabilmesi mümkündür.

Bununla birlikte tedbir, ancak tehlikenin önlenmesinin aksi takdirde umutsuz veya önemli ölçüde daha zor olması durumunda gerçekleştirilebilir. Üçüncü kişilerin kaçınılmaz olarak etkilenmesi durumunda da tedbir gerçekleştirilebilir.

Ayrıca özel hayatın çekirdek alanını düzenleyen 26a maddesine atıfta bulunularak bunun bu tedbir bakımından da geçerli olduğunu, bununla birlikte özel hayatın çekirdek alanına ilişkin verilerin elde edilmemesine yönelik teknik olarak mümkün olduğunca güvenceler getirilmesi gerektiği hüküm altına alınmıştır.

Bunun ötesinde, bilgi teknolojisi sisteminde yalnızca veri elde etmek amacıyla değişikliklerin yapılabileceği; yapılan değişikliklerin teknik olarak mümkün olduğu ölçüde, tedbirin sonunda otomatik olarak geri alınacağı; kullanılan araçların, en son teknolojiye uygun olarak yetkisiz kullanıma karşı korunması gerektiği düzenlenmiştir.

---

[642] § 33c SOG M-V - Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme

[643] Mecklenburg-Vorpommern Kamu Güvenliği ve Düzeni Hakkında Kanunun 33c madddesi: Mecklenburg-Vorpommern - § 33c SOG M-V | Landesnorm Mecklenburg-Vorpommern | Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme | § 33c - Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme | gültig ab: 30.12.2023 (landesrecht-mv.de), Erişim tarihi: 01.06.2024.

Ayrıca kopyalanan verilerin değiştirilmeye, yetkisiz silinmeye ve son teknolojiye yetkisiz erişime karşı korunma gerekliliği de getirilmiştir.

Tedbir kararının usulüne, şekline, içeriğine ve süresine ilişkin de açıkça hükümler getirildiğini görmekteyiz. Bu bağlamda Mecklenburg-Vorpommern eyaletinde yapılmış olan düzenlemenin çok detaylı ve kapsamlı olduğunu vurgulayabiliriz.

d. Aşağı Saksonya Polis ve Zabıta Teşkilatı Kanunu (Niedersächsisches Polizei- und Ordnungsbehördengesetz-NPOG) [644]

Aşağı Saksonya eyaletinde Polis ve Zabıta Teşkilatı Kanununun "Veri işleme yetkileri" başlığı altında "bilgi teknoloji sistemlerinde gizli erişimi" 33d maddesinde düzenlemiştir[645].

Buna göre polis, tehlikenin önlenmesi veya suçun önlenmesi için zorunlu ise, veri sahibi tarafından kullanılan bilgi teknolojisi sistemlerine müdahale ederek; 1. acil bir tehlikeyi önlemek amacıyla tehlikeden sorumlu bulunan bir kişinin, 2. olguların, öngörülebilir bir süre içinde, en azından doğası gereği belirli bir şekilde bir terör suçu işleyeceği varsayımını haklı çıkardığı bir kişinin veya 3. bireysel davranışı, öngörülebilir bir süre içinde terör suçu işleyeceğine dair somut bir olasılık oluşturan bir kişinin sistemlerinden veri elde edebilir.

Tedbir, üçüncü kişilerin kaçınılmaz olarak etkilenmesi durumunda da uygulanabilir.

Bununla birlikte tedbire karar vermekle yetkili olan mahkeme, gecikmesi sakınca bulunan hallerde ise kolluğun yetkili olabileceği düzenlenmiştir. Maddenin devamında kararın şekline, içeriğine, kapsamı ve süresine yönelikte somut düzenleme getirildiğini ifade edebiliriz.

[644] § 33d NPOG - Verdeckter Eingriff in informationstechnische Systeme.
[645] Aşağı Saksonya Polis ve Zabıta Teşkilatı Kanununun 33d maddesi: § 33d NPOG, Verdeckter Eingriff in informationstechnische Systeme | Niedersächsisches Vorschrifteninformationssystem (NI-VORIS) (wolterskluwer-online.de), Erişim tarihi: 01.06.2024.

e. Renanya-Palatina Polis ve Zabıta Teşkilatı Kanunu (Polizei- und Ordnungsbehördengesetz-POG) [646]

Renanya-Palatina Polis ve Zabıta Teşkilatı Kanununun 39. Maddesinde[647] "bilgi teknolojisi sistemlerinde teknik araçların kullanılması yoluyla veri toplama" düzenlenerek eyalet düzeyinde online aramanın düzenlenmiş olduğunu belirtebiliriz. Maddenin 1. fıkrasında, polisin, ilgili kişinin bilgisi olmaksızın, ilgili kişinin kullandığı bilişim sistemlerine teknik araçlarla müdahale edebileceği ve bir kişinin hayatına, bedenine veya özgürlüğüne veya federal devletin ya da bir eyaletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu mallarına yönelik bir tehlikeyi önlemek için bunlardan veri toplanabileceği hüküm altına alınmıştır.

Tedbirin yalnızca tehlikeden sorumlu olan kişilere uygulanabileceği ve yalnızca bu kişiler tarafından kullanılan bilgi teknolojisi sistemlerine müdahale edilebileceği vurgulanmıştır. Bununla birlikte tehlikeyi başka bir şekilde önlemenin mümkün görünmediği veya önemli ölçüde daha zor olacağı ölçüde tedbire izin verilir. Tedbir, bireysel davranışları, öngörülebilir bir süre içinde bir suç işleyeceğine dair somut bir olasılık oluşturan kişilere karşı da izin verilir. Burada söz konusu suçlar bağlamında halkın önemli ölçüde sindirilmesi, bir makamın veya uluslararası bir kuruluşun güç kullanarak veya güç kullanma tehdidiyle hukuka aykırı olarak zorlanması veya bir devletin veya uluslararası bir kuruluşun temel siyasi, anayasal, ekonomik veya sosyal yapılarını ortadan kaldırılması veya ciddi şekilde bozulması ve işlenmelerinin niteliği veya etkileri itibariyle bir devlete veya uluslararası bir kuruluşa önemli zararlar verilmesi sayılmıştır.

Ayrıca tedbirin diğer kişilere uygulanması da mümkün olup, ancak bu durumda, tehlikeden sorumlu olan kişilerin soruşturmasıyla ilgili bilgileri diğer kişilerin sistemlerinde sakladığı ve tehlikenin önlenmesinin başka bir şekilde mümkün görünmediği veya önemli ölçüde daha zor olacağı varsayımını haklı çıkarması durumunda diğer kişilerin bilgi teknolojisi sistemlerine müdahale edilebilir. Bunun

[646] § 39 POG - Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen

[647] Renanya-Palatina Polis ve Zabıta Teşkilatı Kanununun 39. Maddesi: Rheinland-Pfalz - § 39 POG | Landesnorm Rheinland-Pfalz | Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen | § 39 - Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen | gültig ab: 07.10.2020 (rlp.de), Erişim tarihi: 01.06.2024.

ötesinde tedbir, üçüncü şahısların kaçınılmaz olarak etkilenmesi durumunda da gerçekleştirilebilir.

Maddenin 2. fıkrasında, örneğin değişiklik yapma konusunda veya kullanılan araçlar bakımından teknik olarak sağlanması gereken koşullar belirlenmiştir.

Hükmün 3. fıkrasında, 1. Fıkrada belirtilen koşullara tabi olarak, bir eyleme hazırlık için belirli tanımlayıcıların ve bir bilgi teknolojisi sisteminin konumu gibi gerekli verilerin bakımından da teknik araçlar kullanılabileceği düzenlenmiştir.

Maddenin 4. ve son fıkrasında ise, yetkili mahkeme ve kararın hakim tarafından yazılı olarak verilmesi gerektiği belirtilmiş olup, ayrıca kararın içeriğine, kapsamına ve süresi yönelik düzenlemeler getirilmiştir.

Sonuç olarak bahsi geçen tüm eyalet Kanunları bakımından online arama tedbirinin hepsinde oldukça detaylı bir şekilde düzenleme altına alındığını gerek tedbirin koşullarının gerekse uygulanma esaslarının Federal Anayasa mahkemesinin kararları uyarınca net bir şekilde ortaya koyulmuş olduğunu ifade edebiliriz. Bu çerçevede tüm bahsi geçen mevzuatların bilgi teknolojisi sistemlerine gizli erişimin özellikle korunan değerler ve menfaateler bakımından Federal Anayasa mahkemesi kararına uygun şekilde düzenlendiğini görmekteyiz. Buna ek olarak önleme amaçlı online aramada korunan menfaatlerden birine yönelik bir tehdit bulunma gerekliliği de karşılanmıştır.

Ayrıca Federal Anayasa mahkemesinin kararında belirtmiş olduğu ve önemsediği özel hayatın çekirdek alanının korunması gerekliliği de incelediğimiz her eyalet mevzuatında ya doğrudan bilgi teknolojisi sistemlerine gizli erişime izin veren ilgili maddede, ya da çekirdek alanının korunmasını düzenleme altına almış olan ayrı bir maddeye atıfta bulunularak düzenleme altına alındığının altını çizebiliriz. Bununla birlikte mevzuatların bir başka ortak noktası tedbire karar vermeye yetkili makamın hâkim olarak belirlenmiş olması ve kararın şeklinin, koşullarının, kapsamının ve süresinin belirtilmiş olmasıdır

C. Adli Amaçlı Online Arama Düzenlemesi: Alman Ceza Muhakemesi Kanunu'nda Online Arama (Alman CMK m. 100b[648])

Online arama tedbiri Ceza Muhakemesi Kanununun 100b maddesinde düzenleme altına alınmıştır. Ceza Muhakemesi Kanununun en ciddi "soruşturma

[648] Alman Ceza Muhakemesi Kanunu §100 b' nin çevirisi şu şekildedir:

"StPO § 100b Bilgisayarda online arama
1) İlgilinin bilgisi olmadan da, aşağıdaki koşulların varlığı halinde, ilgilinin kullandığı bilgi teknolojisi sistemine teknik araçlarla müdahale edilerek bundaki veriler elde edilebilir (online arama);
1. Somut olgular bir kişinin fail veya şerik olarak 2 inci fıkrada sayılan çok ağır suçlardan birini işlediği veya teşebbüsün cezalandırıldığı suçlarda bunu işlemeye teşebbüs ettiği şüphesini doğuruyorsa,
2. Somut olayda da suç özel bir ağırlık arz ediyorsa ve
3. Maddi gerçeğin araştırılması veya şüphelinin bulunduğu yerin belirlenmesi başka yöntemler uygulandığında oldukça zorlaşacak veya olanaksız hale gelecekse.
(2) 1 inci fıkra 1 numaralı alt bendi anlamında özellikle ağır suçtan aşağıda sayılanlar anlaşılır:
***1. Ceza Kanunundan**:*
*a) Alman Ceza Kanunu 81, 82, 89a, 89c/1-4 maddelerde, 94, 95/3 ve 96/1 maddelerde, her halde 97b ile bağlantılı olarak, ayrıca 97a, 98/1 cümle 2, 99/2 ve 100, 100a/4 maddelerde yer alan, **barışa ihanet, vatana ihanet, demokratik hukuk devletini tehlikeye düşürme suçu ve Devletin dış güvenliğini tehlikeye düşürme suçu,***
*b) **İnternetteki ticaret platformunun amacının**, bu maddenin 2. fıkrasının 1. cümlesinin a ile c bendin' den o bendine kadar ve ayrıca 2. ila 10. no'ya kadar belirtilen **çok ağır suçları mümkün kılmayı veya işlemeyi amaçlaması koşuluyla**, Alman Ceza Kanunu'nun 127. maddesinin 3. ve 4. fıkraları kapsamında **internette suç teşkil eden ticaret platformlarının işletilmesi,***
*c) Alman Ceza Kanunu 129/1 maddesinde yer alan **suç örgütü kurma suçu**, 5. fıkra 3. cümlesi ile bağlantılı olduğu hallerde ve 129a/1, 2, 4, 5 cümle 1, birici seçenek, her halde 129b/1 ile bağlantılı olan **terör örgütü kurma suçu**,*
*d) Alman Ceza Kanunun 146 ve 151 inci maddesinde yer alan **parada ve kıymetli evrakta sahtecilik suçları**, her halde 152 inci madde ile bağlantılı olarak ve de 152a/3 ve 152b/1 ila 4 de düzenlenen suçlar,*
*e) Alman Ceza Kanunun 176/1, 176c, 176d ile 177/6, cümle 2 no. 2 de sayılan **cinsel özgürlüğe karşı işlenen suçlar**,*
*f) Alman Ceza Kanunun 184b/3 1. cümlesi ile 184b/2 maddelerinde düzenlenen **çocuk pornografisi içeren yazıları yayma, edinme ve bulundurma suçu**,*
*g) Alman Ceza Kanununun 211. ile 212. maddelerinde yer alan **nitelikli kasten insan öldürme suçu ile kasten insan öldürme suçu,***
*h) **Kişi hürriyetine karşı işlenen suçlar** (232/2, 3, 232a/1, 3, 4 ile 5. fıkranın ikinci yarı cümlesi, 232b/1, 3, 4. cümlenin 232a/ 4, 5. fıkranın ikinci yarı cümlesi ile bağlantılı olarak, 233/2, 233a/1, 3, 4. fıkranın 2. yarı cümlesi, 234 ile 234a/1, 2, 239a ve 239b,*
*i) **Çete halinde işlenen hırsızlık suçu** (244/1, 2. cümle) **ve çete halinde işlenen ağır hırsızlık suçu** (244a),*
*j) **Nitelikli yağma ve ölümle neticelenen yağma** (250/1 veya 2, § 251),*
*k) Madde 253/4 cümle 2 de belirtilen koşullar altında m. 255 uyarınca işlenen **yağma amaçlı şantaj** ve m. 253 uyarınca **şantajın nitelikli şekli**,*
*l) Madde 260 ve 260a uyarınca **Meslek haline getirilmiş bir şekilde işlenen suçtan elde edilen malı satın alma, çete halinde işlenen yataklık suçu ve meslek haline getirilmiş çete halinde işlenen yataklık suçu**,*
*m) **Öncül suçun** bu maddenin 2. fıkrasının 1 ila 7 cümlelerinde listelenen **ağır suçlardan biri olması halinde**, Madde 261/5 cümle 2 de belirtilen koşullar altında 261. Madde uyarınca **işlenen karapara aklama suçunun çok ağır hali** (261),*
*n) Madde 263a/2 ila bağlantılı olarak madde 263a/5 kapsamındaki hallerde **bilgisayar dolandırıcılığı,***
*o) 335/2 No. 1 ila 3 de belirtilen koşullar altında işlenen ve 335/1 maddede düzenlenmiş olan **rüşvet alma ve rüşvet verme suçlarının çok ağır hali**,*
2. İltica Kanunundan;
*a) **Hakkın kötüye kullanılmasına yönlendirici nitelikte iltica dilekçesi düzenleme suçu** (m. 84/3),*
*b) **Kazanç getirecek ve örgütlü olarak işlenen hakkın kötüye kullanılmasına yönlendirici nitelikte iltica dilekçesi düzenleme suçu** (m. 84a/1),*
3. İkamet Kanunundan;
*a) **Yabancıları kaçak olarak yurda sokma suçu (göçmen kaçakçılığı)** (m. 96/2),*
*b) **Ölüm neticesi doğuran göçmen kaçakçılığı ve meslek haline getirerek ve örgütlü olarak işlenen göçmen kaçakçılığı suçu** (m. 97),*
4. Dış Ticaret Kanunundan:
*a) 17/1, 2 ve 3 maddelerinde ve ayrıca bunlarla bağlantılı olarak ta 17/6 veya 17/7 maddelerinde **belirtilen suçlar,** (örneğin yabancı bir gücün gizli servisi için hareket edilmesi veya ticari olarak veya*

bu tür eylemleri gerçekleştirmeye devam etmek için bir araya gelen bir çetenin üyesi olarak hareket edilmesi),

b) 18/7 ve 18/8 maddelerinde belirtilen suçlar ve ayrıca bunlarla bağlantılı olarak ta 18/10 maddelerinde ***belirtilen suçlar****, (örneğin Avrupa Birliği Konseyi tarafından ortak dış politika ve güvenlik politikası alanında kabul edilen bir ekonomik yaptırım önleminin uygulanması amacıyla Avrupa Toplulukları veya Avrupa Birliği Resmi Gazetesi'nde yayınlanan Avrupa Toplulukları veya Avrupa Birliği'nin doğrudan uygulanabilir bir yasasına aykırı olan ihracat, ithalat, transit, devir, satış, iktisap, tedarik, devir veya yatırım yasağı veya yayın, iletim, dağıtım veya diğer hizmet sunumu yasaklarına veya dondurulan fonların ve ekonomik kaynakların elden çıkarılması yasaklarına aykırı hareket edilmesi),*

5. Uyuşturucu Maddeler Kanunundan:

a) 29/3 cümle 2 no. 1 maddede belirtilen koşullar altında 29/1 cümle 1, No. 1, 5, 6, 10, 11 veya 13, fıkra 3 de ***belirtilen suçların çok ağır halleri,*** *(örneğin ticari olarak hareket etmek suretiyle izinsiz olarak uyuşturucu madde yetiştirilmesi, üretilmesi, ithal edilmesi, ihraç edilmesi, satılması, dağıtılması, başka bir şekilde piyasaya sürülmesi, iktisap edilmesi; ticari olarak hareket etmek suretiyle uyuşturucu maddelerin izinsiz olarak edinilmesi veya başka bir kişiye dağıtılması için bir fırsat sağlanması, bu fırsatı alenen veya bencilce iletilmesi veya başka bir kişinin izinsiz olarak uyuşturucu madde kullanmaya teşvik edilmesi),*

b) 29a, 30/1 No. 1, 2 ve 4 ile 30a maddelerde ***belirtilen suçlar,*** *(örneğin 21 yaşından büyük bir kişi olarak 18 yaşın altındaki bir kişiye izinsiz olarak narkotik uyuşturucu temin edilmesi, ona uygulanması veya doğrudan tüketmesi için kendisine bırakılması; az miktarda olmayan uyuşturucu kaçakçılığı, bunların az olmayan miktarlarda üretilmesi veya dağıtılması yada izinsiz bir şekilde elde bulunması)*

6. Savaş Silahlarının Kontrolü Hakkında Kanundan;

a) 19/2 veya 20/1 maddedeki suçlar, m. 21 ile bağlantılı olarak ta, (Nükleer Silahlara Karşı Cezai Hükümler, Biyolojik ve Kimyasal Silahlara Karşı Cezai Hükümler),

b) 22a/1 maddede ***belirtilen suçların*** *2 inci fıkra ile bağlantılı olarak* ***çok ağır hali,*** *(örneğin ruhsatsız olarak savaş silahlarının imal edilmesi; ithalat, ihracat, Federal Cumhuriyet topraklarından transit geçiş veya gerekli nakliyeye izin verilmeden Federal Almanya Cumhuriyeti topraklarının dışına savaş silahlarının taşınması gibi hukuka aykırı fiiller bakımından kişinin ticari olarak veya başka bir çete üyesinin işbirliğiyle bu tür suçları işlemek için bir araya gelen bir çetenin üyesi olarak hareket etmesi durumu),*

7. Temel Maddelerin İzlenmesi Kanunundan *(=Uyuşturucu Maddelerin Yasadışı Üretimi için Kötüye Kullanılabilecek Hammaddelerin Ticaretinin İzlenmesine İlişkin Kanun)*

19/3 de ***belirtilen suçlar*** *(özellikle bir hammaddeye sahip olan, üreten, ticaretini yapan, ithal eden, ihraç eden, bu Yasanın uygulama alanı içinde veya bu Yasanın uygulama alanı içinde taşıyan, satan, devreden veya başka bir kişinin fiilen elden çıkarma olanağını açan, edinen veya başka bir şekilde temin eden kişinin ticari veya bu tür eylemleri gerçekleştirmeye devam etmek için güçlerini birleştiren bir çetenin üyesi olarak bunları gerçekleştirmesi.)*

8. Yeni Psikoaktif Maddeler Kanunundan:

4/3 no. 1 de ***belirtilen suçlar*** *(yeni bir psikoaktif maddenin kaçakçılığını yapan, pazarlayan veya bir başkasına uygulayan veya piyasaya sürmek amacıyla yeni bir psikoaktif madde üreten veya bu Kanunun Kapsama alanına dahil eden kişinin ticari olarak veya sürekli olarak bu tür suçları işlemek için bir araya gelen bir çetenin üyesi olarak hareket eden veya 21 yaşın üzerindeki bir kişi olarak, 18 yaşın altındaki bir kişiye yeni bir psikoaktif maddenin dağıtılması veya hemen tüketmesi için bu kişiye uygulaması).*

9. Devletler Ceza Kanunundan:

a) ***Soykırım****, m. 6,*

b) ***İnsanlığa karşı suçlar****, m. 7,*

c) ***Savaş suçları****, m. 8 ila 12,*

d) ***Saldırı savaşı suçu****, m. 13*

10. Silâh Kanunundan:

a) 51/1 ila 2 maddede yer alan ***suçların çok ağır*** *hali (kartuşlu mühimmat ateşlemek için bir ateşli silahı edinen, bulunduran, devreden, nakleden, beraberinde götüren, üreten, işleyen, onaran veya ticaretini yapan herhangi bir kişinin ticari olarak veya başka bir çete üyesinin iş birliğiyle bu tür suçları işlemek için güçlerini birleştiren bir çetenin üyesi olarak hareket etmesi durumu)*

b) 52/1 No.1 maddede yer alan suçun, 5 inci fıkra ile ***bağlantılı olarak işlenen çok ağır hali*** *(burada belirtilen bir ateşli silah veya nesneyi edinen, bulunduran, devreden, nakleden, beraberinde götüren, üreten, işleyen, onaran veya ticaretini yapan kişinin ticari olarak veya başka bir çete üyesinin iş*

müdahalesi" olarak tanımlanan online arama tedbiri[649], müdahalenin yoğunluğu itibariyle konutun izlenmesi ile karşılaştırılabileceği ileri sürülmektedir[650]. Bu bağlamda hedef sisteme yüklenen bir arama yazılımının tıpkı bir "program kontrolündeki gizli soruşturmacı" gibi çalıştığı belirtilir[651].

Online arama, öncelikli bir hukuki menfaate yönelik somut bir tehlike olduğuna dair gerçek olguların olması halinde genelde suçların soruşturulması için gerekli olan bütünlük ve gizlilik temel hakkının koruma kapsamına yönelik bir müdahale ile bunun sonucunda ortaya çıkan erişim arasında yer almaktadır[652].

İlgili kişinin kişiliği üzerindeki etkisi bakımından bu erişimin, bilgi edinme temel hakkının koruma sağladığı bireysel veri toplamanın çok ötesine geçmekte olup, iletişim içeriklerinin yanı sıra bir bilgi teknolojisi sisteminde kaydedilen tüm içeriğin ve bir kişinin tüm kullanım davranışının izlenmesi mümkündür. Bu nedenle online arama ile genel kişilik hakkının yansıması ve bilgi edinme konusunda kendi kaderini tayin hakkının bağımsız bir ifadesi olan "bilgi teknolojisi sistemlerinin bütünlüğü ve gizliliği temel hakkının" koruma kapsamına bir müdahale teşkil ettiği anlamına gelmektedir[653]. Çalışmamızın "tarihi gelişimi" inceleyen ikinci bölümde de ifade ettiğimiz gibi, bilgi teknolojisi sistemlerinde kaydedilen veya işlenen kişisel verilerin korunmasını amaçlayan bu temel hak Anayasa da açıkça yer almamaktadır. Federal Anayasa Mahkemesinin 27 Şubat 2008 tarihli online aramanın kabul edilebilirliğine ilişkin kararında, genel kişilik hakkının özel bir biçimi olarak türetilmiştir[654].

---

birliğiyle bu tür suçları işlemek için güçlerini birleştiren bir çetenin üyesi olarak hareket etmesi durumu).
(3) Bu tedbir sadece şüpheli hakkında uygulanabilir. Başka kişilerin bilgi teknolojisi sisteminde bu tedbirin uygulanabilmesi için somut olgulara dayanan aşağıdaki koşulların gerçekleştiğinin kabul edilmesi gerekir:
1. 100e/3. uyarınca verilen kararda tanımlanan şüphelinin başka kişinin bilgi teknolojisi sistemini kullandığı ve
2. Sadece şüphelinin bilgi teknolojisi sisteminde uygulanacak olan tedbir ile maddi olgunun araştırılması veya diğer şüphelilerin ortaya çıkarılmasının sağlanamayacağı kabul edilebiliyorsa.
Bu tedbir, başka kişilerin kaçınılmaz olarak etkilenmesi durumunda da uygulanabilir.
(4) 100a/5 ve 6 maddeleri, 100a/5 cümle 1 no 1 hariç olmak üzere uygulanır. "
[649] Singelnstein/Derin, NJW 2017, 2646, 2647.
[650] BVerfGE 141, 220 Rn. 238.
[651] Freiling/Saffering/Rückert, JR 2018, 9, 16.
[652] BVerfG NJW 2008, 822; BeckOK StPO/Graf StPO §100b Rn. 2.
[653] BVerfGE 120, 274.
[654] BVerfG NJW 2008, 822.

1. Müdahalenin Koşulları

Alman Ceza Muhakemesi Kanunu'nun 100b/1 maddesinde yer alan online aramanın yasal tanımına göre, tedbire maruz kalan kişinin bilgisi olmadan da bu kişi tarafından kullanılan bir bilgi teknolojisi sistemine erişmek ve buradan veri elde etmek için teknik araçlar kullanılabilir.

Bunun için belirli koşulların kümülatif olarak karşılanması gerekmektedir. Bunlar:

Somut olguların bir kişinin fail veya şerik olarak 100b maddesinin 2 inci fıkrasında sayılan çok ağır suçlardan birini islediği veya teşebbüsün cezalandırılabilir olduğu suçlarda bunu işlemeye teşebbüs ettiği şüphesini doğurması, suçun somut olayda da özel bir ağırlık arz etmesi ve maddi gerçeğin araştırılması veya şüphelinin bulunduğu yerin belirlenmesi başka yöntemlerin uygulanması halinde çok daha zor veya faydasız olmasıdır.

Bilgi teknolojisi sistemlerinin kapsamı bakımından, bunun geniş tanımlanarak gerek günümüzde güncel olarak kullanılan gerekse gelecekte kullanılabilecek olan bilgisayar, tablet, cep telefonu ve diğer akıllı sistemleri gibi tüm bilgi teknolojisi cihazlarını içerebileceği gibi belirli işletim sistemleri, giriş yolları, programlama veya özel teknik özellikler belirtmeksizin tüm cihaz ve program türlerini kapsadığını ifade edebiliriz[655].

Kanun koyucunun kullanmış olduğu "tedbire maruz kalan kişinin bilgisi olmasa bile" ifadesi online aramanın ilke olarak gizli bir soruşturma tedbiri olmasına rağmen, ilgili kişilerden birinin veya tamamının izlemeden haberdar olması halinde kabul edilemez hale gelmeyeceğini açıkça ortaya koymaktadır[656]. Ancak kural olarak, ilgili kişinin online arama kararından haberi yoktur[657]. Bu durum, arama yazılımının ilgili kişinin bilgi teknolojisi cihazına gizlice yüklenmesi ve verilerin soruşturma makamı yetkilileri tarafından elde edilmesi için de geçerlidir[658]. Ancak, ilgilinin bilgisi veya rızası tek başına tedbirin yasallığını haklı çıkarmak için yeterli değildir. Zira veri sahibi, online aramadan etkilenebilecek diğer kişiler için de geçerli olmak üzere bir temel hak kısıtlamasına rıza gösteremez[659].

[655] BeckOK StPO/Graf StPO §100b Rn. 8.
[656] MüKoStPO/Rückert StPO §100b Rn. 52.
[657] Soine, NStZ 2018, 498.
[658] Soine, NStZ 2018, 498.
[659] Soine, NStZ 2018, 499.

a. "Nitelikli" suç şüphesinin bulunması

100b I/1'e göre, belirli olguların özellikle ağır bir suçun işlendiği şüphesini doğurması gerekmektedir. Bu doğrultuda online arama yalnızca 100b I/2 de yer alan bir katalog suçuna istinaden geçekleştirilebileceğinden, bu şüphe "nitelikli şuç şüphesi" olarak tanımlanır.

Şüphenin yeterli derecede kanıtlanmış bir olgusal temel aracılığıyla belirli bir somutlaştırma derecesine ulaşmış olması beklenir. Bunun için başlangıç şüphesi yeterli olmayıp, bunu aşan nitelikle bir suç şüphenin varlığı aranır[660]. İçtihata göre, şüphenin yeterli ve kuvvetli nitelikte olması aranmaz[661]. Ancak salt varsayıma dayanan ve tahminden ibaret bulunan şüphenin de yetersiz olduğu ifade edilir. Örneğin tanık ifadelerine, gözlemlere veya başka olgusal kanıtlara dayanan genel yaşam veya suç deneyimine göre, bir kişinin fail veya şerik olarak bir katalog suçu işlediğini veya işlemeye teşebbüs ettiğini önemli ölçüde gösteren somut koşullar aranır[662]. Şüphe, kesin olgusal maddi delillerle belirli bir somutlaştırma ve pekiştirme derecesine ulaşmış olmalı[663]. Ayrıca, şüphenin yeterli bir olgusal temeli olmalı ve önemsiz olmanın ötesine geçmelidir[664].

Buna karşı öğretide bazı görüşler, müdahalenin ciddi boyutu ve özel hayatın çekirdek alanına yakınlığı sebebiyle, online aramanın söz konusu olması halinde suç şüphesine ilişkin gerekliliklerin artırılması, normun anayasaya uygun olarak kısıtlayıcı bir şekilde yorumlanması ve tutuklama tedbiri uyarınca kuvvetli bir suç şüphesinin aranması gerektiği vurgulanmaktadır[665].

Bununla birlikte şüphe özellikle ağır bir suç ile bağlantılı olmalıdır. Bu tür suçlar orta ağırlıktaki suç düzeyini açıkça aşmalıdır[666]. Bir katalog suçu işlemeye teşebbüs de suçu işlemeye teşebbüsün cezalandırılabilir olması halinde yeterlidir[667].

Kanun, nitelikli suç şüphesinin varlığına yönelik kararı vermeye yetkili olan hakime, temyiz mahkemeleri tarafından da gözetilmesi gereken bir takdir yetkisi tanımaktadır[668]. Hakimin kararının tüm hususları ortaya koyması gerekmese de,

---

[660] Köhler in Meyer-Gossner/Schmitt, §100b Rn. 4.
[661] BGH BeckRS 2016, 15673; OLG Hamm BeckRS 2013, 197317; NStZ 2003, 279.
[662] BVerfG NJW 2007, 2752 (2753); Soine, NStZ 2018, 498.
[663] BVerfGE 109, 279, Rn. 247; BVerfGE 100, 313, Rn. 271.
[664] BGHSt 41, 30, 33; BGH BeckRS 2016, 15673.
[665] Knierim/Oehmichen StPO §100b Rn. 71; Kühne, Strafprozessrecht, StPO §100 a Rn. 521.
[666] KK-StPO/Henrichs/Weingast StPO §100b Rn.7.
[667] Köhler in Meyer-Gossner/Schmitt, Rn. 4.
[668]BGHSt 41, 30 (33); BeckOK StPO Graf StPO §100b Rn. 15.

kararın temel dayanağının ve gerekli olan somut olay incelemesinin de en azından ana hatlarıyla belirtilmesi gerekmektedir[669].

b. Somut olayın ağırlığı

100b I/2'ye göre online aramayı gerektiren suçun ayrıca somut olayda özellikle ağır olması gerekmektedir. Bu nedenle, tedbir değerlendirilirken, söz konusu suçun, somut olaydaki katalog suçlarının halihazırda mevcut olan soyut ağırlığına göre de özellikle ağır olup olmadığı incelenmelidir[670].

Bu, ilke olarak suç kataloğunun kapsamına giren, ancak somut olayda yeterli ağırlıkta olmaması nedeniyle online bir arama ile ilişkili bilgi teknolojisi sistemlerinin bütünlüğü ve gizliliği temel hakkının korunmasına yönelik bir müdahaleyi haklı gösteremeyen durumları hariç tutmayı amaçlamaktadır[671].

Suçun ağırlığı, suçun işleniş biçiminden, ilgili yasal çıkarları koruma ihtiyacından, mağdurlara verilen zararın kapsamı ve ciddiyetinden, suça birden fazla potansiyel failin dahil olmasından, diğer katalog suçlarıyla veya organize suçlarla bağlantılarından, örneğin terörist veya aşırılık yanlısı suçlarla ilgili belirli bir motivasyonun bulunmasından kaynaklanabilir[672].

Burada beklenen cezanın bir ölçüt olarak kullanılabileceği savunulmaktadır[673]. Online aramanın ciddi anayasal müdahaleci niteliği göz önünde bulundurulduğunda, bu tedbirin her halükârda somut olarak beş yıllık hapis cezasının altında uygun olmayacağı belirtilmektedir[674].

Ayrıca, ilgili kanunda belirtilen ceza indirimi gerektiren hafifletici haller otomatik olarak göz ardı edilmemeli. Zira bir yandan, soruşturmanın bu aşamasında hafifletici halin kabul edilip edilmeyeceğini tahmin etmek genelde mümkün değildir. Diğer yandan suçun mağdur üzerindeki etkileri o kadar ciddi olabilir ki, bu durum söz konusu suçun özellikle ağır olarak değerlendirilmesine yol açabilir[675].

---

669 LG Rostock StV 2008, 461; BeckOK StPO Graf StPO §100b Rn. 15.
670 MüKOStPO/Rückert, §100b Rn. 49.
671 BeckOK StPO/Graf StPO §100b Rn. 17.
672 Bär in KMR-StPO, §100b Rn. 23.
673 Hauck in Löwe/Rosenberg §100b Rn. 80.
674 Hauck in Löwe/Rosenberg §100b Rn. 80.
675 BeckOK StPO Graf StPO §100b Rn. 18; BT-Drucksache 16/5846, 40.

c. İkincillik ilkesinin uygulanması

100b I/3 gereği online arama ancak soruşturmaya konu olan olayların araştırılmasının veya şüphelinin yerinin tespit edilmesinin başka türlü çok daha zor veya faydasız olduğu hallerde uygulanabilir. Bu düzenlemeyle online aramanın soruşturma tedbirlerinin son çaresi olduğu sonucuna varılır[676]. Dolayısıyla online aramaya yalnızca diğer alternatif koruma tedbirlerinin başarı sağlamadığı veya sağlama ihtimalinin düşük olarak değerlendirildiği hallerde başvurulabilir[677].

2. Müdahalenin Yoğunluğu

Online arama ile ortaya çıkan müdahalenin yoğunluğu, tedbire maruz kalan kişilerin bilgi teknolojisi sistemlerinin izleme olanaklarının kapsamından ortaya çıkmaktadır. Bu sistemler fiilen ölçülemeyecek miktarda veri içermekte ve bunlar genelde bilinçli olarak örneğin özel metin, görüntü ve ses dosyaları gibi yüksek hassasiyete sahip kişisel bilgileri saklamak için kullanılmaktadır[678].

Özellikle de teknolojinin gelişmesiyle birlikte hayatın pek çok alanında bilgi teknoloji sistemlerinin kullanımının artmasının sonucunda oldukça has has kişisel veriler kaydedilmektedir. Bu veriler, ilgili kişilerin kişisel durumları ve yaşam tarzları hakkında ayrıntılı bilgileri, çeşitli iletişim kanalları üzerinden gerçekleştirilen özel ve mesleki yazışmalar ile günlük benzeri, yani son derece kişiselleştirilmiş kayıtları da içerebilir[679].

Veri sahiplerinin gizliliğine güvendikleri veriler yalnızca veri sahiplerinin bilgi teknoloji sistemlerinde değil, üçüncü tarafların sistemlerinde de kaydedilip saklandığı kabul edilmektedir[680]. Devletin böylesine geniş kapsamlı bir veri tabanına erişimi, elde edilen verilerin bir bütün olarak değerlendirildiğinde, davranış ve iletişim profillerinin oluşturulması da dahil olmak üzere, veri sahiplerinin kişilikleri hakkında geniş kapsamlı sonuçlara varılmasına imkân vermesi gibi açık bir riskle ilişkilendirilmektedir[681].

İnternet bağlantısı olan bir bilgisayara sahip olan herkesin, en azından teorik olarak, bu tür bir denetimden etkilenebileceği gerçeği[682] ile özel olarak kullanılan

[676] Köhler in Meyer-Gossner/Schmitt, §100b Rn. 6.
[677] MüKoStPO/Günther §100c Rn. 34; Soine NStZ 2018, 499.
[678] Soine, NStZ 2018, 497.
[679] BVerfGE 120, 274 Rn. 231; BVerfGE 141, 220 Rn. 238.
[680] BVerfGE 141, 220 Rn. 238.
[681] BVerfGE 120, 274, Rn. 232; BVerfGE 141, 220, Rn. 238.
[682] Kemper, ZRP 2007, S. 106.

bilgisayarın "dışarıya aktarılmış bir beyin" gibi olduğu göz önünde bulundurulduğunda, bu önlemin uygulanması halinde devletin bir bilgisayara tek bir erişimle bir vatandaşın neredeyse tam bir imajını elde etme riski bulunmaktadır[683]. Veri korumaya yönelik tehdit, sistemlerin ağ yapısı ve karmaşıklığı ile yüksek kötüye kullanım potansiyeli nedeniyle daha da artmaktadır[684].

Bunun ötesinde, özellikle gizli infiltrasyon yönteminin sistemin uzun süreli izlenmesine ve ilgili verilerin devamlı olarak elde edilmesine olanak sağlaması halinde, elde edilen verilerin kapsamı ve çeşitliliği bu tür bir erişim yoluyla elde edilebilecek verilerin tek seferlik ve seçici veri elde etme yönteminden çok daha fazladır ve temel haklara yönelik müdahale daha ağırdır[685].

Bununla birlikte tedbire maruz kalan kişinin müdahaleden haberdar olmaması sebebiyle devletin gizli erişimini etkileme fırsatının olmaması da müdahalenin ne kadar ciddi olduğuna işaret etmektedir[686].

Ancak ifade edilmelidir ki, kanun koyucunun açığa kavuşturulması istenen ciddi suçlar ve terörizmle ilgili suçlar bakımından bu tedbirin etkinliği hakkında çekinceler de bulunmaktadır. Online arama tedbiri yalnızca bilgi teknolojisi sitemlerinin özel veya devlet "bilgisayar korsanlarından" korunduğuna güvenen ve verilerini "saklamayan" bilişim sistemleri kullanıcıları için başarı vaat etmektedir. Ancak ciddi suç failleri bakımından bunun geçerli olamayacağı, bu kişilerin temkinli davranıp soruşturmayla ilgili verilerin ya şifreleneceği ya da disk veya USB belleği gibi harici veri taşıyıcılarına aktarılacağı ifade edilir[687].

Online aramanın gerçekleştirdiği müdahalenin ciddi boyutta olmadığını destekleyen görüşe göre, bilgi teknolojisi sistemi kullanan kişinin internete girmesi halinde sistemi korumasız ise, bu durumda kendisinin internet trafiğine katılarak verilerini ağ üzerinden genel erişime dolaylı olarak maruz bıraktığı ve bunun sorumluluğunu üstlenmesi gerektiği ileri sürülür. Bu durumda sistem kullanıcısının bilgisayarına virüs bulaştırma riskini göze aldığı[688] ve sanki gönüllü olarak verilerini ilettiği kabul edilir[689]. Bunun neticesinde online arama ile gerçekleşen müdahalenin çok ciddi olmadığı sonucuna varılır. Ancak bu görüşün aksine, burada sistem

[683] Baum/Schantz, ZRP 2008, S. 139.
[684] BVerfGE 120, 274 Rn. 306.
[685] BVerfG Urteil v. 27.02.2008, Rn. 234 f.
[686] Soine, NStZ 2018, 498.
[687] Hartmann in Dölling/Duttge/Rössner, §100b Rn.1; Kutscha, NJW 2007, S. 1172 f.
[688] Hofmann, NStZ 2005, S. 125.
[689] Kemper, ZRP 2007, S. 110; Kutscha, NJW 2007, S. 1171.

kullanıcısının iradesinin dikkate alınması gerektiği, bir kullanıcının örneğin internette gezerken veya e-posta gönderirken bilgi teknolojisi sistemindeki kişisel verilerini ifşa etmek istemeyeceği kanaatindeyiz. Hatta kişinin antivirüs veya firewall yazılımları kullanmak suretiyle güvenlik önlemleri alması halinde, iradesinin kesinlikle kişisel verilerini paylaşmamak ve ifşa etmemek yönünde olduğu kabul edilmelidir.

3. Suç Kataloğu

Federal Anayasa Mahkemesi 100b/2 uyarınca "özellikle ağır suçlar" kataloğunda dikkate alınması gereken online aramanın uygulanmasına ilişkin özellikle katı şartlar getirmiştir. Bu katalog 2021 yılında yürürlüğe giren çeşitli değişikliklerle genişletilmiştir[690].

Online aramanın suç kataloğu Alman CMK m. 100a gereği düzenlenmiş olan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirinin kataloğu ile karşılaştırıldığında, m. 100a da belirtilmiş olan suç kataloğunun sadece "ağır suçları" kapsadığını, online arama tedbirinin suç kataloğunun ise daha dar kapsamlı olduğunu ifade edebiliriz.

Online arama için öngörülen suç kataloğu Alman CMK m. 100c uyarınca düzenlenmiş olan "konutun teknik araçlarla akustik olarak dinlenmesi" tedbiri için de aynı şekilde geçerliliğini korumaktadır[691]. 100c maddesinde kanun koyucu 100b maddesinin suç kataloğuna atıfta bulunmuştur. Bu aynı zamanda kanun koyucunun iki tedbire aynı ölçüde ağırlık verdiğini de göstermektedir[692].

Federal Anayasa Mahkemesi'ne göre kanun koyucu, suçun haksızlığını belirleme ve hangi suçların soruşturma tedbirlerine gerekçe teşkil edeceğine dair karar verme konusunda takdir yetkisine sahiptir. Yasada öngörülen cezanın alt ve üst sınırları bunun için belirleyici bir göstergedir. Federal Anayasa Mahkemesi'nin tanımına göre, üst sınırı en az beş yıl hapis cezasını gerektiren suçlar "özellikle ağır suç" başlığı altında değerlendirilebilir[693]. Suçun temel şeklinin bu koşulu sağlaması halinde, suçun daha az cezayı gerektiren nitelikli hallerinde beş yıldan daha az bir hapis cezası

[690] BGBI. 2020 I 2600, 30.11.2020 tarihli, yürürlüğe girme tarihi 1.1.2021; BT-Drucksache 19/19859;
BGBI. 2021 I 327, 17.03.2021, yürürlüğe girme tarihi 18.03.2021;
BGBI. 2021 I 1810, 22.06.2021, yürürlüğe girme tarihi 1.07.2021;
BGBI. 2021 I 2099, 30.06.2021, yürürlüğe girme tarihi 1.07.2021;
BGBI. 2021 I 3544, 19.08.2021, yürürlüğe girme tarihi 1.10.2021.
[691] Soine, NStZ 2018, Rn. 497.
[692] KK-StPO/Henrichs/Weingast StPO § 100b Rn. 10.
[693] BVerfG, Urteil v. 03.03.2004 – 1 BvR 2378/97, 1084/99, Rn. 235, 238, 241.

öngörülse dahi, bu suçun katalog dışı bırakılmasına bir gerekçe değildir[694]. Bununla birlikte beş yıldan daha yüksek bir azami ceza öngören nitelikli suçların da katalog da sayılmasının anayasa uygun olduğu ifade edilmektedir[695].

100b/2 gereği özellikle ağır suçlardan ne anlaşılması gerektiğini yukarıda zikretmiştik[696].

Özetle, Ceza Kanununda, İltica Kanununda, İkamet Kanununda, Dış Ticaret Kanununda, Uyuşturucu Maddeler Kanununda, Savaş Silahlarının Kontrolü Hakkında Kanunda, Temel Maddelerin İzlenmesi Kanununda, Yeni Psikoaktif Maddeler Kanununda, Devletler Ceza Kanununda ve Silâh Kanununda öngörülmüş özellikle ağır suçlar ile suç kataloğu oluşturulmuş olup, online arama tedbiri bu bahsi geçen özellikle ağır suçlar sebebiyle gerçekleştirilebilir.

Burada dikkat çeken husus, suç kataloğunun insan kaçakçılığı, İkamet, İltica ve Silah Kanunları ihlalleri ve kara para aklama gibi organize suçların tipik faaliyet alanlarını içermesi, dolayısıyla katalog suçlarının büyük bir kısmının organize suçlarla bağlantılı olmalarıdır[697].

Kanun koyucunun ihlal edilen hukuki menfaat ve verilmesi öngörülen ceza açısından özellikle ciddi olan suçları kataloğa dahil ettiği ifade edilse de[698], kataloğun ilgili fiillerin haksızlığı konusunda tutarlı olmaması eleştirilmektedir[699]. Bu bağlamda cürüm ve cünha ayrımı dikkate alınmaksızın, ceza çerçevesi bakımından alt sınırı bir yıldan az hapis cezası veya adli para cezası tehdidi altında olan hukuka aykırı filler olarak tanımlanan çete halinde işlenen hırsızlık, suçtan elde edilen malı satın alma ve kara para aklama suçları gibi cünhaların özellikle ağır suçlar olarak kategorize edilmelerinin doğru olmadığı vurgulanmaktadır. Bunun da kanun koyucunun sadece ilgili suçların ağırlığına göre hareket etmediğini, aynı zamanda katalog suçlarının hayatın belirli alanlarına ve organize suçla mücadeledeki önemlerine göre seçtiğinin bir göstergesi olduğu belirtilmektedir[700].

Bunun ötesinde bu katalogda sayılmış olan tüm suçların özellikle ağır suçlar için anayasal gereklilikleri karşılayıp karşılamadığı öğretide şüpheyle

[694] BVerfG, Urteil v. 03.03.2004 – 1 BvR 2378/97, 1084/99, Rn. 241.
[695] BVerfG, Urteil v. 03.03.2004 – 1 BvR 2378/97, 1084/99, Rn. 241.
[696] Bkz. İkinci Bölüm, II., C.
[697] Hauck in Löwe-Rosenberg, § 100b Rn. 83, 84.
[698] Soine, NStZ 2018, 498.
[699] Hauck in Löwe-Rosenberg, § 100b Rn. 85.
[700] Hauck in Löwe-Rosenberg, § 100b Rn. 85; Kudlich, JR 2003, Rn. 453, 454.

karşılanmaktadır[701]. Federal Anayasa Mahkemesi'nin sadece yaşam, beden, kişi özgürlüğü ve devletin temellerinin veya varlığının ya da insanların varlığının temellerinin etkilendiği ölçüde tehdit altında olan kamu malları gibi önemli yasal menfaatlerin savunulması için önleyici online aramalarına izin verdiği göz önünde bulundurulduğunda, çete halinde işlenen hırsızlık ve kara para aklama suçları gibi malvarlığı ve mülkiyete karşı işlenen suçların ve İltica ve İkamet Kanunu'na karşı işlenen suçlar ile Uyuşturucu Maddeler Kanununda düzenlenmiş olan "ticari uyuşturucu suçlarının" genel olarak bu kapsama alınmasının anayasaya aykırı olduğu ileri sürülmektedir[702]. Bu, bir tehlikeyi önlemek için temel haklara yönelik bir müdahaleye yalnızca Federal Anayasa Mahkemesi tarafından belirtilmiş olan ağır basan önemli yasal menfaatler söz konusu olduğunda izin verilebileceği anlamına gelmektedir. Buradan, önleyici online arama ile ilgili olarak mülkiyet ve malvarlığı gibi yasal menfaatlerin ihlalinin kabul edilmesi gerektiği sonucu çıkmaktadır. Sonuç olarak bu durumun söz konusu yasal menfaatlerin halihazırda ihlal edilmiş olduğu adli amaçlı tedbirler için daha da geçerli olduğu belirtilir[703].

Bununla birlikte online arama için öngörülen suç kataloğun kapsamının oldukça geniş olduğu, diğer müdahaleci tedbir düzenlemelerinin kapsadığı suç kataloglarına kıyasla neredeyse hiçbir önemli sınırlayıcı etkisinin olmadığı eleştirilmektedir[704].

Diğer bir eleştiri konusu ise, online arama suç kataloğunda bulunan suçların yanı sıra bu suçlara teşebbüsün de dahil edilmesidir. Bir suça teşebbüsün, suçun cezai değerini önemli ölçüde azalttığını, bu nedenle "özellikle ağır bir suçun bulunması" kriterinin bir suça teşebbüs halinde karşılanamayacağı ifade edilir[705].

4. Müdahalenin Muhatabı

Online aramaya maruz kalabilecek kişiler Alman CMK m. 100b/3' te düzenleme altına alınmıştır.

[701] Köhler in Meyer/Gossner/Schmtt, § 100b Rn. 7; Eschelbach in Satzger/Schluckebier/Widmaier StPO § 100b Rn. 10; Buermeyer, Gutachterliche Stellungnahme, 11,12.
[702] MüKoStPO/Rückert StPO § 100b Rn. 62; Hauck in Löwe-Rosenberg, § 100b Rn. 86; Eschelbach in Satzger/Schluckebier/Widmaier StPO § 100b Rn. 11.
[703] Buermeyer, Gutachterliche Stellungnahme, 11,12; Kruse/Grzesiek, S. 347.
[704] Hauck in Löwe-Rosenberg, § 100b Rn. 83.
[705] Kruse/Grzesiek, S. 348.

a. Şüpheli

Alman CMK m. 100b/3-1 gereği online arama kural olarak sadece şüpheli hakkında uygulanabilir. Bu bağlamda şüpheli, bir suç işlediğinden şüphelenilen ve hakkında soruşturma başlatılmış olan ya da online arama tedbiri uyarınca bir karar ile hakkında soruşturma başlatılacak olan kişidir. Şüphelinin kimliği tespit edilmeli, ancak şüphelinin ismen bilinmesi gerekmediği, kimliğinin belirlenebilir olması gerektiği anlamına gelir[706].

Düzenleme şüphelinin bilgi teknolojisi sistemi üzerindeki hakkına ilişkin bir koşul getirmediğinden, söz konusu sistemin kiralanan veya ödünç verilen bir cihaz olabileceği gibi bulunan veya çalınan bir cihaz da olabileceği kabul edilmektedir. Burada belirleyici etken, sistemin soruşturma ile ilgili dönemde kesin kullanım için sanığa tahsis edilmiş olmasıdır[707].

Online aramanın şüpheliye karşı uygulanabilmesi için, şüphelinin illa bilgi teknolojisi sisteminin başında olması şartı aranmamaktadır. Bu nedenle online aramanın şüphelinin bilgisayarı başında bulunmaması halinde de gerçekleştirilebileceği, hatta şüphelinin bilgisayar başında oturmamasının avantaj sağlayabileceği, zira aksi takdirde şüphelinin izlemeye işaret edebilecek olası fare hareketlerini ya da ekran etkinliğini fark edebileceği ifade edilmektedir[708].

b. Diğer Kişiler

Bununla birlikte Alman CMK m. 100b/3-2 uyarınca başka kişilerin bilgi teknolojisi sisteminde de online arama tedbiri uygulanabilir. Bunun için somut olgular şüphelinin başka kişinin bilgi teknolojisi sistemini kullandığını ve sadece şüphelinin bilgi teknolojisi sisteminde uygulanacak olan tedbir ile maddi olgunun araştırılması veya diğer şüphelilerin ortaya çıkarılmasının sağlanamayacağını göstermelidir. Bu gereklilik, özellikle şüphelinin kendi cihazlarında suçun izlerini önlemek için diğer kişi veya üçüncü tarafların bilgi teknolojisi sistemlerini bilinçli olarak kullanması halinde karşılanacaktır.

[706] BGH 12.12.1996 – 4 StR 499/96 – NStZ 1997, 294.
[707] KK-StPO/Henrichs/Weingast StPO § 100b Rn. 12.
[708] BeckOK StPO/Graf StPO § 100b Rn. 24.

Buna göre, diğer kişinin suçun faili veya şeriki olmadığını ve bilgi teknolojisi sistemini gönüllü olup olmaması fark etmeksizin şüphelinin kullanımına bıraktığını ifade edebiliriz[709].

Diğer kişi olarak adlandırılabilecek üçüncü bir tarafın bilgi teknolojisi sistemi, bu üçüncü tarafın kendi sistemi olarak kullandığı herhangi bir bilgi teknolojisi sistemi olabilir. Bu durum, üçüncü tarafın sistemdeki verileri işlerken ve kaydederken sanki sadece kendisinin sisteme erişimi varmış ve diğer kişileri sistemin kullanımından menedebilirmiş gibi davranması halinde kabul edilir[710]. Alman Medeni Kanun'u (BGB) uyarınca mülkiyet veya zilyetlik haklarının bu bağlamda önemi bulunmamaktadır. Buna göre, şüpheli tarafından basit bir ortak kullanım, üçüncü bir tarafın BT sisteminin kullanımı için yeterlidir[711].

Diğer kişiler aile üyeleri, komşular veya arkadaşlar olabileceği gibi, örneğin şantaj veya rehin alma mağduru gibi katalog suçun bizzat mağduru da olabilir[712].

Ayrıca bulut bilişim sağlayıcıları da şüphelinin buluta bağlı bir bilgi teknolojisi sistemi kullandığını gösteren belirli olguların bulunması halinde diğer kişiler olarak kabul edilmektedir[713]. Bu örneğin bir bulut sağlayıcısının ilgili kişiye gönderilen, yüklemenin başarılı olduğunu onaylayan veya sağlanan depolama alanının kullanım kapsamı hakkında bilgi sağlayan kayıtlı e-postalar olabilmektedir[714].

Üçüncü taraf bilgi teknolojisi sistemi olarak bir diğer kullanım alanı ise şüphelilerin internet kafelerinden faydalanması düşünülebilir. Ölçülülük ilkesi bakımından, internet kafelerde yapılan online arama, mümkünse, sunucunun ya da bilgisayarın bizzat şüpheli tarafından kullanılan bölümleriyle sınırlı tutulmalıdır. Bir internet kafenin tüm sunucusunun ya da tüm bilgisayarlarının izlenmesi gerekiyorsa, bunun ancak katı ölçülülük gözetilmesi ve öldürme ile savaş suçları gibi çok ağır suçların söz konusu olması halinde mümkün olabileceği ifade edilmektedir[715].

[709] BeckOK StPO/Graf StPO § 100b Rn. 26; Soine, NStZ 2018, 499.
[710] MüKoStPO/Rückert StPO § 100b Rn. 65.
[711] Freiling/Saffering/Rückert JR 2018, 14.
[712] LG Ulm StV 2006, 8; BVerfGE NJW 2007, 2752, 2753; Meyer-Gossner/Schmitt § 100a Rn.19.
[713] KK-StPO/Henrichs/Weingast, StPO § 100b Rn. 4, 13; Roggan, StV 2017, 826.
[714] Soine, NStZ 2018, 499, 500.
[715] Freiling/Saffering/Rückert JR 2018, 14.

Bununla birlikte Alman CMK 100b/3-3 maddesi, online arama tedbirinin başka kişilerin kaçınılmaz olarak etkilenmesi durumunda da uygulanabileceğini düzenleme altına almıştır.

Sistematik sebeplerden dolayı, bu anlamda diğer kişiler ne şüpheli ne de yukarıda belirttiğimiz kapsamdaki bilgi teknolojisi sistemlerinin üçüncü taraf sahipleridir. Birçok durumda online aramayla ilgili, özellikle de şüphelinin bilgi teknolojisi sistemi üzerinden başka kişilerle iletişim kurması halinde, bu başka kişilerin de verileri sisteme kaydedilmektedir[716]. Bu kişilerin soruşturma konusu olan suç ile ilgileri bulunmasa da örneğin şüpheli ile sosyal medya bağlantıları bulunabilir veya şüphelinin bilgi teknolojisi sistemini tesadüfi bir nedenle kullanmış olabilirler[717]. Bu hüküm online aramanın temel haklara ne kadar ciddi bir müdahale teşkil ettiğini göstermektedir, zira şüphelinin bilgi teknolojisi sisteminde bulundurduğu tüm sosyal bağlantıların potansiyel olarak etkilenmesi ve buna ek olarak geçmişe ait kaydedilmiş tüm iletişim içeriklerine erişim de mümkündür[718]. Bu bağlamda, online aramanın çevrimdışı davranış alanına da uzandığı ifade edilir. Zira, bir bilgisayarda depolanan ve online arama için erişilebilir olan ve soruşturma makamlarının potansiyel olarak ilgisini çekebilecek tüm verilerin aynı zamanda görüntü dosyalarını da içermesi ve bunun da şüpheliyle birlikte resmedilen kişileri yetkililerin bakış açısından potansiyel olarak dikkat çekici hale getirebilmesi eleştirilmektedir[719]. Örneğin bir akıllı telefon kamerası aracılığıyla çekilen bir kişinin anlık görüntülerinin bir sosyal ağda yayınlanması ve beğeniler ile yorumlar da dahil olmak üzere çoklu paylaşımın söz konusu olması halinde, bu adımların her biri herhangi bir katılımcının veya hatta olaya karışmamış üçüncü kişilerin cihazlarının online arama için potansiyel bir erişim noktası temsil edebileceği eleştirilerek belirtilmektedir[720].

İfade edilmelidir ki, kanun, kaçınılmazlığın ne zaman söz konusu olduğunu belirtmemektedir. Bu nedenle üçüncü taraflar üzerindeki etkisi, bir ölçülülük kriteri olarak somut olay bazında değerlendirilmelidir. Ancak, üçüncü taraflar üzerindeki kaçınılmaz etkinin, ölçülülük kapsamında oldukça anlamsız bir özellik olduğu ileri sürülmektedir. Zira, online arama kararı verildiğinde, üçüncü tarafların etkilenip

[716] MüKoStPO/Rückert StPO § 100b Rn. 68.
[717] Soine, NStZ 2018, Rn. 500.
[718] Köhler in Meyer-Gossner/Schmitt, § 100b Rn.11.
[719] KriPoZ 1/2019, S. 25.
[720] KriPoZ 1/2019, S. 25.

etkilenmeyeceğini tahmin etmenin genellikle imkânsız olduğu belirtilmektedir[721]. Ölçülülük denetimi yoluyla üçüncü taraflar üzerindeki etki dikkate alınacaksa, bu durum potansiyel bir etkinin düzenli olarak sadece bir öngörü kararının parçası olarak üstünkörü bir şekilde ele alınacağı anlamına gelmektedir. Bu bakımdan, tedbir uygulanmadan önce gerçek bir değerlendirme için bilgi eksikliği söz konusu olacaktır. Kaçınılmazlık genellikle bir sistem araştırıldığında, üçüncü tarafların verileri de dahil olmak üzere orada depolanan tüm verilerin etkilenmesi gerçeğinden kaynaklanır. Bu nedenlerle, üçüncü tarafların kaçınılmaz olarak etkilenmesi özelliği, tedbirin kapsamının sınırlandırılması veya ölçülülüğün sağlanması için uygun olarak değerlendirilmemektedir[722].

c. Üçüncü tarafların olası iş birliği yükümlülüğü

Kanun koyucu, online arama için bir bilgi teknolojisi sistemine gizli erişimi şart koşsa da telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinin aksine, online arama için telekomünikasyon hizmet sağlayıcıları gibi, bilgi teknolojisi hizmet sağlayıcıları bakımından bir iş birliği yapma yükümlülüğü getirmemiştir[723]. Bunun neticesinde soruşturma makamları internet veya telekomünikasyon sağlayıcıları ile koordinasyon sağlamadan sisteme sızma yöntemlerinden faydalanmalıdır.

Üçüncü tarafların olası iş birliği yükümlülüğüne yönelik Stuttgart Yüksek Bölge Mahkemesi 19.05.2021 tarihinde karar vermiştir[724]. Bu karara göre, Alman CMK m. 100b gereği öngörülen online aramanın, örneğin bir bulut hizmeti sağlayıcısı gibi bir bilgi teknolojisi hizmet sağlayıcısının sunucusunda depolanan üçüncü bir tarafın verilerini teslim etmeye ve bu konuda gizliliği korumaya zorlamak için bir yetki temeli oluşturmadığını açıklamıştır. Bunun gerekçesi olarak, online arama tedbiri bakımından özellikle bir iş birliği yükümlüğüne dair bir hükmün bulunmaması gösterilmektedir[725]. Mahkeme, savcılığın gerekçelerinin aksine, online arama kapsamında teknik bir sızmadan daha hafif bir tedbir olarak üçüncü bir tarafın iş birliği yapma yükümlülüğüne hükmedilmesini uygun görmeyip, bunun bir eksi olarak değil,

[721] Hauck in Löwe-Rosenberg § 100b StPO Rn. 117.
[722] Hauck in Löwe-Rosenberg § 100b StPO Rn. 117.
[723] Knierim/Oehmichen, Kapitel 20 – Quellen-TKÜ und Online-Durchsuchung, Rn. 77.
[724] OLG Stuttgart, Beschl. V. 19.05.2021 – 2 Ws 75/21.
[725] Beckmann, OLG Stuttgart: Herausgabe von auf Server gespeicherten Daten eines Dritten und Verpflichtung zur Verschwiegenheit keine Onlinedurchsuchung nach § 100b StPO und unzulässig, Erişim: OLG Stuttgart: Herausgabe von auf Server gespeicherten Daten eines Dritten und Verpflichtung zur Verschwiegenheit keine Onlinedurchsuchung nach § 100b StPO und unzulässig (beckmannundnorda.de), Erişim tarihi: 01.06.2024.

aksine bir artı olarak değerlendirilmesi gerektiğini vurgulamıştır. Bununla birlikte mahkeme, online arama düzenlemesinin üçüncü taraflarla olan ilişkiyi kapsamadığını, yalnızca devlet soruşturma makamları ile şüpheliler arasındaki ilişkiyle ilgili olduğunu belirtmektedir. Kanun koyucunun, üçüncü tarafların haklarına online aramada öngörülenin ötesinde müdahale etmeyi ve örneğin onları iş birliğine zorlamayı istemesi halinde, bunun yalnızca anayasal nedenlerle açık bir düzenleme gerektireceğini belirtmektedir.[726]

5. Yükümlülükler

Alman CMK m. 100b/4 gereği, m. 100a/5 ile m. 100a/6 uyarınca telekomünikasyon yoluyla iletişimin denetlenmesi tedbirine uygulanan teknik güvenlik ile rapor tutma hükümleri online aramanın uygulanmasında aynı şekilde geçerlidir. Yalnızca kaynak telekomünikasyon yoluyla iletişimin denetlenmesi için geleneksel telekomünikasyon gözetimi ile işlevsel eşdeğerliğin sağlanmasına ilişkin özel gereklilik içeren m. 100a/5-1 No. 1 hariç tutulmuştur.

Özellikle, bilgi teknolojisi sisteminde yalnızca veri toplama için gerekli olan ve tedbirin sonunda teknik olarak mümkün olduğu ölçüde otomatik olarak eski haline getirilecek değişikliklerin yapılması teknik olarak sağlanmalıdır.

Bununla birlikte, teknik araçların her kullanımında belirli hususların kaydedilmesi özellikle hüküm altına alınmıştır. Bu doğrultuda kapsamlı belgelendirme özellikle bir tedbirden önceki adımları, uygulama sürelerini, teknik araçları ve elde edilen verilerin ayrıntılarını anlaşılır kılmalıdır.

a. Teknik güvenlik önlemleri alma yükümlülüğü

Teknik güvenlik önlemleri alma yükümlülüğü, bilgi teknolojisi sisteminde yalnızca veri elde etmek için gerekli olan (Alman CMK m. 100a/5-1 No.2) ve tedbirin sonunda teknik olarak mümkün olduğunca otomatik olarak geri döndürülen değişikliklerin yapılmasının sağlanmasını kapsamaktadır (Alman CMK m. 100a/5-1 No.3).

Bu düzenlemenin tedbire maruz kalan kişi tarafından kullanılan bilgi teknolojisi sistemine müdahaleyi gerekli olan mutlak asgari düzeyde sınırlandırmak

[726] Müller/Schlothauer/Knauer, § 50 Cybercrime und Datenkriminalitaet, Rn. 300.

ve veri güvenliğini sağlamak amacıyla ölçülülük ilkesinin bir yansımasını temsil ettiği ifade edilir[727].

Zira online aramanın gerçekleştirilebilmesi için bilgi teknolojisi sistemine teknik araçlar kullanmak suretiyle sızılması gerekmektedir. Ancak günümüzde bilgisayarlar genellikle koruyucu önlemler yükleyen çeşitli anti-virüs ve internet koruma programları ile donatılmıştır. Bir katalog suçu şüphesini destekleyen verileri aramak amacıyla sistemin bağlı olduğu veri ağları üzerinden online bir arama sırasında sisteme sanal olarak gizlice girebilmek için bahsedilen güvenlik duvarlarının aşılması gerekmektedir[728]. Teknik olarak bu, çalışmamızın birinci bölümünde de ele aldığımız gibi, ya yazılım modifikasyonu yöntemiyle sisteme sızma bakımından internet sağlayıcıların manipülasyon girişimlerinden (web sitelerinin özellikle manipüle edilmesi suretiyle) faydalanılması ya da doğrudan sistemdeki güvenlik açıklarının dikkate alınarak ilgili açığa göre uyarlanmış ve soruşturulan kişinin yardımını gerektirmeyen özel yazılımların kullanılması suretiyle yapılabilir.

Bilgi teknolojisi sistemlerinin bu şekilde manipüle edilmesi, müdahale sırasında dikkate alınacak teknik güvencelere tabidir[729]. Bu bağlamda bilgi teknolojisi sisteminde yalnızca veri elde etmek için gerekli olan tedbirlerin uygulanmasına olanak tanınmıştır. Bununla birlikte yapılan tüm değişiklikler, teknik olarak mümkün olduğu ölçüde tedbirin sonunda otomatik olarak kaldırılmalıdır. Dolayısıyla bilgi teknolojisi sistemi mümkün olduğunca eski hale getirilmelidir.

Bunun sonucunda tedbire maruz kalan kişinin bilgi teknolojisi sistemlerinin gizliliğinin ve bütünlüğünün garanti altına alınması temel hakkına müdahale sonlandırılmış olacaktır. Bunun dışında bu önlem aynı zamanda kullanılan soruşturma yönteminin yetkisiz erişimden korunmasına da hizmet eder[730]. Ayrıca bilgi teknolojisi sistemine yüklenmiş olan yazılımların kötü niyetli kişilerin amaçları doğrultusunda kullanılarak bu sistemlere saldırılması önlenmek istenir[731]. Bunun ötesinde, bilgi teknolojisi sisteminin işlevselliğinin kalıcı ve önemli ölçüde bozulması halinde de yapılan değişikliklerin geri alınması gerekmektedir[732].

[727] BT-Drucksache 18/12785, 53.
[728] BeckOK StPO/Graf StPO §100b Rn. 30.
[729] BeckOK StPO/Graf StPO §100b Rn. 30.
[730] Soine, NStZ 2018, Rn. 502.
[731] Eschelbach in Satzger/Schluckebier/Widmaier StPO § 100b Rn. 26; Soine, NStZ 2018, Rn. 502; BeckOK StPO/Graf StPO §100b Rn. 31.
[732] Soine, NStZ 2018, Rn. 502.

Teknik güvenlik önlemleri alma yükümlülüğü, soruşturmacıların yalnızca bu müdahale için gerekli seçeneklerle sınırlı olan ve bu nedenle amaçlanan veri toplama için gerekli olan yazılımı kullanabileceği anlamına gelmektedir (Alman CMK m. 100a/1-1 No.2).

Teknik olarak mümkün olduğu ölçüde, veri toplama sonrasında değişikliklerin geri alınması bakımından, geri alma işlemi otomatikleştirilmelidir. Bu, kullanılan yazılımın, önlem tamamlandıktan sonra aramayı gerçekleştiren kişinin komutuyla kendini kaldırabilmesi gerektiği anlamına gelir[733]. Bunun ötesinde, yapılan değişikliklerin manuel olarak geri alınması zorunluluğu kanunda yer almamaktadır[734]. Ayrıca kullanılan teknik araçların, yani arama yazılımının, en son teknolojiye uygun olarak yetkisiz kullanıma karşı korunması gerektiği hüküm altına alınmıştır (Alman CMK m. 100a/5-2). Böylelikle kanun koyucunun online aramayı talep eden otoriteye teknik araçların yetkisiz kişiler tarafından yasadışı olarak kullanılması için bir tür garantörlük yükümlülüğü getirdiği ifade edilmektedir[735].

Son olarak, veri ve delil korumasının sağlanması için, kopyalanan verilerin değiştirilmeye, yetkisiz silinmeye ve yetkisiz erişime karşı teknolojinin son gelişmelere uygun olarak korunmasını sağlamak için özen gösterilmelidir (Alman CMK m. 100a/5-3).

b. Rapor tutma yükümlülüğü

Teknik araçların kullanımında, tedbire maruz kalan kişinin haklarının etkili bir şekilde korunmasını ve mahkemede toplanan delillerin güvenilirliğini sağlamak için özel raporlama düzenlemelerine uyulmalıdır[736].

Alman CMK m. 100a/6 uyarınca genel olarak her teknik aracın kullanımında belirli bilgilerin belgelendirilmesi gerektiği hüküm altına alınmıştır. Bunlar;

1. teknik aracın adı ve kullanım zamanı,
2. bilgi teknolojisi sisteminin tanımlanması ve üzerinde yapılan geçici olmayan değişiklikler,
3. elde edilen verilerin tanımlanmasını sağlayan bilgiler,
4. tedbiri gerçekleştiren organizasyonel birim hakkındaki bilgilerdir.

[733] BeckOK StPO/Graf StPO §100b Rn. 31.
[734] Soine, NStZ 2018, Rn. 502.
[735] BeckOK StPO/Graf StPO §100b Rn. 32.
[736] Soine, NStZ 2018, Rn. 502; BeckOK StPO/Graf StPO §100b Rn. 34.

Bu bilgilerin raporlanması, yasal koruma olasılığı açısından olumlu karşılanmaktadır[737].

Kullanılan teknik araçların belgelenmesi sayesinde müdahalenin uygulanma şekli ile kapsamı geriye dönük olarak her an izlenebilir. Kullanım zamanının raporlanması ise müdahalenin ve veri tabanının zaman içinde belirli, açık bir zamana tahsis edilmesini mümkün kılar[738].

Bilgi teknolojisi sisteminin tanımlanması için raporlanan bilgiler daha sonra bu sistemin gerçekten önlemin hedefi olup olmadığını kontrol etmek için kullanılabilir. Sistemin üzerinde yapılan geçici olmayan değişikliklerin belirlenmesi, bir yandan sistemin ve dolayısıyla muhtemelen veri tabanının da etkilenip etkilenmediğini, öte yandan, üçüncü tarafların sisteme yönelik müteakip saldırıları durumunda, bunların yapılan değişikliklerle desteklenip desteklenmediği veya etkinleştirilip etkinleştirilmediği kontrol etmeyi mümkün kılar[739].

Elde edilen verilerin tanımlanmasını sağlayan bilgilerin raporlanması bir müdahalenin olası hukuka aykırılığının daha sonra tespit edilmesi açısından önemli olabilir. Bunun dışında ele geçirilen verilerin müdahalenin hedefi olup olmadığının belirlenmesi konusunda da bu raporlama önem teşkil edebilir[740].

Tedbiri gerçekleştiren organizasyonel birim hakkındaki bilgiler bir yandan tedbire tanıklık edenlerin daha ayrıntılı olarak belirlenmesini, diğer yandan da tedbiri uygulayan birimin sorumluluğunun tespit edilmesini mümkün kılmaktadır[741].

Son olarak, özel hayatın çekirdek alanına ilişkin bulguların elde edilmesi ve ardından uygun şekilde silinmesi halinde, bu bulguların da Alman CMK m. 100d/2-3 uyarınca belgelenmesi ve böylece bir silme kaydının dosyada tutulması gerekir. Bunun amacı, ilgili kişinin tüm süreç boyunca tedbirin yasallığını kontrol edebilmesini sağlamaktır[742].

c. Verileri silme yükümlülüğü

Online arama sırasında tespit edilen verilerin silinmesi "Gizli tedbirlere ilişkin usul düzenlemeleri" başlıklı Alman CMK m. 101/8 uyarınca gerçekleşir. Buna göre, tedbir yoluyla elde edilen kişisel verilerin, ceza soruşturması ve tedbirin herhangi bir

[737] Park, 2022, Rn. 927.
[738] BeckOK StPO/Graf StPO §100b Rn. 36; Soine, NStZ 2018, Rn. 503.
[739] BeckOK StPO/Graf StPO §100b Rn. 37; Soine, NStZ 2018, Rn. 503.
[740] BeckOK StPO/Graf StPO §100b Rn. 38.
[741] BeckOK StPO/Graf StPO §100b Rn. 39.
[742] BT-Drucksache 18/12785, 56.

yargısal denetimi için artık gerekli olmadığı hallerde, derhal silinmesi gerekir. Silme işlemi kayda geçirilmelidir. Silme işlemi yalnızca tedbirin olası bir yargısal denetimi için ertelendiği sürece, veriler yalnızca veri sahiplerinin rızası olmadan bu amaç için kullanılabilir. İşlemleri buna göre kısıtlanmalıdır.

d. Bilgilendirme yükümlülüğü

Alman CMK m. 101/1, 101/4-1 No. 4, tedbire maruz kalan kişiyi ve önemli ölçüde etkilenen kişileri 100b maddesi uyarınca alınan online arama tedbiri konusunda bilgilendirmek ve müteakiben başvurulabilecek kanun yollarını ve bunun için öngörülen süreyi belirtmekle yükümlü kılmaktadır.

İşlevsel açıdan, bildirim savcılığın sorumluluğundadır[743]. Ancak Alman CMK m. 101/4-No.4 gereği tedbirden etkilenen kişilerin korunmaya değer menfaatleriyle çatışması halinde bildirim ertelenebilir. Bu durumda ertelemenin nedenleri kayda geçirilmelidir. Soruşturma açısından taktiksel nedenler tedbirden etkilenen kişinin korunmaya değer menfaatlerini teşkil etmez. Bunun yerine, bildirimin ilgili kişinin yasal menfaatlerine yönelik ciddi bir tehdit oluşturması gerekir[744].

Alman CMK m. 101/5 gereği, bildirimin, soruşturmanın amacını, bir kişinin hayatını, fiziksel bütünlüğünü, kişisel özgürlüğünü ve önemli mal varlığını tehlikeye atmadığı hallerde mümkün olan en kısa sürede yapılır.

Bununla birlikte Alman CMK m. 101/6 uyarınca ertelenen bildirimin tedbirin bitiriminden itibaren on iki ay içinde yapılmadığı hallerde, ertelemenin devam edilmesi için mahkeme onayı gerekir. Bu durumda mahkeme devam eden ertelemenin süresini belirler. Bildirim için koşulların büyük ihtimalle gelecekte de karşılanmayacağı düşünülürse, mahkeme bildirimden nihai olarak feragat etmeyi kabul edebilir.

6. Sınırları

a. İçerik bakımından

Alman CMK m. 100b uyarınca online arama tedbiri ile tedbire maruz kalan kişinin bilgi teknolojisi sisteminde kaydedilmiş tüm verilere erişim sağlanabilir.

[743] MüKoStPO/Günther § 101 Rn. 44.
[744] Park, Durchsuchung und Beschlagnahme, § 4 Rn. 929.

Böylece ilgili kişinin kişiliği hakkında kapsamlı bilgi edinilebilir ve bütün kullanım davranışı çok yönlü izlenebilir[745].

Ancak kaydedilmiş bütün içeriklerin erişimin hedefi olması ciddi endişelere yol açmaktadır. Bu çekinceler bir yandan temel haklara yönelik bu tür bir müdahalenin özel bir gerekçeye dayanması gerekliliğinden kaynaklanmaktadır[746].

Bu açıdan online arama tedbirini konutun teknik araçlarla akustik olarak dinlenmesi tedbiriyle karşılaştırdığımızda, mukayese edilebilir benzer bir durumun bulunmadığı ifade edilebilir. Zira konutun teknik araçlarla dinlenmesinde, tedbir başlamadan önce konuşulanlara erişmek mümkün değildir. Online arama ile tedbir kararından önce bilgi teknolojisi sisteminde üretilmiş ve kaydedilmiş tüm içeriklere ulaşılabilinir. Dolayısıyla online arama kapsamında veri dizilerinin geçmişe kadar uzanması konutun teknik araçlarla dinlenmesinin çok ötesine geçmektedir[747]. Bu nedenle, veri erişiminin hedefi olabilecek "veri havuzu" için bir zaman sınırının gerekli olduğu ifade edilmektedir. Öte yandan, sadece telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri temelinde gerçekleştirilebilen telekomünikasyon içeriğinin izlenmesinden kesin bir ayrımın yapılması gerektiği belirtilir[748].

Bilgi teknolojisi sistemlerinin verilerinin büyük bir kısmı telekomünikasyon yoluyla bu sistemlere girse de bu sistemlerin aynı zamanda bilgi teknolojisi sisteminin kendisi tarafından üretilen, örneğin GPS verileri gibi önemli sayıda veriyi de içerdiği ifade edilir. Bu bağlamda, ilgili verilerin niteliği ve kaynağı bakımından daraltılmalarının önemli olduğu vurgulanmaktadır[749]. Nitekim örneğin GPS verilerine ulaşılamadığı takdirde, tedbire maruz kalan kişinin davranış profilinin oluşturulması imkânsız hale gelir ve böylelikle bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü garanti etme hakkı korunmuş olur.

Alman CMK m. 100d/1 uyarınca online arama tedbirinin yalnızca özel hayatın çekirdek alanından bilgi elde edileceği varsayımına ilişkin olgusal göstergelerin bulunması halinde, tedbire başvurulamaz. Ancak online aramada bu genellikle önceden kesin olarak öngörülebilir değildir[750].

[745] BT-Drucksache 18/12785, 54.
[746] Pretz, Freilaw 2/2016, S. 130, 131.
[747] Sieber/Brodowski, Teil 19.3 Strafprozessrecht, VI. Online Durchsuchung Rn. 161.
[748] Park, § 4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 932.
[749] Park, § 4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 932.
[750] Roggan StV 2017, 828; Kruse/Grzesiek, S. 349.

Özel hayatın çekirdek alanı hakkında bilgi edinmenin muhtemel olması halinde, tedbirden en başından itibaren kaçınılması gerekmez. Bu nedenle, online aramayı önlemek için özel hayatın çekirdek alanıyla ilgili bilgilerin soruşturma hedefi kapsamına giren içerikle bağlantılı olduğuna dair somut göstergelerin varlığı dahi veri elde etme yasağına yol açmaz[751].

Alman CMK m. 100d/3-1 gereği özel hayatın çekirdek alanına ilişkin verilerin elde edilmemesi teknik olarak sağlanmalıdır. Bu bağlamda özellikle bilgi teknolojisi güvenlik önlemleri kullanılmalıdır.[752] Örneğin mikrofonlara ve web kameralarına genel olarak erişilmediği takdirde teknik sağlama kabul edilebilir, ancak bunun tedbirin uygulanmasında gerçekten sağlanabilmesi çok mümkün görünmemektedir[753]. Buna rağmen tedbire maruz kalan kişinin özel hayatının çekirdek alanıyla ilgili elde edilen bulgular söz konusuysa, bu durumda Alman CMK m. 100d/3-2 uyarınca bu veriler ya derhal silinmeli ya da savcılık tarafından verilerin kullanılabilirliği ve silinmesine ilişkin bir karar için karar veren mahkemeye iletilmelidir. Bu hüküm, verinin kullanılabilirliğine karar verecek ve böylece ilgili kişinin çıkarlarını koruyacak bağımsız bir organa duyulan ihtiyacı dikkate almaktadır[754].

Dolayısıyla Federal Anayasa Mahkemesi'ne göre, çekirdek alanla ilgili verilerin veri toplama öncesinde veya sırasında ayrıştırılamaması halinde, son derece kişisel verilerin elde edilme olasılığının bulunması olasılığında da, bilgi teknolojisi sistemine erişime izin verilir. Bu bağlamda kanun koyucu, Federal Anayasa mahkemesi tarafından iki aşamalı mekanizma[755] olarak geliştirilen veri değerlendirme ve veri kullanımı düzeyindeki güvenceler aracılığıyla tedbire maruz kalan kişinin koruma ihtiyaçlarını dikkate almalı ve bu tür erişimin etkilerini en aza indirmelidir[756]. Alman CMK m. 100d/3-3 uyarınca mahkemenin verilerin kullanılabilirliğine ilişkin kararı sonraki işlemler için bağlayıcıdır.

b. Yetki bakımından

Alman CMK m. 100e/2-1 gereği online arama tedbirine başvurulabilmesi için savcının Mahkemeler Teşkilatı Kanunu'nun 74a/4 (GVG) hükmü gereğince yetki

[751] BVerfGE 120, 274 Rn. 281.
[752] BVerfGE 120, 274 (338).
[753] Kruse/Grzesiek, S. 349.
[754] BVerfG NJW 2004, 1007; BVerfG NJW 2007, 2757.
[755] Bkz. İkinci Bölüm I G.
[756] BVerfG NJW 2016, 1795.

bölgesinde bulunduğu eyalet mahkemesinin devlet güvenlik dairesinde talepte bulunması gerekmektedir.

Tedbire kararı vermeye yetkili daire, Eyalet Yüksek Mahkemesinin yetki bölgesinde bulunan, ceza yargılamasında görevli olmayan 3 hâkimden oluşan devlet güvenlik dairesine (Staatsschutzkammer) aittir.

Gecikmesinde sakınca bulunan hallerde ise karar vermeye yetkili dairenin başkanının da bu kararı vermeye yönelik yetkisi düzenlenmiş olup, bu durumda 3 gün içinde bu kararın mahkeme dairesi tarafından onaylanması gerekmektedir[757]. Dolayısıyla savcılığın online arama kararı verilmesi bakımından herhangi bir yetkisinin bulunmadığını görmekteyiz.

Ancak bu noktada bir hususun vurgulanması gerekmektedir. Alman Ceza Muhakemesi Kanunu'nun 100e/2-1 maddesinin açık lafzına göre, online arama kararı yalnızca savcılığın talebi üzerine verilebilir. Bunun neticesinde, gecikmesinde tehlike bulunan hallerde dahi savcının talebi olmaması halinde hakim re'sen karar verme yetkisine sahip değildir[758].

Tedbir kararını veren mahkeme aynı zamanda suçun ağırlığını da tespit etmekle yükümlüdür. Gerektiğinden fazla veri elde edilmesini önlemek için, ilgili bilgiler mahkeme kararında mümkün olduğunca kesin bir şekilde belirtilmelidir[759]. Ayrıca, gereklilik ve orantılılığa ilişkin temel hususlar kararın gerekçesinde gösterilmelidir[760]. Alman CMK m. 100e/3 mahkemenin verdiği tedbir kararının şeklini ve içeriğini düzenlemektedir. Buna göre tedbir kararı yazılı olarak verilir.

Kararda belirtilmesi gereken hususlar şu şekildedir:

- mümkün olduğunca, tedbirin yöneltildiği ilgili kişinin adı ve adresi,
- tedbir kararına esas teşkil eden suç
- tedbirin niteliği, kapsamı, süresi ve bitiş tarihi,
- tedbir tarafından elde edilecek bilgilerin niteliği ve muhakeme için önemi,
- verilerin elde edileceği bilgi teknolojisi sisteminin mümkün olduğunca kesin bir tanımı.

Bunların dışında Alman CMK m. 100e/4 uyarınca tedbirin alınması veya uzatılmasına ilişkin gerekçeler, gereklilikleri ve temel hususları ortaya koymalıdır.

[757] Park, §4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 918.
[758] Park, Rn. 918.
[759] Freiling/Safferling/Rückert JR 2018, 9, 3.
[760] Soine, NStZ 2018, Rn. 503.

Özellikle her somut olaya istinaden şüpheye yol açan spesifik olguların ile tedbirin gerekliliği ve orantılılığına ilişkin temel hususların belirtilmesi gerekmektedir. Bu düzenleme ile online arama tedbirinin su istimal edilmemesi için usule ilişkin bir başka güvence getirildiğini ifade edebiliriz[761].

Gerek online aramaya karar verilirken gerekse tedbirin uygulanmasında gözetilmesi gereken ölçülülük ilkesine göre, online arama yoluyla yapılan müdahalenin her zaman beklenen sonuçlarla orantılı olması gerekmektedir. Bu bağlamda Alman CMK 100e/5 maddesinin önemli olduğunu belirtmek gerekir. Zira tedbir kararı verildikten sonra kararın şartlarının artık karşılanmaması halinde, karara dayanılarak alınan tedbirler derhal sonlandırılmalıdır. Kararı veren mahkeme, tedbirin sona erdirilmesinden sonra tedbirin sonuçları hakkında bilgilendirilmelidir. Bunun ötesinde, kararı veren mahkeme kaydedilen ilerleme hakkında da bilgilendirilmelidir. Kararın gerekliliklerinin yerine getirilmemesi halinde, savcılık tarafından sonlandırma kararı verilmemişse, mahkeme tedbirin sonlandırılmasına karar vermelidir. Ayrıca tedbir mahkeme başkanı tarafından da sonlandırılabilir.

c. Zaman bakımından

Tedbire maruz kalan kişinin bilgi teknolojisi sistemine gizli erişim yalnızca bir kez ve münferit olarak gerçekleşmemekte, aksine sisteme erişim sağlandıktan sonra uzun bir süre sistem izlenebilmektedir[762].

Alman CMK m. 100e/2-4 uyarınca, online arama tedbiri en fazla bir ay ile sınırlı olmalıdır. Elde edilen soruşturma sonuçları dikkate alınarak, koşulların devam etmesi şartıyla, her durumda bir aydan fazla olmamak üzere uzatmaya gidilme imkânı tanınmıştır. Kararın süresinin toplam altı aya uzatıldığı ve uzatmanın devam etmesinin talep edildiği hallerde kararın yüksek bölge eyalet mahkemesi tarafından verileceği düzenlenmiştir. Kanun koyucunun uzatma taleplerine yönelik azami bir süre sınırı getirmemesi nedeniyle, online aramanın koşulların devam etmesi halinde uzun bir zaman dilimine yayılarak uygulanabileceğini ifade edebiliriz. Bununla birlikte belirtilmelidir ki, her talepte en fazla 1 aylık süre verilebileceğinden, soruşturma makamları sürenin sonunda tedbir kararının alınmasına ilişkin koşulları değerlendirmek zorunda kalmaktalar.

[761] Soine, NStZ 2018, Rn. 503.
[762] BT-Drucksache 18/12785, S. 54.

Her ne kadar online aramaya yönelik taleplerde azami tedbir süresinin talep edilmesinin önlenmesi gerektiği, tedbir süresinin sistemdeki veri hacmine göre değerlendirmesi gerektiği ifade edilse de[763], bunun fiilen en azından ilk talep bakımından mümkün olamayacağı kanaatindeyiz. Zira online arama yapmak üzere mahkemeye başvurulduğunda, soruşturmaya konu olan bilgi teknolojisi sisteminin veri hacmi hakkında henüz bilgi sahibi olunamaz, en fazla tahmin yürütülebilir. Bu nedenle de bir soruşturma çerçevesinde savcılığın ilk kez online arama kararını talep etmesi halinde, bir aylık gizli erişimi talep etmesi olağandır.

d. Kişi bakımından

Kişi bakımından sınırlama da tanıklıktan çekinme hakkı bulunan kişilere değinmek gerekir.

Alman CMK m. 100d/5-1 uyarınca online arama mesleki gizlilik sebebiyle tanıklıktan çekinme hakkı olan kişilere uygulanamaz. Tanıklıktan çekinme hakkı olan kişiler Alman CMK m. 53'te düzenlenmiştir. Buna göre, örneğin din görevlileri, sanık müdafileri, avukatlar, hukuk müşavirleri, noterler, doktorlar gibi meslek mensupları mesleki sıfatlarıyla bildikleri şeyler hakkında tanıklıktan çekinebilirler.

Tanıklıktan çekinme ile ilgili belirlenmiş olan mesleki gizliliğe tabi olan kişiler bakımından herhangi bir ayrım söz konusu değildir. Alman CMK m. 53 'te sayılmış olan tüm meslek mensupları koşulların sağlandığı takdirde tanıklık yapmaktan çekinebilir[764].

Tedbirin uygulanması sırasında veya sonrasında meslek sebebiyle tanıklıktan çekinme hakkının söz konusu olması durumunda, Alman CMK m. 100d/2 doğrudan uygulanır. Bunun neticesinde bu veriler ya ivedilikle silinmeli ya da verilerin kullanılabilirliği ve silinmesi hakkında bir karar verilmesi için karar veren mahkemeye sunulmalıdır.

Alman CMK m. 100d/5-2 uyarınca ise, sanığın yakınlarının tanıklıktan çekinme hakkının bulunduğu düzenleme altına alınmıştır. Bununla birlikte mesleki gizliliğe tabi olan kişilerle bir mesleğin ortaklaşa icrası da dahil olmak üzere sözleşmeye dayalı bir ilişki durumunda, meslek öncesi faaliyetlere yardımcı olunması veya başka bir yardımcı faaliyet icra edilmesi durumunda da tanıklıktan çekinme hakkı bulunmaktadır. Bu bahsi geçen kişiler bakımından, online arama kararı hukuka uygun

[763] Park, § 4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 935.
[764] MüKoStPO/Günther § 100c Rn. 71.

bir şekilde genel olarak verilebilir. Ancak bu karar ile elde edilen verilerden, temelde yatan güven ilişkisinin öneminin göz önünde bulundurulması suretiyle, söz konusu olayın gerçeklerinin araştırılması veya suçlanan kişinin nerede olduğunun tespit edilmesindeki menfaatle orantısız olmaması halinde yararlanılabilir[765].

7. Delil değerlendirilmesi

Ceza muhakemesinde karar verme yetkisini haiz olan yetkililerin, elde edilen delillerden sonuç çıkarıp bu sonucu kararlarında kullanmalarına delillerin değerlendirilmesi denir[766].

Bu kapsamda hem maddi hukuk bakımından doğru hem de adaletin sağlanması bakımından adil bir karar verilmesi amaçlanır[767]. Maddi gerçeğe ulaşılmaya çalışılırken, maddi ceza hukuku açısından önemli olan tüm hususların tek tek ispatına çalışılmalıdır[768]. Bununla birlikte Ceza muhakemesi hukuku, kendi alanına ilişkin uyuşmazlıklara yönelik, adaletin sağlanmasının yanı sıra toplum düzeninin korunmasına hizmet de eder[769].

Ceza muhakemesi hukuku, bireyin temel hak ve özgürlüklerine saygı göstererek ve kanunların belirlediği sınırlar dahilinde maddi gerçeğe ulaşmalıdır. Bu bağlamda gerek muhakeme sürecinin hukuka uygun bir şekilde gerçekleştirilmesiyle gerekse muhakeme sonucunda uyuşmazlığın hukuki çerçeve dahlinde doğru bir şekilde çözüme kavuşturulmasıyla birlikte ceza muhakemesi adaleti sağlama amacına ulaşır[770].

Hukukun üstünlüğü altında ceza yargılamalarında maddi gerçeğin ne pahasına olursa olsun tespit edilmesi düşünülemez[771]. Bu nedenle delil yasakları ile buna sınırlamalar getirilmektedir[772]. Maddi gerçeğin kendisi bir amaç değil, her yargılamanın meşruiyet dayanağıdır. Dolayısıyla maddi gerçeğin tespiti hukukun üstünlüğü kurallarına bağlı olmalıdır[773]. Maddi gerçeğin araştırılmasının, öncelikli olarak korunması gereken insan hakları ve insanlık onuru gibi üstün menfaatlerle

---

[765] Park, § 4 Durchsuchung und Beschlagnahme im EDV-Bereich, Rn. 936; MüKOStRO/Rückert § 100b Rn. 73.
[766] Öztürk/Erdem/Tezcan, Ceza Muhakemesi Hukuku, s.. 389; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 420; Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s 328.
[767] Karakehya, İÜHFM C. LXV, S. 2, Ceza Muhakemesinin Amacı, S.123
[768] Volk, Klaus, Grundkurs StPO, C.H. Beck Verlag, München 2005, S. 4.
[769]Karakehya, İÜHFM C. LXV, S. 2, Ceza Muhakemesinin Amacı, S. 131.
[770] Karakehya, İÜHFM C. LXV, S. 2, Ceza Muhakemesinin Amacı, S. 131.
[771] BGHSt 14, 358 (365) = NJW 1960, 1580 (1582); BGHSt 31, 304 (308) = NJW 1983, 1579 (1571).
[772] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 491.
[773] Kubiciel, HRRS 2014, 204 (208).

çatışması halinde, ulaşılmış bilgi kabul edilemez ve değerlendirilemez[774]. Bu doğrultuda hukuka aykırı delillerin ceza muhakemesinde delil olarak değerlendirilmesi mümkün olmayacaktır. Sonuç olarak, ceza yargılamalarında mutlak maddi gerçekten ziyade, usulüne uygun olarak tesis edilmiş ve "usuli gerçek" olarak adlandırılan bir gerçek benimsenir[775].

Bununla birlikte ceza muhakemesinde "delil serbestisi" ilkesi geçerli olup, delillerin değerlendirilmesi bakımından hâkim ve savcı serbesttir. Delil serbestisi ilkesi bir taraftan her şeyin delil olmasını, soruşturma ve kovuşturma evrelerinde delillerin incelenmesini ve değerlendirilmesini kapsarken, diğer taraftan ise hâkimin delilleri vicdani kanaatine göre tartmasını da içerir[776].

"Delil serbestisi" ilkesi iki yönden sınırlandırılmıştır. Bunlardan biri değerlendirilecek olan delilin yalnızca duruşmaya getirilmiş ve huzurda tartışılmış deliller olması gerekliliğidir (CMK m. 217/1). Diğer sınırı ise yalnızca hukuka uygun şekilde elde edilen delillerin değerlendirilebilmesidir. Dolayısıyla hukuka aykırı yöntemlerde elde edilen delilin değerlendirilmeye alınması ve hükme esas teşkil etmesi mümkün olamaz[777].

Bu bağlamda, delillerin değerlendirilmesi bakımından "vicdani delil sisteminin" benimsenmiş olduğu, bunun sonucunda delillerin hâkimin vicdani kanaatiyle serbestçe takdir edildiği vurgulanmalıdır[778]. Vicdani kanaat, maddi uyuşmazlığı çözmeye yetkili makamın, duruşmada yapılan muhakeme faaliyeti sonucunda, aklını rehber yaparak ve hukukun koyduğu usul ve esaslar içerisinde kalarak, maddi olayın oluş biçimine dair ulaştığı, kendi açısından şüpheye yer vermeyen bir kanaat olarak tanımlanmaktadır[779]. Hâkimin vicdani kanaati maddi gereceğe ilişkin oluşacaktır. Maddi gerçekte onu yansıtan delillerin yardımıyla bulunabilir[780].

---

[774] Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 337; Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 34.
[775] Joecks, 4. Auflage 2015, Einl. Rn. 4; Eisenberg, Beweisrecht der StPO, 10. Auflage 2017, Rn. 329.
[776] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 329; Gökçen/Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, S. 2928.
[777] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, s. 329; Gökçen/Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, S. 2929.
[778] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 389; Feyzioğlu, Ceza Muhakemesinde İspatın Ölçütü Olarak Vicdani Kanaat, s. 23, 240 vd.
[779] Feyzioğlu, s. 109.
[780] Karakehya, İÜHFM C. LXV, S. 2, Ceza Muhakemesinin Amacı, S. 127.

Çalışmanın bu bölümünde öncelikle hukuka uygun elde edilmiş delillerin değerlendirilmesi incelenecek olup, sonrasında ise hukuka aykırı elde edilmiş deliller ve bunların nasıl değerlendirildiği, özellikle delil yasakları ve online arama tedbiri çerçevesinde bunların nasıl ele alındığı irdelenecektir. Devamında ise, tesadüfen elde edilen verilere, başka kanunlara dayanarak elde edilmiş verilere ve yurt dışındaki bilgi teknolojisi sistemlerinde kaydedilmiş verilere yönelik açıklamalar yapılacaktır.

a. Hukuka uygun elde edilmiş delillerin değerlendirilmesi

Ceza muhakemesinde maddi gerçeğin ortaya çıkarılmasında yapılan işlemlerin hukuka uygun yürütülmesi esastır[781]. Bu nedenle delillerin hukuka uygun şekilde elde edilmesi önem teşkil eder. Bu bağlamda bir olayın ispatına yönelik kullanılan delil vasıtalarının hukuk düzenince kabul edilen vasıtalardan olması gerekir.

Online arama ile edilen bulguların, yani verilerin mahkemeye sunulması olasılıkları açısından, bunların kaydedildiği veri taşıyıcısının fiziki delil ("*Augenscheinsobjekt*") olarak ana duruşmanın bir parçası haline getirilmek suretiyle hâkimin huzurunda tartışılması mümkündür[782]. Online arama sonuçlarını nasıl kullanacağı ve veri kaydının güvenilirliği konusunda kendisini nasıl ikna edeceği, açıklığa kavuşturma görevi temelinde hâkimin takdirine bırakılmıştır[783].

Çoğu durumda, veri taşıyıcısındaki veriler görüntü, metin, ses, video gibi farklı bilgi türlerini içerecektir. Bu verilerin yargılamada kullanılabilmesi için uygun programlar kullanılarak algılanabilir bilgilere dönüştürülmesi gerekir[784]. Bu dönüşüm sırasında verilerin gerçekliğinin ve bütünlüğünün tehlikeye atılmamasını sağlamak önemlidir[785].

Verilerin metin veya resim dosyalarında olduğu gibi bunların çıktısının alınması mümkünse, bu çıktılar belge olaraktan mahkemeye sunulabilir[786]. Ancak bu durumda söz konusu çıktıların manipüle edilme riski bulunduğundan, orijinal veri taşıyıcısına kıyasla delil değeri azalmış olur.

Buna ek olarak, basit yazılı, sesli veya görüntülü bilgilerden oluşmayan ve mahkemenin anlayabileceği bir bilgi içeriği elde etmek için öncelikle

[781] Gökçen/Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, S. 2934.
[782] BGH NStZ 2014, 347; OLG Nürnberg StraFo 2015, 102.
[783] Hauck in Löwe/Rosenberg, StPO, §100b Rn. 121.
[784] MüKoStPO/Rückert StPO §100b Rn. 75.
[785] Dewald/Freiling, Forensische Informatik, S. 244.
[786] BGHSt 27, 135, 137.

görselleştirilmesi ve işlenmesi gereken veri paketlerinin çevirisi ve değerlendirilmesi söz konusu olduğunda bir adli bilişim uzmanına ihtiyaç duyulmaktadır[787].

(1) Asıl ceza yargılamasında

Yasal tedbirlere dayanılarak elde edilen kişisel verilerin asıl ceza yargılamasında mı yoksa diğer ceza yargılamalarında mı kullanılacağı konusunda bir ayrım yapılmalıdır. Diğer ceza yargılamaları farklı soruşturma evrelerini ifade etmemekte olup, aksine, diğer ceza yargılamaları, tedbire neden olan suçtan farklı olarak başka bir suç anlamına gelmektedir[788]. Bu nedenle, kişisel verilerin asıl ceza yargılamasındaki ilk suçla mı yoksa başka bir cezai suçla mı bağlantılı olarak kullanılıp kullanılmayacağı konusunda bir ayrım yapılması gerekmektedir[789].

Online aramanın düzenlenmiş olduğu Alman CMK. m. 100b uyarınca elde edilen kişisel verilerin ceza yargılamasında değerlendirilmesine yönelik herhangi bir düzenleme yapılmamıştır. Yalnızca Alman CMK m. 100d/2-1 gereği özel hayatın çekirdek alanını ilgilendiren özel kişisel bilgilerin kullanılması yasaklanmıştır[790].

Bununla birlikte, bir katalog suçun işlenmesine yönelik şüphenin sonradan ortadan kalkması halinde de delillerin kullanılabileceği varsayılabilir. Örneğin online aramanın emredildiği zamandan farklı olarak suçun bir çete hırsızlığı değil de basit bir hırsızlık olması halinde, tedbirden elde edilen kişisel veriler de ilgili bir hırsızlık suçlaması için delil olarak kullanılabilir[791]. Nitekim online arama kararının hukuka uygun şekilde verilmesi önemlidir ve bu hukuka uygunluk bilinen olgulardaki değişiklikten etkilenmez[792].

(2) Diğer ceza yargılamalarında

Online arama tedbiri ile elde edilen delillerin başka ceza yargılamalarında değerlendirilmesi bakımından Alman CMK m. 100e/6-1 hükmü geçerlidir. Buna göre, veriler, izlemeye tabi tutulan kişilerin rızası olmaksızın, yalnızca 100 b maddesi uyarınca tedbir kararı verilebilecek bir suçun soruşturulması veya bu tür bir suçla

[787] MüKoStPO/Rückert StPO §100b Rn. 75.
[788] Köhler in Meyer-Gossner/Schmitt, § 479 Rn.3; Wittig in BeckOK StPO § 479 Rn. 5.
[789] MüKoStPO/Rückert StPO §100a Rn. 314.
[790] MüKoStPO/Rückert StPO §100b Rn. 76.
[791] Köhler in Meyer-Gossner/Schmitt §100a Rn.32.
[792] MüKoStPO/Rückert StPO §100a Rn. 318.

itham edilen kişinin nerede olduğunun belirlenmesi için diğer ceza davalarında kullanılabilir.

Burada önemli olan husus, diğer ceza yargılamasında da söz konusu soruşturulan suçun online arama yapılabilmesi için koşulların karşılamamasıdır[793]. Dolayısıyla 100e/6-1 hükmü gereği "varsayımsal olarak yasal bir müdahale[794]" bulunduğu kabul ediliyor. Somut olarak bu, diğer ceza yargılamalarının sadece soyut olarak bir katalog suçun soruşturulmasıyla ilgili olması değil, varsayımsal olarak verilerin kullanılacağı yargılamalar için 100b kapsamında bir tedbir kararı verilmesine ilişkin tüm maddi gerekliliklerin incelenmesi gerektiği anlamına gelmektedir[795]. Bu nedenle, verilerin Ceza Muhakemesi Kanunu hükümlerine uygun olarak yeni amaç için elde edilip edilemeyeceğinin kontrol edilmesi önemlidir[796].

(3) Tehlikenin önlenmesi amacıyla

Adli amaçlı bir online tedbiri sonucunda elde edilen verilerin tehlikenin önlenmesi amacıyla değerlendirilmesi Alman CMK 100e/6-2 uyarınca düzenlenmiştir.

Buna göre, verilerin tehlikenin önlenmesi amacıyla kullanılmasına yalnızca münferit bir durumda bir kişinin yaşamına veya özgürlüğüne, devletin güvenliğine veya varlığına ya da nüfusa hizmet eden, olağanüstü kültürel değeri olan veya Alman Ceza Kanunu'nun 305. Maddesinde belirtilen başkalarının mülkiyetinde olan bir binayı, bir gemiyi, bir köprüyü, bir seti, inşa edilmiş bir yolu, bir demiryolunu veya diğer herhangi bir yapı gibi önemli değere sahip nesnelere yönelik bir tehlikenin önlenmesi için izin verilir. Veriler, münferit durumlarda diğer önemli varlıklar için acil bir tehdidi önlemek için de kullanılabilir. Tehlikenin önlenmesi ya da tehlikenin önlenmesi için alınan tedbirlerin yargılama öncesi ya da yargısal denetimi için verilere artık ihtiyaç duyulmaması halinde, bu verilerin kayıtları tehlikenin önlenmesinden sorumlu kurum tarafından derhal silinmelidir. Silme işlemi kayıt altına alınmalıdır. Silme işlemi yalnızca olası bir ön yargılama veya adli inceleme için erteleniyorsa, veriler yalnızca bu amaç için kullanılabilir; başka amaçlar için kullanılmaları engellenmelidir.

[793] MüKoStPO/Rückert StPO §100a Rn. 320.
[794] "Gedanke des hypothetischen Ersatzeingriffs".
[795] BGH 26.4.2017 - 2 StR 247/16, NJW 2017, 3173 (3177).
[796] Singelnstein, ZStW 120 (2008), 853 (881).

Bu çerçevede tartışılan bir husus, adli amaçlı elde edilmiş verilerin tehlikenin önlenmesi amacıyla kullanımı için sadece hukuka uygun şekilde elde edilmiş verilerin değerlendirilip değerlendirilememesidir. Asıl ceza yargılaması bağlamında veri elde etme işleminin yasal olması, verilerin tehlikenin önlenmesi amacıyla kullanılabilmesi için yalnızca ilgili tehlikenin önlenmesi yasasının gerektirmesi halinde bir ön koşuldur[797].

(4) Tehlikenin önlenmesi amacıyla elde edilmiş verilerin Ceza yargılamasında değerlendirilmesi

Alman CMK m. 100e/6-3 ile tehlikenin önlenmesi amacıyla elde edilmiş verilerin ceza yargılamasında değerlendirilmesine yönelik bir düzenleme getirilmiştir.

Buna göre, kullanılabilir kişisel veriler kolluk hukuku kapsamında önleyici online arama tedbiri yoluyla elde edilmişse, bu veriler, bu bağlamda izlenen kişilerin rızası olmaksızın yalnızca ceza yargılamalarında, adli amaçlı online aramayı düzenleyen Alman CMK m. 100b uyarınca tedbirlerin alınmasına neden olabilecek bir suçun soruşturulması veya bu tür bir suçla itham edilen kişinin nerede olduğunun belirlenmesi için kullanılabilir.

Burada önemli olan husus, önleyici online aramalarından elde edilen bulgular, ancak bunlara dayanarak adli amaçlı online aramanın da mümkün olabileceği durumlarda bunların kullanılabilir olmasıdır. Özellikle, sadece bir katalog suç şüphesinin varlığı yeterli değildir. Bunun yerine, bir online arama emri için gerekli olan tüm maddi koşullar ceza yargılamasında kullanıldığı andaki durum dikkate alınarak varsayılmalıdır[798].

Kanun koyucu bu düzenlemenin kapsama alanını kolluk düzenlemeleriyle sınırlandırmış[799].

Buna karşı, Anayasayı Koruma Kanunları ile bağlantılı olan bulguların iletilmesi ve bunların değerlendirilmesi ile ilgili olarak, kanun koyucu online arama bağlamında bu konuda herhangi bir hüküm getirmemiştir.

Bir anayasayı koruma otoritesi tarafından toplanan kişisel veri ve bilgilerin soruşturma makamlarına aktarılması yasal olarak oldukça sorunlu bir durumdur. Bunun nedeni, anayasayı koruma makamının izleme yetkisinin kolluk yetkisi anlamda

[797] MüKoStPO/Rückert StPO §100b Rn. 80.
[798] BGH 26.4.2017 – 2 StR 247/16, NJW 2017, 3173 (3177); MüKoStPO/Rückert StPO §100b Rn. 90.
[799] MüKoStPO/Rückert StPO §100b Rn. 91.

illa bir tehlikenin varlığına bağlı olmamasıdır[800]. Gerekli olan tek şey, anayasanın korunmasına özgü istihbarat için yeterli bir ihtiyaçtır. Bu durum, gözetim tedbirinin münferit olayda istihbarat gözetimi gerektiren belirli bir konunun açıklığa kavuşturulması için gerekli olması ve gözetim ihtiyacına ilişkin yeterli fiili emarelerin bulunması halinde geçerlidir[801]. Bu nedenle istihbarat yoluyla elde edilen bilgilerin soruşturma makamlarına aktarılması yalnızca özel ağır suçlar bakımından söz konusu olabilmektedir. Bu, somut ve kanıtlanmış koşulların olgusal bir temel olarak mevcut olduğu belirli olgulara dayanan bir şüphenin varlığını gerektirir[802].

b. Hukuka aykırı elde edilmiş delillerin değerlendirilmesi

(1) Genel olarak delil yasakları

Sınırsız bir maddi gerçek arayışının pek çok kişisel ve toplumsal değeri tahrip edeceği kabul edildiğinden, maddi gerçek arayışı ilkesine artık mutlak bir değer atfedilmemektedir[803]. Delil yasağı olarak bilinen maddi gerçeğin araştırılmasına yönelik bazı sınırlamalar, söz konusu kişisel ve toplumsal değerleri korumayı amaçlamaktadır[804]. İşte hukuk devleti ilkesine dayalı ceza yargılamalarında delil elde edilmesi ve değerlendirilmesi işlemlerine getirilen sınırlamalara delil yasakları denir[805].

Hukuka uygunluğun denetimi delil yasakları ile güvence altına alınır. Bu yasaklar delilin elde edilmesi, ileri sürülmesi ve değerlendirilmesi için geçerlidir[806].

Delil yasakları delillerin serbestçe araştırılmasının sınırını çizer. Zira Ceza Mahkemesinde maddi gerçeğin her ne pahasına olursa olsun araştırılması mümkün değildir. Bu doğrultuda delil yasaklarının, maddi gerçeğin araştırılması ilkesinin sınırını oluşturduğu kabul edilir[807].

İfade edilmelidir ki, delil yasakları gerek savunma ve iddia makamlarına yönelik, gerekse yargılamayı gerçekleştiren hakim veya hakimlere yönelik

---

[800] BeckOK StPO/Graf StPO §100b Rn.61.
[801] BVerfG NJW 2022, 1583.
[802] BVerfG NJW 2022, 1583; BeckOK StPO/Graf StPO §100b Rn.61.
[803] Öztürk, CMUK Reformu ve Delil Yasakları, s. 39.
[804] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 400.
[805] Öztürk, Grundlagen der Beweisverbote im türkischen und deutschen Strafverfahrensrecht, Zeitschrift für die gesamte Strafrechtswissenschaft, Berlin, New York, 1992, s. 667; Öztürk, Kovuşturma Mecburiyeti, s. 54 vd.
[806] Özbek, Ceza Muhakemesi Hukukunda Delil Yasakları, Alman-Türk Karşılaştırmaı Ceza Hukuku, Cilt III, İstanbul 2010, s. 913.
[807] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 430; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 430.

sınırlamalar getirmektedir[808]. Delil yasaklarının kabul edilmesinin temel nedeni, başta işkence olmak üzere hukuka aykırı ifade sorgu yöntemleriyle elde edilen delillere karşı mücadeledir[809].

Delil Yasakları da kendi içinde "delil elde etme yasakları" ile "delil değerlendirme yasakları" olarak ikiye ayrılır. Yargıtay tarafından delil elde etme yasakları, delillerin elde edilmiş şekline ilişkin yasaklar olarak tanılanırken, delil değerlendirme yasakları ise, hukuka uygun elde edilmiş olsa bile, o delilin yargılamada ortaya konulup değerlendirilmesine ilişin yasaklar olarak ifade edilir[810]. Bu yasaklar, suçlulukla mücadelede devletin sahip olduğu gücün hukuk devleti ilkesine uygun bir biçimde kullanımı ve insan hakları ihlallerinin önlenmesi bakımından ayrıca önemlidir.

Delillerin değerlendirilmesi bakımından öğretide mutlak ve nispi hukuka aykırılıklar[811] ile maddi ve şekli hukuka aykırılıklar[812] olmak üzere farklı görüşler belirtilmektedir. Kural olarak Hukuka aykırı yollarla elde edilen delilin gerek soruşturma gerekse kovuşturma evresinde kullanılması yasaktır.

Mutlak değerlendirme yasağı bakımından, hukuka aykırı elde edilmiş delilin muhakemede belirleyici rol alabileceği düşüncesiyle, yargılamanın hakkaniyetinin zedeleneceğinden yola çıkarak, bu deliller mutlak bir şekilde kullanılamamaktadır. Bu bağlamda delilin elde edilmesi sırasında önemli ya da önemsiz, az ya da çok gibi kriterler dikkate alınmaz. Dolayısıyla hukuka aykırılığın boyutuna bakılmaksızın katı bir yaklaşım söz konusudur[813]. Hukuka aykırı elde edilen delil açısından "yasak ağacın meyvesi de yasaktır" anlayışından yola çıkarak, mutlak değerlendirme yasağı kabul edilir[814].

Nisbi değerlendirme yasağı bakımından, ihlal edilen kuralın koruduğu hukuki değerden yola çıkılmak suretiyle, yalnızca temel haklar ihlal edilerek ve kanunun mutlak aykırılık olarak düzenlediği ihlaller sonucunda elde edilen delillerin kullanılamayacağı benimsenmektedir. Kanunun mutlak aykırılık olarak öngördüğü ihlaller dışındaki aykırılıkların ise yasak kapsamında bulunup bulunmadığının, her

[808] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuk u, S. 334.
[809] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuku, S. 334.
[810] Yargıtay Ceza Genel Kurul, 10.12. 2013, 483/599.
[811] Centel/Zafer, Ceza Muhakemesi Hukuku, s. 771 vd; Özbek, Ceza Muhakemesi Hukukunda Delil Yasakları, s. 915.
[812] Özbek/Doğan/Bacaksız/Tepe, Ceza Muhakemesi Hukuku, s. 673.
[813] Akyürek, s. 66.
[814] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuk u, S. 338.

somut olayda hakim tarafından değerlendirilmesi gerektiği kabul edilir. Bu değerlendirmede ihlal edilen hak ile ortaya çıkan menfaat arasındaki oran dikkate alınmalıdır.

Nisbi değerlendirme yasağını kabul etmiş olan Almanya'nın da dahil olduğu Kara Avrupa Hukuk sisteminin hukuka aykırı deliller konusunda mutlak değerlendirme yasağının aksine esnek bir delil değerlendirme yolunu seçtiğini ifade edilebiliriz[815].

Buna karşılık Türk Hukuk Sisteminde, Anglo-Amerikan hukuk sisteminde olduğu gibi, geçerli olan delil yasağı mutlak delil yasağıdır[816]. Zira Anayasa m. 38/6 gereği, *"kanuna aykırı olarak elde edilmiş bulgular delil olarak kabul edilemez";* CMK m. 217/2 uyarınca ise *"yüklenen suç, hukuka uygun şekilde elde edilmiş her türlü delille ispat edilebilir"* hükümleri, delilin elde edilmesi aşamasında söz konusu olan herhangi bir hukuka aykırılığın, elde edilen delilin Ceza muhakemesinde kullanılamayacağına sebep olacağını net bir şekilde düzenlemişler[817]. CMK da örneğin yasak yöntemlerle elde edilmiş delillerin değerlendirilmesinin açıkça düzenlenmiş olduğu hallerin dışında de delilin elde edilmesi aşamasında herhangi bir hukuka aykırılığın gerçekleşmesinin, elde edilen delilin değerlendirilmesi sonucuna yol açmayacağı ortaya konmakta olup[818], ceza muhakemesinde hukuka aykırı elde edilmiş delillerin, delil yasağı olarak nitelendirilmesi gerektiği ifade edilmektedir[819].

Yargıtay nezdinde kısaca hukuka aykırı delillerin değerlendirilmesine değinecek olursak, Yargıtay, işlenen suçun niteliği, ihlal edilen hukuki diğer, elde edilen delile bir daha ulaşıp ulaşamama durumu ve ihlalin sonuca etkili olup olmadığı gibi kriterlerle hukuka aykırı elde edilmiş delilin değerlendirilmesine karar vermektedir[820]. Yukarıda belirttiğimiz Anayasa ve CMK düzenlemelerini dikkate aldığımızda mutlak delil yasağının uygulanması gerektiğini, ancak uygulamada Yargıtayın bu prensibin esnetildiğini ifade edebiliriz[821].

---

[815] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuk u, S. 346.
[816] Centel/Zafer, Ceza Muhakemesi Hukuku, s. 693: Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku,s. 395.
[817] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 431.
[818] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 395;
Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 432.
[819] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuk u, S. 346.
[820] Yargıtay Ceza Genel Kurulu, 26.06.2007, 147/159; Yargıtay Ceza Genel Kurulu, 13.03.2012, 8-278/96; Yargıtay Ceza Genel Kurulu, 29.11.2005, 7-144/150.
[821] Gökçen/Balcı/Alşahin/Çakır, Ceza Muhakemesi Hukuk u, S. 345.

(2) Online arama bakımından delil yasakları

(a) Delil Elde Etme Yasakları

Delillerin elde etme yasakları, delil konusu yasakları, delil aracı yasakları ve delil metodu yasakları olmak üzere üç alt başlık halinde ele alınır[822].

Delil konusuna ilişkin yasaklar belirli olguları ceza soruşturmasının tamamen dışında bırakırken, delil aracı yasakları belirli delil elde etme araçlarının yasaklanmasını, delil metodu yasakları ise belirli delil elde etme yöntemlerinin yasaklanmasını öngörmektedir[823].

Özel hayatın çekirdek alanını düzenleyen Alman CMK m. 100d/1 uyarınca, online aramaya yönelik delil elde etme yasağı getirilmiştir. Buna göre, online arama tedbirinin yalnızca özel hayatın çekirdek alanından bilgi elde edileceği varsayımına ilişkin olgusal göstergelerin bulunması halinde tedbir uygulanamaz. Alman CMK m. 100d/1 düzenlemesinin bir delil konusuna ilişkin yasak getirmiş olduğunu ifade edebiliriz[824].

Özel hayatın çekirdek alanının kapsamına yönelik Alman Ceza Muhakemesi Kanununda herhangi bir tanımlama yapılmamıştır. İlgili kişilerin insan onurunun korunması merkezi bir öneme sahiptir[825]. Devlet gözetiminden korunmak suretiyle her vatandaş, sezgiler ve duygular gibi içsel süreçlerin yanı sıra düşüncelerini, görüşlerini ve deneyimlerini ifade edebilmelidir[826]. Bu nedenle kişilerin yakınlarıyla kurdukları özel iletişimler özellikle korunur[827]. Devletin bu dokunulmaz çekirdek alana erişimi her zaman yasaktır[828].

Bunun ötesinde Alman CMK m. 100d/5-1 uyarınca online arama mesleki gizlilik sebebiyle tanıklıktan çekinme hakkı olan kişilere uygulanamaz. Dolayısıyla bu kişilerle yapılan tüm görüşmeler ve iletişim süreçleri bakımından delil elde etme yasağı söz konusudur.

---

[822] Kühne Strafprozessrecht, 9. Auflage 2015, S. 566; Dencker, Verwertungsverbote im Strafprozess, Köln 1997, s. 13 vd.
[823] Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 337; Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 270f.
[824] Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 337.
[825] BT-Drucksache 15/4533, 14.
[826] BVerfGE 109, 279 (313) = NJW 2004, 999 (1002).
[827] BVerfGE 109, 279 (319) = NJW 2004, 999 (1004).
[828] Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 349.

(b) Delil Değerlendirme Yasakları

Delil değerlendirme yasakları belirli soruşturma bulgularının ceza yargılamasında değerlendirilmesine olanak tanımaz.

Delil değerlendirme yasakları bağımlı ve bağımsız olmak üzere ikiye ayrılır. Bağımlı delil değerlendirme yasakları delillerin hukuka aykırı olarak elde edilmesinin bir sonucu olarak ortaya çıkarken, bağımsız delil değerlendirme yasakları delillerin elde edilmesine yönelik yasaklardan bağımsız olarak söz konusu olur[829].

Alman Ceza Muhakemesi Kanunu delil değerlendirilmesine ilişkin örneğin Alman CMK m. 136a uyarınca yasak ifade ve sorgu yöntemleri, Alman CMK m.52, m.53 ve m.53 a uyarınca tanıklıktan çekinme hakları ile ilgili ihlaller ve Alman CMK m. 97/1 uyarınca el koyma tedbiri ile bağlantılı gibi bir dizi yasağı hüküm altına almıştır. Bununla birlikte yıllar içinde delil değerlendirilmesine ilişkin çok sayıda yazılı olmayan yasakta gelişmiştir[830].

Delil elde edilmesi sırasındaki ihlallerin delilin değerlendirilmesini engelleyebilse de bu durum her zaman zorunlu olarak geçerli değildir[831]. Federal Anayasa Mahkemesi yazılı olmayan delil değerlendirme yasaklarının gerekçelendirilmesi için oldukça katı şartlar getirmektedir[832]. Federal Anayasa Mahkemesi delillerin değerlendirilmesine ilişkin yazılı olmayan yasakların belirlenmesi bakımından üç ana yaklaşım geliştirmiştir; Bunlar "koruma amacı", "haklar alanı" ve "değerlerin tartımı" teorileridir[833].

Koruma amacı teorisi *(=Schutzzwecktheorie)*, delillerin kullanılabilirliğini, ihlal edilen delil elde etme yasağının koruma amacına bağlı kılmaktadır[834] ve sanığın temel haklarını ihlal etmeyen hukuku aykırı delillerin değerlendirilmesi uygun olarak kabul etmektedir[835].

---

[829] Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 289.
[830] Grossmann, JA 2010, 241 (246).
[831] Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 290.
[832] BVerfG NJW 2010, 287; BVerfG NJW 2010, 2937 (2938).
[833] Gökçen/Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, S. 2936; Grossmann, JA 2010, 241 (246).
[834] Roxin/Schünemann, Strafverfahrensrecht, 29. Aufl. 2017 S. 174; Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 290f.
[835] Gökçen/Çakır, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, S. 2936.

Haklar alanı teorisine *(=Rechtskreistheorie)* göre, ihlalin şüphelinin/sanığın haklar alanını önemli ölçüde etkileyip etkilemediği ya da onun için önemsiz olup olmadığına bağlıdır[836].

Baskın görüşün savunduğu değerlerin tartımı teorisi *(=Abwägungslehre)* gereği, her somut olayda etkilenen vatandaşın menfaatleri, devletin suçun soruşturulması ve kovuşturulmasındaki menfaatine karşı tartılmalıdır. Bu çerçevede hem ihlalin önemi hem de suçun ağırlığı göz önünde bulundurulmalıdır[837].

Söz konusu teorilerin dışında bir de "itiraz çözüm yolu" (=Widerspruchslösung) vardır. Bu durumda delil değerlendirilmesine karşı sanık tarafından açıkça itiraz edilmesi beklenmektedir[838]. Ancak online arama tedbiri ile gerçekleşen müdahalenin ağırlığı sebebiyle online aramanın ihlali söz konusu olduğunda, beyan edilen bir itiraz gerekliliğinden feragat edilmesi gerektiği ifade edilmektedir[839].

Ayrıca ifade edilmelidir ki, delil değerlendirme yasakları mahkemenin suç şüphesini doğrulamak veya çürütmek için kullanabileceği delilleri kısıtladığından, yalnızca münferit durumlarda açık bir kanun hükmü uyarınca ya da önemli nedenlerle tanınabilecek bir istisna olarak kabul edilir. Zira bunun sonucunda maddi açıdan doğru ve adil bir kararın verilmesi engellenebilmektedir[840].

Bu nedenle, ana duruşma dışında meydana gelen temel hak ihlalleri, ana duruşmaya dayanan ceza hükmünün de anayasa hukukunu ihlal ettiği anlamına gelmez[841].

Anayasal açıdan bakıldığında, delillerin kullanılmasına ilişkin bir yasağın varsayılması, ancak sanığın hukukun ihlali nedeniyle yargılamanın seyrini ve sonucunu etkilemek için yeterli fırsata sahip olmaması halinde, gerçeğin rastgele araştırılması için asgari gerekliliklerin artık karşılanamaması halinde, bilgilerin kullanılması genel kişilik hakkına orantısız bir müdahaleye yol açması halinde uygun olarak kabul edilir[842]. Ayrıca, yasal hükümlere aykırı olarak elde edilen bilgilerin

---

[836] BGHSt 11, 213 (215) = NJW 1958, 557 (558); Roxin/Schünemann, Strafverfahrensrecht, 29. Aufl. 2017 S. 174; Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 340.
[837] Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 291; Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 339.
[838] Kindhaeuser, Strafprozessrecht, 4. Auflage 2016, 290f.; Beulke/Swoboda, Strafprozessrecht, 14. Auflage 2018, 341f.
[839] Eschelbach in Satzger/Schluckebier/Widmaier, StPO §100a Rn. 34 und §100e Rn. 32.
[840] BVerfG NJW 2012, 907 Rn. 117; BeckOK StPO/Graf StPO §100b Rn. 47.
[841] BVerfG Beschl. v 7.12.2011 – 2 BvR 2500/09, 1857/10, Rn. 117.
[842] BVerfG NJW 2012, 907 Rn. 117; BVerfG NJW 2005, 1917; BeckOK StPO/Graf StPO §100b Rn. 47.

kullanılabilirliği, bu durumun hukuka aykırı delil elde edilmesini destekleyeceği durumlarda onaylanamaz. Bu nedenle, delillerin değerlendirilmesinin yasaklanması, özellikle temel hak güvencelerinin kasıtlı veya sistematik olarak göz ardı edildiği ciddi, kasıtlı veya objektif olarak keyfi hukuk ihlallerinden sonra gerekli olabilir[843].

i. Özel Hayatın Çekirdek Alanının İhlali

Bir delil değerlendirme yasağı olarak Alman CMK m. 100d/2 uyarınca özel hayatın çekirdek alanına yönelik bir ihlal hüküm altına alınmıştır. Buna göre, online arama tedbiri yoluyla elde edilen özel hayatın çekirdek alanına ilişkin bilgiler değerlendirilemez.

Bu delil değerlendirme yasağı mutlaktır ve kapsamlı üçüncü taraf, sonuçsal ve uzak etkilere sahiptir[844].

Özel hayatın çekirdek alanını ilgilendiren bilgilerin elde edilmemesi teknik olarak sağlanmalıdır. Yine de bu tür bilgilerin elde edilirse, bunlar derhal silinmelidir. Bunların elde edilmesi ve silinmesi belgelenmelidir.

Bununla birlikte Alman CMK m. 100d/5-2 uyarınca Alman CMK m. 52 ve m. 53a uyarınca tanıklıktan çekinme hakkı tanınan kişiler bakımından nisbi delil değerlendirme yasağı geçerlidir. Bu çerçevede bu karar ile elde edilen verilerden, temelde yatan güven ilişkisinin öneminin göz önünde bulundurulması suretiyle, söz konusu olayın gerçeklerinin araştırılması veya suçlanan kişinin nerede olduğunun tespit edilmesindeki menfaatle orantısız olmaması halinde yararlanılabilir. Dolayısıyla burada yapılması gereken değerlendirme kapsamında müdahalenin ağırlığı devletin suçun soruşturulması ve kovuşturulmasındaki menfaati açısından tartılmalıdır[845].

ii. Şekli koşullarda eksiklikler

Tedbire yönelik karar alınması sırasındaki esaslı şekli eksiklikler elde edilen bilgilerin kullanılamaz hale gelmesine yol açabilir. Örneğin, online arama kararı vermeye yetkilendirilmiş bölge eyalet mahkemesi dairesi tarafından kararın verilmemesi ya da gecikmesinde sakınca bulunan hallerde mahkeme başkanının yerine

[843] Kochheim, KriPoZ 2/2018, S. 67.
[844] BVerfGE109, 279 (331) _ NJW 2004, 999 (1003).
[845] Grossmann, JA 2019, 241, Rn. 247.

savcılık tarafından kararın verilmesi durumunda bir delil değerlendirme yasağı kabul edilir[846].

Bununla birlikte, Alman CMK m. 100d/5-1 uyarınca online arama mesleki gizlilik sebebiyle tanıklıktan çekinme hakkı olan kişilere uygulanamadığından, aksi bir durumda elde edilen bilgiler delil değerlendirme yasağı teşkil eder ve kesinlikle yargılamada kullanılamaz[847].

Online aramanın uygulanma şekliyle ilgili olarak mahkeme kararına uyulmaması halinde, bunun kullanılıp kullanılamayacağını münferit davanın koşulları belirler. Bu bağlamda kararın süresine ilişkin eksiklikler bakımından, örneğin ilk karar ile uzatma kararı arasında kazara kısa süreli bir boşluğun bulunması gibi kısa süreli aşımlar delilin değerlendirilmesine ilişkin bir yasak niteliği taşımamaktadır[848]. Ancak bu iki karar arasındaki boşluğun sadece birkaç saat veya birkaç gün kadar olması gerektiği vurgulanmaktadır[849]. Kararda herhangi bir sürenin belirtilmediği hallerde, yasal süre sınırının aşılıp aşılmadığına bakılır[850].

Temel hakların etkili bir şekilde korunmasını ve mahkemedeki delillerin güvenilirliğini sağlamaya hizmet eden rapor tutma yükümlülükleri bakımından ise, bunların bilinçli ve/veya ciddi şekilde ihlal edilmesi halinde delil değerlendirme yasağı söz konusu olabilmektedir. Zira rapor tutma yükümlülükleri mahkemeye, sanığa ve müdafiine, online aramanın maddi açıdan kabul edilebilirlik şartlarına uygunluğunu gözden geçirme fırsatı vermeyi amaçlar[851].

Yazılı şekil şartı gibi diğer basit ihlaller genellikle delillerin değerlendirilmesinin yasaklanmasıyla sonuçlanmaz[852]. Buradaki ölçü bunların ciddi, bilinçli veya keyfi usul ihlalleri olmaması gerekliliğidir[853].

iii. Maddi koşullarda eksiklikler

[846] BGHSt 35, 32 (33); BGH NStZ-RR 2002,, 176; BeckOK StPO/Graf § 100b Rn. 48; MüKoStPO/Rückert, § 100b Rn.82; Hauck in Löwe-Rosenberg, 100b Rn. 137.
[847] BeckOK StPO/Graf § 100b Rn. 48.
[848] BGHSt 44, 243 (249, 250).
[849] MüKoStPO/Rückert, § 100b Rn.83.
[850] BGHSt 53, 294 (300) = NJW 2009, 2463 (2464).
[851] MüKoStPO/Rückert, § 100a Rn. 351.
[852] BGH NStZ 1996, 48; BVerfG BeckRS 2001 30217941; BeckOK StPO/Graf StPO §100 b Rn. 49.
[853] BverfG BeckRS 2005, 27151; BeckOK StPO/Graf StPO §100 b Rn. 49.

Bir katalog suçuna yönelik eksiklikler bakımından, farklı olasılıklar söz konusu olabilir. Online arama kararının verildiğinde belirli olgulara dayanan bir katalog suç şüphesinin bulunmadığı hallerde, elde edilen bilgiler delil olarak kullanılamaz[854].

Ancak, ceza yargılaması sırasında bir online arama kararı için yasal gerekliliklerin değişmesi halinde, başlangıçta mümkün olmayan izleme tedbirinin meydana gelen değişiklik sonucunda uygulanması halinde, buradan elde edilen deliller değerlendirilebilir[855].

Öte yandan, bir varsayım hatası nedeniyle yanlışlıkla bir katalog suçuna yönelik şüphenin varsayılması ve somut olayın olgularının başka bir katalog suç şüphesini haklı çıkarması halinde, bu hata zararsızdır[856].

Aynı şekilde online arama kapsamındaki kararın dayandırıldığı katalog suçlara ilişkin şüphenin daha sonra gerekli kesinlikte doğrulanmaması halinde, online aramanın temelde yatan iddialarla yakın bağlantısı olan ciddi suçlara ilişkin delil sağlaması halinde de delil değerlendirme yasağı yoktur[857]. Ancak katalog suçu ile bağlantılı olmayan başka suçlar bakımından elde edilen delillerin değerlendirilmesi mümkün değildir[858].

Belirli olgulara dayanan bir şüphenin varlığını değerlendirirken, kanun hâkime bir takdir yetkisi tanımaktadır. Bir online arama kararının ancak bu takdir alanını aşması ve bu nedenle kararın makul olmaması halinde hukuka aykırılığı kabul edilir ve bu nedenle delil olarak değerlendirilmesi mümkün olamamaktadır. Ancak bu durumda, delilin kullanımının yasaklanması ancak sanığın kullanıma zamanında itiraz etmesi halinde düşünülebilir[859].

Modern bilişim sistemlerinde işlenen büyük, çeşitli ve önemli veri miktarları nedeniyle, tedbirin ölçülülüğü, özellikle toplanan veri miktarı bakımından, diğer gizli izleme tedbirlerine kıyasla daha da önemlidir. Buna göre, ölçülülük ilkesinin ihlal edilmesi halinde temel haklar bakımından gerçek bir tartım hatasının bulunması durumunda, delillerin kullanılmasının yasaklanması varsayılmalıdır[860]. Bu örneğin

[854] BGHSt 31, 304 (308, 309); BGHSt 47, 362 (365).
[855] BGH NJW 2009, 791 (792); BeckOK/Graf StPO §100 b Rn. 50.
[856] BGH NJW 2003, 1880 (1881); Grossmann, JA 2019, 241 (247).
[857] BGHSt 28, 122 (127, 128).
[858] BeckOK/Graf StPO §100 b Rn. 50.
[859] BGH NJW 2006, 1361 (1362) = NStZ 2006, 402; BeckOK/Graf StPO §100 b Rn. 51.
[860] MüKoStPO/Rückert, § 100b Rn.86.

veri miktarının orantılılık açısından yanlış ağırlıklandırılmasını içerebilir veya gizlilik veya etki alanı gibi diğer önemli dengeleyici faktörlere uyulmamasını içerebilir[861].

Kararın gerekçelendirilmesindeki hatalar genellikle elde edilen bulguların kullanılamayacağı ve dolayısıyla delil yasağı anlamına gelmemektedir[862]. Bu durumda hakim, kararın verildiği tarihi dikkate alarak soruşturmanın durumunu yeniden gözden geçirmeli ve kararın haklılığını bu temelde analiz etmelidir[863]. Bu durumda elde edilen deliller ancak kararın genel olarak anlaşılabilir olması ve kararın uygulanabilirliğine yönelik önemli şüphelerin bulunmaması halinde değerlendirilebilir[864].

İkincillik ilkesi gereği başka tedbirlerin öncelikli olarak kullanılabilirliği bakımından hakimin takdir yetkisi bulunmaktadır. Takdir yetkisinin aşıldığı hallerde ise delil değerlendirme yasağı kabul edilebilir[865]. Delil değerlendirme yasağı ancak sanığın kullanıma zamanında itiraz etmesi halinde söz konusu olur[866].

Online arama kararının uygun olmayan delillere dayanarak verilmesi halinde, eğer karar başka delillere istinaden de verilebilir olsaydı, elde edilen deliller yargılamada yasağa tabi olmayıp değerlendirilebilir[867].

c. Tesadüfen elde edilen veriler

Usulüne uygun olarak emredilen bir online arama sırasında asıl yargılamayla doğrudan ilgili olmayan ancak diğer yargılamaların gerçekleştirilmesine ve dolayısıyla başka soruşturmaların başlatılmasına sebep olabilecek tesadüfen bilgi elde edildiği hallerde, bu bilgiler Alman CMK m. 477/2 gereği kullanım ve yararlanma hükmüne uygun olarak diğer katalog suçların soruşturulması için aktarılabilir[868].

Bu düzenleme, varsayımsal ikame müdahalesi fikrine dayanmaktadır[869]. Buna göre, Ceza Muhakemeleri Usulü Kanunu uyarınca bir tedbire yalnızca belirli suçların işlendiği şüphesiyle izin veriliyorsa, bu tür bir tedbir sonucunda elde edilen kişisel veriler, tedbirden etkilenen kişilerin rızası olmaksızın, yalnızca bu Kanun uyarınca soruşturulması için böyle bir tedbire hükmedilebilecek suçların soruşturulması için

[861] MüKoStPO/Rückert, § 100b Rn.86.
[862] BGH NVwZ 2006, 1327 (1328); BGHSt 47, 362 (367); BeckOK/Graf StPO §100 b Rn. 52.
[863] BGH NJW 2009, 791 (792).
[864] LG Kiel StV 2006, 405 (406); BeckOK/Graf StPO §100 b Rn. 52.
[865] BGHSt 41, 30 (35f.).
[866] BGH NJW 2006, 1361 (1362) = NStZ 2006, 402; BeckOK/Graf StPO §100 b Rn. 53.
[867] BGH BeckRS 2015, 1573; BeckOK/Graf StPO §100 b Rn. 54.
[868] BeckOK/Graf StPO §100 b Rn. 59.
[869] BT-Drucksache 16/5846, S.66.

diğer ceza yargılamalarında delil olarak kullanılabilir[870]. Burada esas belirleyici unsur, tedbire karar veren hâkimin ceza yargılaması temelinde varsayımsal bir değerlendirmede hiç şüphesiz buna uygun bir arama emrini verip vermemesidir[871].

Tesadüfen elde edilen bilgilerin dışında, örneğin tedbire maruz kalan kişinin sızılan bilgi teknolojisi sisteminin mikrofon işlevini etkinleştirdikten sonra yaptığı konuşmalar gibi online arama tedbiriyle dolaylı olarak elde edilmiş veriler de söz konusu olabilmektedir. Bu durumda elde edilen veriler yalnızca online aramanın yanı sıra kaynak telekomünikasyon yoluyla yapılan iletişimin denetlenmesine yönelik bir dinleme emri de verilmişse kullanılabilir.

Bununla birlikte ses kayıtları da dahil olmak üzere görüntü ve video kayıtları, ancak Federal Almanya Anayasası'nın 13/1 maddesi ile korunan alanda, yani konutta yapılmamışsa, özel hayatın çekirdek alanının ihlali hariç tutulmuşsa ve konut dışında akustik veya optik izleme için bir kararın bulunması halinde delil yasağı niteliği taşımamaktadır[872].

Son olarak bu çerçevede "smart speaker" olarak bilinen Google Home ve Amazon Alexa gibi dijital asistanların elde ettikleri verilerin delil yasağı oluşturup oluşturmamasına değinmekte fayda olacaktır. Bu dijital asistanlar sesli komut ile örneğin müzik çalabiliyor, görüşme ayarlayabiliyor, evdeki ışık veya ısınma sistemini düzenleyebiliyor. Bunlar ayrıca internette alışveriş yapmak veya bilgi edinmek için veya kısa mesajlar ve görüntülü aramalar yoluyla bir iletişim aracı olarak da kullanılabilir[873]. Bu dijital asistanların işleyici bakımından ifade edilmelidir ki, bunlar bulundukları alanda konuşulanları sürekli olarak değerlendirir ve ses dizisini servis sağlayıcının sunucusuna iletir. Komutlar buradaki bulutta analiz edildikten sonra, talimat yerine getirilir. Dijital asistan niteliğindeki bir bilgi teknolojisi sisteminin online aranması ile tedbire maruz kalan hedef kişinin yanı sıra bilinmeyen diğer kişilerin de etkilenmesi söz konusu olabilecektir. Zira sesli komutların türü önceden bilinmediğinden, iletişimi oluşturan bileşenlerle karşılaşılacağı her zaman tahmin edilmelidir. Bu durumda elde edilen bilgilerin kullanılabilirliği ancak özel hayatın çekirdek alanını ilgilendirmeyen bilgiler bakımından ve online arama emrine ek olarak

[870] BVerfG, 18.3.2009 – 2 BvR 2025/07 Rn. 18.
[871] BGH, 26.4.2017 – 2 StR 247/16 Rn. 40; Kochheim, KriPoZ 2/2018, S. 68.
[872] Roggan, StV 2017, 821 (826).
[873] Soine, NStZ 2018, 497 (504).

konutun gözetimi ve telekomünikasyon yoluyla iletişimin denetlenmesi tedbiriyle mümkün olabilecektir[874].

d. Yurt dışındaki bilgi teknolojisi sistemlerinde kaydedilmiş veriler

(1) Devlet egemenliği sorunu

Soruşturma ile ilgili verilerin, genellikle bir bulut sağlayıcısının sunucusu gibi yurt dışındaki bir veri depolama cihazında saklanması halinde, soruşturma makamları uluslararası istinabe olarak tanımlanan adli yardımlaşma seçeneklerine sahiptir. Avrupa Birliğinde ise "Avrupa Soruşturma Emrine" başvurulabilir[875].

Bunun dışında yurtdışında bulunan verilere doğrudan erişim, buna ilişkin herhangi bir uluslararası anlaşma bulunmaması sebebiyle, uluslararası hukuka aykırı olarak kabul edilmektedir[876]. Böyle bir durumda yabancı devletin egemenliğine karşı bir ihlal söz konusu olur. Bu nedenle Alman cezai yargı yetkisi ve buna bağlı olarak devletin olayları aydınlatmaya yönelik yetkileri ulusal sınırlarda sona erer. Yurtdışından delil elde edilmesi gerektiği anda, soruşturma makamı uluslararası adli yardımlaşma yoluna başvurmalıdır.

Bunun ötesinde AB Siber Suçlar Sözleşmesinin de online bağlamında doğrudan gizli erişim için bir yetki vermediğini ifade edebiliriz. Sözleşmenin 32. Maddesi *"İzin Verilmiş veya Kamuya Açık Olma Durumu Söz konusu Olduğunda, Depolanmış Bilgisayar Verisine Trans-border Erişimi"* düzenlemektedir. Buna göre, yetkili makamlar, sözleşmenin tarafı olan diğer bir devlet topraklarında bulunan kamuya açık depolanmış bilgisayar verilerine, bu topraklardaki bir bilgisayar sistemi aracılığıyla erişebilir veya bu bilgisayar sistemi aracılığıyla verileri kendilerine iletmeye yasal olarak yetkili olan kişinin rızasını alarak bu verileri alabilir. Ancak online arama ile bir taraftan kamuya açık olmayan verilere erişim sağlanmak istenilirken diğer taraftan ise online arama tedbirinin doğası gereği gizli olan erişim tedbire maruz kalan kişinin rızası dışında gerçekleşir[877].

Ayrıca AB Siber Suçlar Sözleşmesi'nin ikinci ek protokolü *"Saklanan bilgisayar verilerinin acil bir durumda hızlandırılmış ifşası"* başlığını taşıyan 9.

[874] Soine, NStZ 2018, 497 (504).
[875] MüKoStPO/Rückert, § 100b Rn. 94.
[876] Zerbes/EGhazi NStZ 2015, 425 (430).
[877] Park, §4 Durchsuchung und Beschlagnahme im EDV Bereich, Rn. 937.

maddede telekomünikasyon ve tele medya sağlayıcılarının içerik verilerine sınır ötesi erişim için Siber Suçlar Sözleşmesinin 35. maddesine göre 24-7 ağı olarak tanımlanan ulusal temas noktaları aracılığıyla çok hızlandırılmış bir adli yardım yolu içermektedir. Ancak bu düzenleme ile de doğrudan erişim imkânı sağlanmamaktadır[878].

Dolayısıyla online arama bağlamında güncel hukuki durum dikkate alındığında, devletlerin egemenliklerini ihlal etmeden yurtdışındaki bir sunucuya erişmek mümkün değildir. Ancak bu durum eleştirilmektedir, zira tedbire maruz kalmaktan çekinenler, verilerinin depolandığı yeri yurtdışına taşıyarak online aramadan kaçabilirler[879].

Yurtdışındaki veri depolama sağlayıcılarına doğrudan erişim sağlanarak devletlerin egemenliklerinin ihlal edilmesi halinde, erişilen devletin bu delil kullanımına açıkça itiraz etmesi ve adli yardımı reddetmesi durumunda, delillerin kullanılması kesinlikle mümkün değildir[880].

Bunun dışında hukuki sürece uyulmayarak, yani adli yardımlaşmaya başvurmadan doğrudan erişim ile devletlerin egemenliklerinin ihlal edilmesi, genel olarak delillerin kullanılmasının yasaklanmasına yol açmamaktadır. Nitekim bu durum sanığın temel haklarla korunan menfaatlerini değil, yabancı devletin egemenlik haklarını etkiler. İçtihat hukukunun geliştirdiği değerlerin tartımı teorisi burada da geçerlidir. Buna göre, kural olarak, yalnızca bilinçli, keyfi veya ciddi hatalı ihlaller delil kullanımının yasaklanmasına sebep olabilir[881].

Online arama bakımından, çoğu bulut sağlayıcıları gibi veri depolama sağlayıcılarının verilerinin yurt dışında depolandığı ifade edilmektedir. Bu nedenle soruşturma makamları depolama sağlayıcılarına erişmek istedikleri takdirde, bunların yurt dışında bulunabileceği ihtimalini dikkate alarak nerede bulunduklarını araştırmalıdır. Bunun teknik veya soruşturma nedenleriyle mümkün olmaması durumunda ve yukarıda belirttiğimiz bilinçli, keyfi veya ciddi hatalı bir ihlalin bulunmaması sebebiyle genellikle bir delil değerlendirme yasağı kabul edilmez. Öte yandan, verilerin yurt içi veya yurt dışında bulunduğuna dair herhangi bir değerlendirmenin yapılmadığı hallerde, soruşturma yetkilisi egemenliğin ihlalini

[878] MüKoStPO/Rückert, § 100b Rn. 94a.
[879] Park, §4 Durchsuchung und Beschlagnahme im EDV Bereich, Rn. 937.
[880] BGH 8.4.1987 – 3 StR 11/87, BGHSt 34, 334 (344) = NJW 1987, 2168.
[881] BVerfG 9.11.2010 – 2 BvR 2101/09, NStZ 2011, 103.

bilinçli olarak göze alır ve bu surette genel olarak delillerin kullanılmasına ilişkin bir yasak söz konusu olabilmektedir[882].

Bu durum daha sonra adli yardım talebinde bulunulması ve yabancı devletin delil kullanımına itiraz etmemesi halinde değişebileceği gibi varsayımsal olarak yasal ikame müdahale fikri ile de değişkenlik gösterebilir. Yabancı devletin toplanan verileri teslim etmesi için gerekli koşullar yerine getirilmişse ve adli yardım talebinde bulunulması halinde yabancı devletin de verileri teslim edebileceği varsayılıyorsa, delillerin kullanılmasına ilişkin bir yasağın söz konusu olmadığına karar verilmiştir[883].

(2) Encro-Chat (Kripto Mesajlaşma) ile Bağlantılı Delillerin Değerlendirilmesi

Yabancı yargılamalarda elde edilen delillerin Alman Ceza yargılamalarında kullanılabilirliği bakımından "Encro-Chat" adı altında bilinen kripto mesajlaşma yoluyla elde edilen veriler Alman Yargısını 2020 yılı itibariyle yakından ilgilendirmiştir.

Şubat 2022'de Federal Yargıtay Mahkemesi 6. Ceza Dairesi, Encro-Chat verilerinin ceza yargılamalarında delil olarak kullanımını ilk kez ilkel bir şekilde ele almış ve delillerin kullanılabileceğine hükmetmiştir[884].

Federal Yargıtay 5. Ceza Dairesi'nin Mart 2022'de verdiği ikinci bir kararda, mahkeme Encro-Chat aracılığıyla elde edilen verilerin kullanılabilirliği konusunu ayrıntılı olarak ele almış, verilerin kullanımının uluslararası ceza hukuku, anayasa hukuku ve ceza muhakemesi hukuku çerçevesinde meşru olduğunu belirtmiştir[885].

Temmuz 2022'de Federal Yargıtay mahkemesinin 4. Ceza Dairesi, verilerin kullanılabilirliğine ilişkin bir karar daha vermiştir. Bu çerçevede Fransız makamları tarafından kripto mesajlaşma hizmeti aracılığıyla telekomünikasyonun izlenmesinden elde edilen bulgular, ağır cezai suçların soruşturulmasına hizmet etmeleri halinde Alman ceza yargılamalarında delil olarak kullanılabilecektir[886].

Federal Yargıtay mahkemesi Encro-Chat verilerinin ceza yargılamalarında kullanılabileceklerinin hangi gerekçelere dayandırdığını incelemeden önce Encro-

[882] MüKoStPO/Rückert, § 100b Rn. 95.
[883] BGH 21.11.2012 – 1 StR 310/12, NStZ 2013, 596.
[884] BGH Beschluss v. 8.2.2022 – 6 StR 639/21; BGH BeckRS 2022, 2981 NJW-Spezial 2022, 216.
[885] BGH Beschluss v. 2.3.2022 – 5 StR 457/21; BGH BeckRS 2022, 5306.
[886] BGH Beschluss v. 6.7.2022 – 4 StR 63/22

Chat hakkında genel bilgiler verilip, bu çerçevede Enco-Chat'in özellikle nasıl işlediği ortaya koyulacaktır.

(a) Encro-Chat Hakkında Genel Bilgiler

Encro-Chat, 2015 yılında Avrupa da kurulmuş bir şifreli iletişim teknolojisi sağlayıcısı olup, teknik olarak değiştirilmiş akıllı telefonlar (kripto telefonlar) ile bir iletişim uygulaması (Encro-Chat) sunmaktaydı. Kullanıcıları arasındaki iletişim yalnızca kısa mesajlar aracılığıyla gerçekleşebiliyor ve yalnızca Encro-Chat kullanıcıları arasında kurulabiliyordu[887].

Encro-Chat'in amacı, şifrelenmiş kısa mesajlar aracılığıyla mümkün olabildiğince güvenli bir şekilde iletişim kurabilmekti. Bu amaçla kripto telefonlardan GPS sensörleri, mikrofonlar, kameralar gibi şifreli mesajlaşma için gerekli olmayan tüm bileşenler çıkarılmıştır[888]. Dolayısıyla saf iletişim için gerekli olmayan, ancak örneğin gizli dinleme yoluyla kullanıcıların yerini tespit etmeyi veya izlemeyi mümkün kılan tüm cihaz bileşenleri kaldırılmıştır.

Cihazlar özellikleri sebebiyle anonimlik garantisi ile satılmıştır[889]. Zira cihaz veya SIM kart ile kullanıcısının hesabı arasında hiçbir bağlantı bulunmamaktaydı[890]. Bununla birlikte kripto telefonlarda "panik pin kodu" olarak adlandırılan bir şifrenin girilmesinin ardından kısa bir süre içinde tüm içeriğin silinmesi için kullanılabilen bir silme işlevi de bulunmaktaydı[891].

Ayrıca Encro-Chat yazılımı uçtan uça şifrelemeye sahiptir. Bu nedenle tüm iletim istasyonlarında iletilen verilerin şifrelenmesi söz konusu olup, yalnızca iletişim ortakları, yani iki kripto telefonun başındaki kullanıcılar iletinin şifresini çözebilmekteydi[892].

Belirtilen tüm özellikler ve şifreleme teknolojisi nedeniyle, soruşturma makamlarının hizmet aracılığıyla yapılan iletişimlere erişmesi veya cihazların içeriğini okuması veya düzenlemesi imkansızdı. Encro-Chat ürünleri için resmi satış noktaları bulunmuyor, sadece anonim kanallar üzerinden altı aylık kullanım süresi için 1610

[887] Kipker/Bruns, MMR 2022, 363.
[888] LG Bremen Urteil vom 29.7.2022 – 3 KLs 370 Js 17306/21 (2/22), BeckRS 2022, 43017 Rn. 1, Beschluss des LG Berlin vom 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22); Heermann, ZD-Aktuell 2022, 01213.
[889] Derin/Singelnstein NStZ 2021, 449; Gebhard/Michalke, NJW 2022, 655; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 550.
[890] Beukelmann, NJW-Spezial 2022, 248.
[891] BGH, Beschl. 2.3.2022 – 5 StR 457/21 NStZ 2022, 435 (436); Beukelmann, NJW-Spezial 2022, 248.
[892] Kipker/Bruns, MMR 2022, 363 (364).

avroya ve yalnızca nakit olarak temin edilebiliyorlardı. Ayrıca kayıtlı bir şirketin veya şirket yetkililerin bulunması da mümkün değildi[893].

Fransa da 2017 ve 2018 yıllarında yürütülen bazı soruşturmalarda şüphelilerin Encro-Chat aracılığıyla organize uyuşturucu kaçakçılığı yaptıklarına dair göstergelere rastlanmıştır[894]. Ancak soruşturma makamlarının ele geçirdikleri telefonların şifreleme nedeniyle okunması mümkün olmamıştır. Şüphelilerin bu kriptolu cep telefonlarını uyuşturucu kaçakçılığı ile bağlantılı olarak kullandıklarını itiraf etmeleri ve bu cihazların uyuşturucu kaçakçılığı ve organize suçlarla ilişkili olarak tekrar tekrar ortaya çıkması üzerine Fransız soruşturma yetkilileri konuyu yakından takibe almıştır[895].

Bunun neticesinde, suç işlemek amacıyla kurulmuş bir suç örgütü ve bir şifreleme cihazının izinsiz temini, transferi ve ithalatı şüphesiyle soruşturma başlatılmıştır. Bu kapsamda Encro-Chat kullanıcıları arasındaki şifreli iletişimin Fransa da işletilen bir sunucu üzerinden yürütüldüğü tespit edilmiştir[896].

Bunun üzerine Fransız mahkemesinin izniyle sunucudaki verilere erişilip, bunun sonucunda Hollandalı bir sağlayıcıya ait 66.134 SIM kartın sisteme kayıtlı olduğu ve bunların çok sayıda Avrupa ülkesinde kullanıldığı ortaya çıkmıştır[897]. Ayrıca toplam 121 ülkede aktif olan 32.477 kripto-telefonu tespit edilmiştir[898]. Bu çerçevede Encro-Chat'in en sık kullanıldığı beş ülke sırasıyla Hollanda, İspanya, Birleşik Krallık, Almanya ve İtalya olarak belirlenmiştir[899].

Fransız soruşturma yetkilileri hem Encro-Chat'in sunucusuna hem de son cihaz olan kriptolu telefonlara casus yazılım yükleyerek depolanan içeriğe erişim sağlamıştır ve devam eden iletişimleri de izleyebilmiştir[900].

Kısa not olarak oluşturulan 3477 metin dosyasının kısmi şifresinin çözülmesi, bunların şüphesiz yasadışı faaliyetlerle, özellikle de uyuşturucu kaçakçılığıyla bağlantılı olduğunu ortaya koymuştur[901]. Fransız savcılığının talebi üzerine Fransa'daki bir mahkeme, 1 Nisan 2020 tarihinden itibaren Fransız sunucusu üzerinden

[893] BGH, Beschl. 2.3.2022 – 5 StR 457/21, NStZ 2022, 435 (436).
[894] BGH, Beschl. 2.3.2022 – 5 StR 457/21, NStZ 2022, 435 (436).
[895] Heermann, ZD-Aktuell 2022, 01213.
[896] Heermann, ZD-Aktuell 2022, 01213.
[897] BGH, Beschl. 2.3.2022 – 5 StR 457/21, NStZ 2022, 435 (436).
[898] Beukelmann, NJW-Spezial 2022, 248.
[899] BGH, Beschl. 2.3.2022 – 5 StR 457/21, NStZ 2022, 435 (436).
[900] LG Berlin NStZ 2021, 696 (697); Derin/Singelnstein NStZ 2021, 449 (450); Gebhard/Michalke, NJW 2022, 655.
[901] Heermann, ZD-Aktuell 2022, 01213.

çalışan ve telefonlarda depolanan verilerin teknik araçlarla izlenmesine izin vermiştir. İlk bulgulara göre, Fransa'da aktif olan telefonların %63,7'si kesinlikle suç amaçlı kullanılırken, geri kalan cihazlar (%36,3) ya kısmen aktif değildir ya da henüz analiz edilmemiştir. Savcılık ve mahkeme, ilk ayda elde edilen verileri analiz ettikten sonra Encro-Chat kullanıcılarının "neredeyse tamamen suçlulardan oluştuğunu" varsaymıştır[902].

Federal Kriminal Dairesinin, Europol aracılığıyla Almanya'daki Encro-Chat kullanıcıları tarafından çok sayıda ciddi suç işlendiğine dair bilgi alması üzerine Frankfurt am Main Cumhuriyet Başsavcılığı Siber Suçlarla Mücadele Merkez Ofisi, kimliği bilinmeyen kişiler hakkında soruşturma başlatmıştır[903]. Almanya ile ilgili Encro-Chat verilerinin aktarılması ve Alman ceza davalarında kullanılmasına izin verilmesi amacıyla 2 Haziran 2020 tarihinde Fransa'ya bir Avrupa Soruşturma Emri için talepte bulunulmuş[904], her iki talep 13 Haziran 2020 tarihinde bir Fransız mahkemesi tarafından onaylanmıştır[905].

Alman makamlarına aktarılan verilerin analiz edilmesi üzerine toplam 3.200 soruşturma başlatılmış olup, 1.400 tutuklama emri verilmiştir. Soruşturma yetkilileri Almanya'da yaklaşık 3.000 Encro-Chat kullanıcısı tespit etmiş, 357 milyon avroluk mal varlığını dondurmuş ve 61 milyon avroluk mal varlığına da el koymuştur. Ayrıca 6,3 tondan fazla esrar, 1.100 kilogramdan fazla kokain, yaklaşık 590 kilogram sentetik uyuşturucu, yaklaşık 73 kilogram eroin ve 158.000'den fazla ecstasy tablet ele geçirilmiştir[906].

(b) Alman ceza yargılamalarında elde edilen verilerin kullanılabilirliği

Fransa'daki soruşturma tedbirleri yoluyla elde edilen verilerin Alman ceza yargılamalarında kullanılabilirliği oldukça tartışmalı bir konudur. Almanya'daki içtihadın çoğunluğu[907] söz konusu verilerin kullanılabilirliği konusunda herhangi bir

[902] BGH, Beschl. 2.3.2022 – 5 StR 457/21, NStZ 2022, 435 (437).
[903] Kipker/Bruns, MMR 2022, 363 (364) Redaktion FD-StrafR 2022, 452559.
[904] Böhm, NJW 2017, 1512.
[905] Beukelmann, NJW-Spezial 2022, 248.
[906] EncroChat-Razzia: 1.400 Haftbefehle gegen Organisierte Kriminalität | Presseportal, Erişim tarihi: 01.06.2024: ; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 550.
[907] OLG Karlsruhe, Beschluss vom 10.11.2021 – 2 Ws 261/21; OLG Rostock, Beschluss vom 11. Mai 2021 – 20 Ws 121/21; OLG Schleswig, Beschluss vom 29.4.2021 − 2 Ws 47/21; OLG Bremen, Beschluss *vom* 18.12.2020 – 1 Ws 166/20.

sorun görmezken, öğretideki hakim görüş[908] bunları delil yasağı kapsamında değerlendirilmesi gerektiğini ileri sürer.

Karşılıklı adli yardımlaşma yoluyla elde edilen delillerin kullanılmasına ilişkin bir yasağın, uluslararası hukuk ilkelerinin, kamu düzeninin ya da karşılıklı adli yardımlaşma kanunu hükümlerinin ihlali gibi karşılıklı adli yardımlaşmaya özgü nedenlerle ortaya çıkabileceğini ya da doğrudan anayasadan veya diğer usul kanunlarından kaynaklanabileceğini belirten Federal Yargıtay, Encro-Chat verileri bakımından bunlardan hiç birinin söz konusu olmadığını belirterek Encro-Chat verilerinin delil olarak Ceza Yargılamalarında kullanılabileceğine hükmetmiştir[909].

Federal Yargıtay elde edilen verilerin ceza yargılamalarında kullanılmasının yasal dayanağının Alman CMK m. 261 olduğunu belirtmektedir. Alman CMK m. 261 uyarınca, hâkimin delilleri serbestçe takdir etmesi ilkesi düzenlenmiş olup, buna göre "ortaya sürülen delillerin sonuçları hakkında mahkeme, duruşmada oluşan serbest kanaatine göre karar verir." Federal Yargıtay, söz konusu düzenlemenin delilin Almanya'da veya karşılıklı adli yardımlaşma yoluyla elde edilip edilmediğine bakılmaksızın geçerli olduğunu, Alman hukukunun adli yardımlaşma yoluyla elde edilen verilerin kullanımına ilişkin herhangi bir kısıtlama öngörmediğini ileri sürmektedir[910].

Bu bağlamda, elde edilen bilgiler, somut olaydaki suçun ciddi olması ve online aramayı düzenleyen Alman CMK m. 100b/2 maddesi anlamında suç kataloğunda bulunan özellikle ağır bir suç teşkil etmesi, soruşturulacak olayların aydınlatılmasının aksi takdirde önemli ölçüde daha zor veya nafile olması ve özel hayatın çekirdek alanının etkilenmemesi halinde, Alman CMK m. 261uyarınca kullanılabilir[911].

Adli yardımlaşma konusunun yanında, Alman CMK m. 100e/6'nın delillerin sınır ötesi kullanımı için uygun bir yasal dayanak olup olmadığı da tartışılmaktadır. Federal Yargıtay, özellikle de gizli erişim tedbirlerine yönelik usuli düzenlemeler içeren Alman CMK m. 100e/6'nın doğrudan uygulanabilir olmadığını, yalnızca ölçülülük kapsamında dikkate alındığını ifade etmektedir[912].

[908] Derin/Singelnstein, NStZ 2011, 449-454; Strate, HRRS 2022, S. 15 ff; Gebhard/Michalke, NJW 2022, 655-659.
[909] BGH Beschluss v. 2.3.2002 – 5 StR 457/21, NStZ 2022, 435 (439).
[910] BVerfG NJW 2012, 907 Rn. 120, 137 vd.
[911] BGH Beschluss v. 2.3.2002 – 5 StR 457/21, NStZ 2022, 435 (443).
[912] BGH Beschluss v. 2.3.2002 – 5 StR 457/21, NStZ 2022, 435 (438).

Federal Yargıtay kararında, delil olarak değerlendirilen verilerin belirli koşullar altında Alman Anayasası'nın 10. maddesi ile korunan telekomünikasyon gizliliğinin ihlalini içerebileceğini, ancak burada Alman CMK m. 100 e/6-1 gibi kullanım kısıtlamaları öngören düzenlemeleri de dahil ederek ölçülülük ilkesini gözettiğinden, verilerin yargılamalarda kullanılabileceğine hükmetmiştir[913].

Bununla birlikte, başka bir devletin egemenlik hakkına izinsiz müdahale gibi uluslararası hukuk ilkelerinin ihlali nedeniyle de delil değerlendirme yasağının söz konusu olmadığı Federal Yargıtay tarafından vurgulanmaktadır. Fransa'nın, sağlanan bilgilerin Alman ceza yargılamalarında kullanılmasına tam ve koşulsuz olarak izin verdiği, bu nedenle uluslararası hukuk kapsamında zorunlu bireysel korumanın açık bir ihlalinin söz konusu olmadığı ifade edilmektedir[914].

Federal Yargıtay mahkemesi ayrıca, insan hakları veya Avrupa hukuku kapsamındaki temel değerlerin ihlali veya karşılıklı adli yardımlaşmada incelenecek "kamu düzeni (ordre public)" anlamında temel hukuk devleti gerekliliklerinin ihlalinin de bulunmadığını ileri sürmektedir. Federal Yargıtay, Fransız soruşturma makamlarının ilk veri erişiminden sonra Encro-Chat tarafından sunulan hizmetin tamamen suç faaliyetlerini desteklemeye yönelik bir ağ olduğunu gösteren bilgilere sahip olmasıyla, soruşturmalarını çok sayıda yabancı ülkedeki Encro-Chat cep telefonu kullanıcılarını da kapsayacak şekilde genişlettiklerini ve ancak bu surette Encro-Chat'in suç amaçlı kullanım kapsamını ve yapısını belirleyebildiklerini vurgulamaktadır[915].

Bunun ötesinde temyiz başvurusunda bulunan kişinin, Avrupa Soruşturma Emri çıkarılmadan önce Fransız ve Alman polis makamları arasında veri alışverişi veya diğer iş birliklerinde karşılıklı adli yardımlaşma anlaşmalarının ihlal edildiğini iddia etmediği belirtilmektedir. Yargıtay, bu tür bir bilgi alışverişinden elde edilen verilerin kullanımına ilişkin gerekliliklerin, Avrupa Soruşturma Emri yoluyla elde edilen verilerin kullanımına ilişkin gerekliliklerden daha katı olmaması nedeniyle bu durumu konu dışı olarak değerlendirmekte ve Fransız veya Alman makamlarının temyiz başvurusu yapan kişinin bireysel haklarını kasıtlı veya sistematik olarak engellediğinin açıkça ortaya konulmadığını veya kanıtlanmadığını savunmaktadır[916].

[913] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 551.
[914] BGH Beschluss v. 2.3.2002 – 5 StR 457/21, NStZ 2022, 435 (439).
[915] BGH Beschluss v. 2.3.2002 – 5 StR 457/21, NStZ 2022, 435 (440).
[916] Heermann, ZD-Aktuell 2022, 01213.

Literatürün büyük bir kısmını temsilen Singelnstein[917], Encro-Chat verilerinin ceza yargılamalarında kullanılamamasının başlıca sebepleri olarak, Fransız makamlarının tedbirlerinin, müdahalelerinin yoğunluğu ve kapsamı bakımından Alman hukuku çerçevesinde izin verilebilecek olanın çok ötesine gittiğini; özellikle, online arama tedbirini düzenleyen Alman CMK 100 b maddesi uyarınca bir online aramaya eşdeğer olarak yorumlanamayacaklarını belirtmektedir. Rastgele bulguların sistematik olarak araştırılmasını amaçlayan şüpheden bağımsız, hedefsiz ve geniş bir alana yayılmış gizli kitle gözetiminin, cezai bir usul tedbirinden ziyade istihbarat servisinin bilgi toplaması olarak tanımlanabileceği ve kesinlikle buna dayanarak soruşturmaların başlatılmasının Alman Ceza Muhakemeleri Usulü Kanunu'nda herhangi bir yasal dayanakla desteklenemeyeceği ve anayasal değerlerle bağdaştırılamayacağı ileri sürülmektedir[918].

Sonuç olarak, bu şekilde elde edilen verilerin Alman ceza yargılamalarında farklı bir amaç için kullanılmasının da anayasal ve cezai usulün ön koşulundan yoksun olduğu, yani kullanılacak verilerin Alman ceza yargılaması için tekrar elde edilmesi gerektiği vurgulanmaktadır.

Alman hukuk sisteminde böyle bir tedbirin düzenlenmemesi sebebiyle bu tedbirden elde edilen verilerin Alman ceza yargılamalarında kullanılamayacağı; Fransız makamları tarafından gerçekleştirilen tedbirin Alman hukuku kapsamında hiçbir koşulda gerçekleştirilmemesi gerektiği açık olmakla birlikte, Encro-Chat'ten elde edilen verilerin çok sayıda Alman ceza yargılamasında kullanılıyor olmasının endişeye yol açtığı belirtilmektedir[919].

Ortaya çıkarılan suçların ciddiyetine yapılan atfın, verilerin kullanımına ilişkin yasal gerekliliklerin eksikliğini telafi etmediği, bu uygulamanın artık tek seferlik istisnai bir vaka olmadığı, Encro-Chat'ten sonra dinlemeye karşı korumalı olarak pazarlanan diğer iletişim hizmetleri sağlayıcılarına da benzer yöntemlerle sızıldığı ve güvenli iletişime karşı bu tür hedefli eylemlerin kabul edilmemesi gerektiği eleştirilmektedir[920].

Bu noktada, Fransız Ceza Muhakemesi Kanunu'nun temel hak ve özgürlüklere Alman Ceza Muhakemesi Kanunu'ndan daha fazla müdahale ettiğini vurgulamak

[917] Derin/Singelnstein, NStZ 2021, 449-454.
[918] Derin/Singelnstein, s. 451.
[919] Derin/Singelnstein, s. 452.
[920] Derin/Singelnstein, s. 453.

gerekir. 2023 yılında Fransız Ceza Muhakemesi Kanunu'na, ses ve görüntü kayıtlarının uzaktan etkinleştirilmesi ve teknik cihazlara erişilerek yerlerinin tespit edilmesi yoluyla elektronik cihazlardan delil elde edilmesini sağlayan düzenleme getirilmiştir[921]. Özellikle terör suçları ve organize suçlarla bağlantılı soruşturmalarda Fransız soruşturma makamları tarafından başvurulabilen "uzaktan etkinleştirme" suretiyle erişim yöntemi Almanya'da mümkün değildir.

Sonuç olarak, Encro-Chat verilerinin Alman Ceza yargılamalarında kullanılabilirliğine ilişkin Federal Anayasa Mahkemesine toplam beş bireysel başvuru gerçekleşmiş olup[922], henüz hüküm verilmemiştir. Encro-Chat ile ilgili çok sayıda dava göz önünde bulundurulduğunda, söz konusu verilerin kullanılmasına ilişkin dönüm noktası niteliğinde bir kararın kesinlikle faydalı olacağı kanaatindeyiz.

19 Ekim 2022 tarihinde Berlin Bölge Mahkemesi, Encro-Chat verilerinin Alman ceza yargılamalarında kullanılabilirliği konusuna açıklık getirmek üzere bir Encro-Chat davasını Avrupa Adalet Divanının huzuruna taşımıştır[923]. Avrupa Adalet Divanı, 30 Nisan 2024 tarihli kararında Encro-Chat'ten elde edilen verilerin kullanımına ilişkin gerekliliklere açıklık getirmiştir[924].

Buna göre, bir savcı Avrupa Soruşturma Emri aracılığıyla belirli koşullar altında verilerin bir üye devletten diğerine aktarılmasını emredebilir. Bunu yapmak için, savcılık "halihazırda elde edilmiş olan delillerin iletilmesi emrini vermekten", "iç hukuktaki soruşturmalarda yetkili" olması gerekmektedir. Bu durumda bir hâkimin açık iznine gerek kalmayacaktır. Ayrıca, emri veren üye devlette delillerin elde edilmesine ilişkin şartların yerine getirilmesi gerekmez.

Ancak, temel haklara riayet edilip edilmediğinin mahkemede kontrol edilmesi mümkün olmalıdır. Buna ek olarak, izlemenin gerçekleştirildiği Üye Devlet zamanında bilgilendirilmelidir. Üye devlet daha sonra izleme tedbirine itiraz edebilir, ki bu, üye devletlerin egemenliğine ve bireyin korunmasına hizmet eder. Ayrıca, ceza mahkemesi, "ilgili kişi bu konuda yorum yapabilecek durumda değilse" ve bu delil gerçeklerin değerlendirilmesini önemli ölçüde etkileyebilecekse, delili dikkate almamalıdır.

[921] Detaylı bilgi için bkz. Murat Balcı/Kerim Çakır, Investigation Authorities' Ability to Secretly Obtain Evidence From Electronic Devices Through Remote Activation in the French Penal Procedural Code, Bilişim Hukuk Dergisi 2023/2, s. 127 vd.
[922] BVerfG Az. 2 BvR 684/22; 2 BvR 1832/22; 2 BvR 2143/22; 2 BvR 64/23; 2 BvR 1008/23
[923] LG Berlin, Beschluss vom 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22).
[924] EuGH, 30.04.2024 - C-670/22.

Avrupa Adalet Divanı'nın kararının, sınır ötesi ceza yargılamalarında iş birliği ve veri alışverişi için yasal zeminin netleştirilmesine yardımcı olduğunu ifade edebiliriz. Genel olarak, Avrupa Adalet Divanının açıklamalarının Avrupa Soruşturma Emri normlarının bireyi koruyan niteliğini de ortaya koyduğu, ilgili tarafların temel haklarının korunmasını sağlarken aynı zamanda Avrupa Birliğinde cezai soruşturmaların etkinliğini de desteklediğini göstermektedir. Berlin Bölge Mahkemesi Adalet Divanının kararı ışığında Encro-Chat verilerinin delil olarak kullanılıp kullanılamayacağına karar vermelidir.

Son olarak Encro-Chat verilerinin ceza yargılamalarında kullanılabilirliğine ilişkin Avrupa İnsan Hakları Mahkemesine de iki tane başvuru yapıldığı, ancak henüz karar verilmediği belirtilmelidir[925].

D. Online Aramanın Uygulaması, istatistiksel rakamlar

Online aramanın teknik açıdan karmaşık bir müdahale tedbiri olması, hedef sistemin teknik ortamının iyi bir şekilde hazırlanmasını ve araştırılmasını gerektirmesi sebebiyle, online aramanın 2017 yılında adli amaçlı Alman Ceza Muhakemesi Kanunu'na eklendiğinde, uygulamada çok az sayıda uygulanacağı varsayılmıştır[926]. Özellikle de arama yazılımının tedbire maruz bırakılmak isteyen kişinin bilgi teknoloji sistemine yüklenmesinin zorlu bir süreç olduğu belirtilmiştir[927].

Bununla birlikte uygun yazılım geliştirmenin zorlukları da vurgulanmış, örneğin, Federal Başsavcılık 2019 yılında 550'den fazla terör suçlarıyla ilgili soruşturma başlattığını, ancak bilgi teknoloji sistemi niteliğindeki hedef cihaz için uygun yazılım geliştirmenin "büyük bir teknik çaba" gerektirdiğini, bu soruşturmaların hiçbirinde online arama tedbirine başvurulmadığını açıklamıştır[928].
Önleyici online aramaların istatiksel rakamları, gizli veri olarak sınıflandırılmaları sebebiyle açıklanmamaktadır. Buna karşılık, adli tedbir niteliğindeki online aramalar bakımından Alman Ceza Muhakemesi Kanununda özel olarak düzenleme[929] yapılmıştır.

[925]EGMR v. 3.1.2022 – Nr. 44715/20; 47930/21.
[926] Kochheim, KriPoZ 2/2018, S. 63; Sinn, Stellungnahme zum Entwurf 18/11272, s. 9.
[927] Sinn, Stellungnahme zum Entwurf 18/11272, s. 9.
[928] Flade, Florian, Überwachungssoftware: Der Bundestrojaner, den keiner nutzt | tagesschau.de, Erişim tarihi: 01.06.2024:
[929] §101b/1, 3 Alman CMK

Bu çerçevede, istatistiksel kayıt tutma ve raporlama yükümlülükleri getirilmiş olup, Federal Adalet Dairesi *("Bundesamt für Justiz")* tarafından uygulanmış olan tedbirlerin tablo halinde internette yayınlanacağı düzenlenmiştir. Buna göre özellikle raporlanması istenilen hususular aşağıdaki gibidir:

- Online arama için hâkim emri bulunan dava sayısı,
- İlk ve yenileme emirleri olarak ayrılmış gözetim emirlerinin sayısı,
- Her bir vakanın altında yatan suç,
- Soruşturulan kişinin bilgi teknolojisi sistemine izinsiz erişimin fiilen gerçekleştirildiği dava sayısı.

18.12.2020 tarihinde ilk kez 2019 yılı kapsayacak şekilde rapor açıklanmıştır. 2019 yılı öncesinde ise adli tedbir niteliğindeki online aramaya terörle mücadele davalarında başvurulmadığı belirtilmektedir[930]. Bununla birlikte, online aramanın adli tedbir olarak düzenlenmesi ve 2017 de yürürlüğe girmesiyle birlikte Federal Kriminal Dairesinin *("Bundeskriminalamt")* bu tedbiri hiç gerçekleştirmediği, önleyici tedbir olarak ise çok az sayıda uyguladığı kamuya sızmıştır[931].

2020 itibariyle açıklanmış istatiksel rakamları içeren raporlar bakımından;

2019 raporu, online arama için 22 ilk arama emri ve 11 uzatma emri verildiğini ve yalnızca 12 çevrimiçi aramanın fiilen gerçekleştirildiğini göstermektedir. Bu davalarda isnad edilen suçlar barışa ihanet, vatana ihanet, demokratik hukuk devletini tehlikeye düşürme ve Devletin dış güvenliğini tehlikeye düşürme, suç ve terör örgütü kurma, cinsel özgürlüğe karşı işlenen suçlar, Kişi hürriyetine karşı işlenen suçlar, nitelikli yağma ve ölümle neticelenen yağma, yağma amaçlı şantaj şantajın nitelikli şekli, karapara aklama suçunun çok ağır hali, Uyuşturucu Maddeler Kanunu ile bağlantılı ciddi narkotik suçlar ve Savaş Silahlarının Kontrolü Hakkında Kanunundan bir suç ile ilgilidir[932].

2020 raporu ise online arama için 12 ilk arama emri ve 11 uzatma emri verildiğini ve yalnızca 8 çevrimiçi aramanın fiilen gerçekleştirildiğini belirtmektedir. 2020 yılında verilen online arama kararı emirleri ise çoğunlukla suç ve terör örgütü kurma, çocuk pornografisi içeren yazıları yayma, edinme ve bulundurma suçu, çete

[930]https://www.tagesschau.de/investigativ/staatstrojaner-103.html, Erişim tarihi: 01.06.2024: 23.03.2024

[931] MüKOStPO/Rüückert StPO §100b Rn.3; Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen (netzpolitik.org), Erişim tarihi: 01.06.2024. 23.03.2024.

[932] BfJ - Justizstatistiken (bundesjustizamt.de), Übersicht Online-Durchsuchung 2019 , Erişim tarihi: 01.06.2024:

halinde işlenen hırsızlık suçu ve çete halinde işlenen ağır hırsızlık suçu, Nitelikli yağma ve ölümle neticelenen yağma, yağma amaçlı şantaj şantajın nitelikli şekli ile Uyuşturucu Maddeler Kanunu ile bağlantılı ciddi narkotik suçlar ile ilgilidir[933].

2021 raporu gereği ise 15 ilk arama ve 5 uzatma emri verilmiş olup, yalnızca 9 online arama fiilen gerçekleştirilmiştir. 2021 yılında söz konusu suçlar barışa ihanet, vatana ihanet, demokratik hukuk devletini tehlikeye düşürme ve Devletin dış güvenliğini tehlikeye düşürme, suç ve terör örgütü kurma, öldürme ve nitelikli öldürme, kişi hürriyetine karşı işlenen suçlar, göçmen kaçakçılığı ile Uyuşturucu Maddeler Kanunu ile bağlantılı ciddi narkotik suçlar ile ilgilidir[934].

Bu istatistiklerden görüldüğü üzere, adli tedbir olarak düzenlenmiş olan online arama 2019, 2020 ve 2021 yıllarında fiilen yalnızca toplam 29 kez gerçekleştirilmiştir. Online aramaya uygulamada kısıtlı bir şekilde başvurulma nedenleri olarak ciddi yasal engeller, casus yazılımın izlenecek olan bilgi teknoloji sistemine yüklenmesi gibi tedbirin teknik zorlukları ve yüksek kaynak harcamaları ifade edilmektedir[935].

[933] BfJ - Justizstatistiken (bundesjustizamt.de), Übersicht Online-Durchsuchung 2020, Erişim tarihi: 01.06.2024:
[934] BfJ - Justizstatistiken (bundesjustizamt.de), Übersicht Online-Durchsuchung 2021, Erişim tarihi: 01.06.2024.
[935] Graf, §100b Rn.2; MüKOStPO/Rüückert StPO §100b Rn.3.

ÜÇÜNCÜ BÖLÜM
TÜRK HUKUK SİSTEMİNDE ONLİNE ARAMA- HUKUKİ ÇERÇEVE, UYGULANABİLİRLİK İLE ÖNERİLER

I. Hukuki Çerçeve

A. Genel Olarak Türkiye'deki Hukuki Çerçeve

Online arama, devlet yetkilileri tarafından veri elde etmek amacıyla üçüncü tarafların bilgi teknolojisi sistemlerine yaptıkları gizli bir müdahaledir. Bugünkü tanımıyla bilgisayar, telefon, v. b. birçok sistemi kapsayan[936] bilgi teknolojisi sitemlerine gizli erişim, tedbirden önce kaydedilmiş olan bilgiler de dahil olmak üzere, sistemde depolanan tüm bilgilerin aktarılması için yazılım aracılığıyla sisteme sızılmasını gerektirir[937].

Bu tür gizli erişim yoluyla, bilgi teknolojisi sisteminin verileri İnternet bağlantısı üzerinden iletilebilir ve kullanıcıları hakkında kapsamlı davranış ve kişilik profilleri oluşturulabilir. Dolayısıyla, online arama tedbiri temel hak ve özgürlüklere ciddi bir ihlal teşkil etmekte olup, bu bağlamda genel kişilik hakkının yansıması olan "bilgilerin kaderini belirleme hakkı" ile "bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü sağlama hakkına yönelik[938] müdahale gerçekleşmektedir.

[936] Bilgi teknolojisi sistemleri için Bkz. Birinci Bölüm IV A 1.
[937] BGH Bschluss v. 31.01.2007 – StB 18/06, MMR 2007; S. 237; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, S. 545.
[938] BVerfG 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833 ff; Grossmann, GA 2018, 433; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, S. 545.

Anayasa'nın 13. maddesi gereği, "temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceğinden", yetkilendirme için yasal dayanak gereklidir. Bu nedenle Türk Hukuk Sisteminde gerek önleyici kolluk gerekse istihbarata yönelik düzenlemelerde ve Ceza Muhakemesi Kanunu'nda online arama için yasal dayanağın bulunup bulunmadığının incelenmesi gerekmektedir.

Bu çerçevede sırasıyla 2559 Sayılı Polis Vazife ve Salahiyet Kanunu (PVSK), 2803 Sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunu, 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile Ceza Muhakemesi Kanunu'nu gözden geçirilerek, Alman Hukukunda gerek önleyici gerekse adli amaçlı düzenleme altına alınmış olan online arama bakımından Türk Hukukunda bir yetkilendirme sebebinin bulunup bulunmadığı tespit edilecektir.

B. Önleme Amaçlı Düzenlemelerinde Online Arama Görünümü

Dijital çağda bilginin önemi göz ardı edilemeyecek kadar büyüktür. Günümüzde bilginin elde edilmesi, depolanması ve ihtiyaç halinde kullanılması, mevcut çok çeşitli bilgi teknolojisi sistemleri sayesinde oldukça kolaydır. Bu durum, bilgi teknolojisi sistemlerinin kullanıcıları gibi gerçek kişilerin yanı sıra tüzel kişiler ve devletlere de fayda sağlamaktadır.

Bilginin erişilebilirliği bazı avantajlar sunsa da çeşitli riskleri de barındırmaktadır. Bu bağlamda, kişisel verilerin korunması gibi bireyin özel hayatının çekirdek alanını etkileyen verilerin korunması ihtiyacı ortaya çıkmıştır.

Ulusal güvenliğin, kamu düzeninin ve güvenliğinin sağlanması ile suçla mücadele, devlet kurumlarının temel hedefleridir. Bu hedeflere ulaşmak için, farklı bilgi türlerinin toplanması, depolanması ve gerektiğinde kullanılması yapılan işin doğası gereği gerekli ve vazgeçilmezdir[939]. Suçların ve bununla birlikte tehlikenin önlenmesi amacıyla çeşitli veriler de elde edilmektedir. Bu çerçevede yetkili idari otoriteler suçların önlenmesine yönelik stratejilerini geliştirmek ve önleyici faaliyetlerini planlamak üzere veri toplar, kaydeder ve gerektiğinde kullanır.

Strateji belirleme konusunda ihtiyaç duyulan veriler istihbarat kuruluşları tarafından sağlanmaktadır. İdari kolluğun görevi ise belirli suçların işlenmesini

[939] Küzeci, Kişisel Verilerin Korunması, s. 444.

önlemek amacıyla birtakım faaliyetler gerçekleştirmek ve bu doğrultuda veri elde etmektir.

Özellikle organize suçla mücadele bakımından, devletler günümüzde organize suçlulukla mücadele onların karmaşık ve gizli yapısını deşifre edebilmek için yeni yöntemler uygulamak zorunda kalmaktadır[940]. Bu kapsamda gizli yöntemler aracılığıyla veri elde edilmeye çalışılarak suçların önüne geçilmesi amaçlanmaktadır. İfade edilmelidir ki, önleyici faaliyet sırasında veri elde edilmesi, yöntemlerin çoğunlukla istihbarat kavramı adı altında değerlendirilmesine yol açmaktadır. Ancak istihbarat faaliyetleri münferit suçların önlenmesine değil, ulusal güvenliğin sağlanması amacıyla, demokratik hukuk devletine yönelik tehdit unsurlarına karşı çeşitli stratejilerin belirlenmesine hizmet eder[941]. Bir görüşe göre istihbarat, *"esasları Anayasa'da gösterilen devlet düzenini veya kişilerin güvenliğini tehdit eden faaliyetlerin yerine getirilmesinden önce, hukuka uygun olmak koşulu ile, çeşitli teknik ve yöntemlerle bilgi toplama faaliyeti"* olarak tanımlanırken[942], diğer bir görüş ise*, "elde edilen kişisel veya her türlü bilginin kullanılarak, devlete veya topluma yönelik önemli tehlikelerin sezilmeye çalışılması, bunlardan anlamlandırılan sonuçlar çıkarılması"* olarak ifade etmektedir[943]. Bu bağlamda istihbarat, devletlerin varlığına, anayasal düzenine, toprak bütünlüğüne, güvenliğine ve bağımsızlığına tehdit oluşturabilecek unsurları engellemek için önemli bir rol oynamakta olup, devletlerin özellikle ulusal güvenlik konularında başvurdukları vazgeçilmez bir araçtır[944].
Çalışmamızın ilk bölümünde açıkladığımız üzere[945], kamu düzeni ve güvenliğine zarar veren unsurların önlenmesi ve tehlike yaratan unsurların ortadan kaldırılması için kullanılan yöntemler "önleyici tedbirler" çerçevesinde değerlendirilebilir. Ancak zamanla dünyada yaşanan değişim, ortaya çıkan suç tipleri ve organize suçlar gibi nedenlerle devletlerin suç politikalarında yaşanan değişimlere paralel olarak, tehlikenin bertaraf edilmesinden, tehlikenin önlenmesine doğru bir yönelim söz konusu olmuştur[946].

Bununla birlikte bazı önleyici amaçlı tedbirler ile istihbari faaliyetlerin iç içe geçtiğini ve önleyici tedbirlerin istihbarı faaliyeti de kapsadığı belirtilmelidir. Bu

[940] Özbek, Gizli Görevli, s.61, 62.
[941] Taştan, s. 95.
[942] Geleri/İleri, s.33.
[943] Yenisey, Kolluk Hukuku, s.373.
[944] Taştan, s. 95.
[945] Bkz. Birinci Bölüm V A 1.
[946] Yenisey, Kolluk Hukuku, s.346.

durum özellikle örgütlü suçlar bakımından kullanılan "suçla önleyici mücadele" kavramı kapsamında ortaya çıkmaktadır[947]. Bunun bir örneği, 5397 sayılı Kanunla polise devredilen suçların önlenmesine yönelik istihbarat yetkileridir. 5397 sayılı kanunun genel gerekçesinde "*ülkemizde önleyici amaçlı istihbarat dinlemesi düzenlenmediğinden, hazırlanan Teklif ile, bu önemli eksiklik giderilecekti*r,"; *"devlete yönelik tehlikelerin yakın bir tehdit haline gelmeden, yani doğmadan bertaraf edilmesi için, bilgi toplama, değerlendirme ve iletişime müdahale yanında takibe alma, gözleme ve tarassut gibi başka yetkilere de ihtiyaç vardır"* geçmektedir[948]. Burada yöntem aracılığıyla belli suçların oluşmasıyla mücadele edilmesi söz konusudur. Ayrıca ilgili yöntemlerin uygulanması bakımından, "EGM İstihbarat Dairesi Başkanı", "İstihbarat Komisyonu" gibi mercilerin yetkili olması ve bunun yanında MİT K. m.6/11'de kullanılan "önleyici istihbarat" terimi de bu görüşün yansıması olarak gösterilebilir[949]. Bunun ötesinde PVSK, JTK ve MİT Kanununa eklenen önleyici amaçlı istihbari yetki için öğretide "önleme dinlemesi" ile "istihbari dinleme" kavramlarının kullanıldığını görmekteyiz[950]. Öğretideki farklı bir görüş ise, önlemenin bir amaç istihbaratın ise daha ziyade belirli bir disiplin dahilinde ve veri analizine yönelik bilimsel yöntemler aracılığıyla gerçekleştirilen bilgiyi toplama, değerlendirme, analiz etme ve kullanım alanına ulaştırma sürecini kapsayan bir yöntem olması sebebiyle "istihbarat amaçlı dinleme" kavramının tercih edilmesinin daha uygun olduğunu ifade etmektedir[951].

Sonuç olarak hem kolluk hem de istihbarat birimlerine önleyici ve istihbari amaçlı veri elde etme imkanı verildiği anlaşılmaktadır. Önleyici kolluk faaliyetleri ile istihbari faaliyetler kapsamında elde edilen verilerin, ceza muhakemesinde kullanılabilirliği ise ayrı bir çalışmanın konusunu oluşturacak kadar kapsamlıdır. Bu sebeple, öğretide önleyici veya istihbari faaliyetler kapsamında elde edilen verilerin, ceza muhakemesinde delil olarak kullanılamayacağı yönündeki görüşe[952] katıldığımızı belirtmekle yetiniyoruz.

---

[947] Erdem, s.307.
[948] https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss962m.htm, Erişim tarihi: 01.06.2024.
[949] Eroğlu, s.90-91, 99.
[950] Ataman, s.62; Taştan, s.108; Dağ, s.143.
[951] Ersan Şen, s.68.
[952] Özbek, s. 149. Alman Ceza Muhakemesi Kanunu m. 100e/6-3'te tehlikenin önlenmesi amacıyla elde edilmiş verilerin ceza muhakemesinde değerlendirilmesi konusunda açık düzenleme bulunmaktadır. Buna ilişkin açıklamalarımız için bkz. İkinci Bölüm C 7a (4).

1. 2559 Sayılı Polis Vazife ve Salahiyet Kanununda Polisin PVSK Ek Madde 7 Kapsamındaki Yetkileri

Konumuz bakımından önemli olan ve polise istihbarat yetkisi veren PVSK ek madde 7 1985 yılında PVSK' ya eklenmiştir.

a. Polisin Genel İstihbarat Yetkisi (Ek Madde 7/1)

PVSK ek m. 7 uyarınca, *"Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde ve sanal ortamda*[953] *istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla iş birliği yapar."*

Bu düzenleme ile polise doğrudan istihbarat yetkisinin verildiğini, ülke seviyesinde ve sanal ortamda istihbari yöntemlerle bilgi toplayarak, elde ettiği bilgileri değerlendirme, yetkili mercilere veya diğer kullanım alanlarına ulaştırma görevi tanındığı vurgulanabilir.

Bu noktada önemle ifade edilmelidir ki, polis bu yetkisini ancak PVSK ek m. 7 'de belirtilen amaçlarla kullanabilir. Bu amaçlar, *Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamaktır.* Sonuç olarak, polisin bu amaçların dışında istihbari yetkisini kullanması mümkün değildir.

Bu hüküm ile polise, suç öncesi alan olarak tanımlayabileceğimiz ön alan soruşturması yapma yetkisi verildiği, ancak bunun hukuk devleti ilkesine uygun olmadığı ifade edilmektedir[954]. Bunun sebebi olarak, maddede polisin istihbarat faaliyeti sırasında ne tür tedbirleri uygulayacağının ve bunların koşullarının belirtilmemiş olmaması ile polisin maddedeki istihbarat yetkisini kullanması için bir suçun işlenmesi tehlikesinin ya da işlenmiş olmasının da şart koşulmaması gösterilmektedir. Bunların kabul edilemeyeceği, özellikle polisin bilgi toplama yetkisinin doğması bakımından "belli olayların" ortaya çıkmış olması ve bu olaylara dayanan şüphenin belli kişiler üzerinde yoğunlaşmasının aranması gerektiği

[953] Söz konusu hükme "ve sanal ortamda" ibaresi, 02.01.2017 tarih ve 680 sayılı KHK'nin 28. maddesi ile eklenmiştir.(R.G. no: 29940 mükerrer, 06.01.2017) (09/11/2016 tarih ve 6757 s.k. m.21 ile aynen kabul, R.G. no: 29898, 24.11.2016).

[954] Özbek, Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları, s.78.

vurgulanmaktadır. Ayrıca polise bu şekilde istihbarat yetkisi vermenin bir süre sonra polisi "istihbarat yapan gizli polise" dönüştürmesi riski bulunduğu belirtilmektedir[955].

Burada üzerinde durulması gereken husus, maddede sayılmış olan yetkilerin online arama tedbiri ile örtüşüp örtüşmediğidir. İfade edildiği üzere, online arama tedbiri, tedbire maruz kalan kişinin bilgi teknolojisi sistemine gizlice erişimi ve sistemdeki bütün verilerin ele geçirilmek suretiyle soruşturma makamlarına aktarılmasını kapsamaktadır. PVSK m. 7/1' de belirtilmiş olan *"sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır"* ibaresi açık kaynak istihbaratı olarak nitelendirilmekte olup, bu istihbari yöntem internet ve sosyal medya üzerinden elde edilen verileri kapsamaktadır. Bu şekilde elde edilen verilerin işlenmesi yoluyla bilgilerin kişisel veri haline getirilerek işlenmesi ve değerlendirilmesinden yola çıkarak[956], Alman hukuk sisteminde düzenlenen çevrimiçi arama tedbiri ile örtüşmediği sonucuna varabiliriz.

b. Telekomünikasyon Yoluyla Yapılan İletişimin ve İnternet Veri Trafiğinin Denetlenmesine İlişkin Yetkileri (Ek Madde 7/2-5)

PVSK ek m. 7' ye eklenen fıkralar ile polise telekomünikasyon yoluyla yapılan iletişimin önleme amacıyla tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması yetkisi verilmiştir. 1 Şubat 2018 tarihinde, 2017 yılında KHK ile yapılan değişiklikle, "internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen verilerin denetimi" de hükme eklenmiştir.

Bu çerçevede getirilmiş düzenlemeler şu şekildedir:

" (2) Birinci fıkrada belirtilen görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar ile bilişim suçlarının işlenmesinin önlenmesi amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanının veya bilişim suçlarıyla sınırlı olmak üzere bilişim suçları ile ilgili daire başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen

[955] Özbek, Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları, s.78.
[956] Aydın, AİHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması, s. 222.

veriler tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç kırk sekiz saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.[957][958]

(3) Yetkili ve görevli hâkim, Ankara ağır ceza mahkemesi üyesidir.

(4) Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları, ilgili internet bağlantı adresi veya bağlantıyı tespite imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir[959]*.*

(5) Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir. Durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir."

Önleme dinlemesi olarak adlandırabileceğimiz PVSK ek madde 7/2-5 uyarınca, bir suç kataloğuna atıfta bulunulduğunu ifade edebiliriz. Söz konusu suçlar şu şekilde özetlenebilir:

---

[957] (1) 27/3/2015 tarihli ve 6638 sayılı Kanunun 5 inci maddesiyle, bu fıkranın üçüncü cümlesinde yer alan "yirmidört saat" ibaresi "kırk sekiz saat" şeklinde değiştirilmiştir.

[958] 2/1/2017 tarihli ve 680 sayılı KHK'nin 28 inci maddesiyle, bu fıkrada yer alan "yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün veya İstihbarat Dairesi Başkanının" ibaresi "yazılı suçlar ile bilişim suçlarının işlenmesinin önlenmesi amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanının veya bilişim suçlarıyla sınırlı olmak üzere bilişim suçları ile ilgili daire başkanının" şeklinde değiştirilmiş, aynı fıkraya "telekomünikasyon yoluyla yapılan iletişim" ibaresinden sonra gelmek üzere "veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler" ibaresi eklenmiş, daha sonra bu hüküm 1/2/2018 tarihli ve 7072 sayılı Kanunun 27 nci maddesiyle aynen kabul edilerek kanunlaşmıştır.

[959] 2/1/2017 tarihli ve 680 sayılı KHK'nin 28 inci maddesiyle, bu fıkrada yer alan "veya iletişim bağlantısını" ibaresi ", ilgili internet bağlantı adresi veya bağlantıyı" şeklinde değiştirilmiş, daha sonra bu hüküm 1/2/2018 tarihli ve 7072 sayılı Kanunun 27 nci maddesiyle aynen kabul edilerek kanunlaşmıştır.

1. Bilişim suçları (TCK m. 243-245),
2. Örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu (TCK m. 188/5),
3. Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar,
4. Casusluk suçları hariç İkinci Kitap Dördüncü Kısmın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçların (305, 318, 319, 323, 324, 325 ve 332. maddeler hariç)[960].

İletişimin dinlenmesinin yalnızca hükümde sayılmış olan belirli suçların önlenmesi bakımından düzenleme altına alındığının yerinde olduğu kanaatindeyiz. Zira özel hayatın ve haberleşmenin gizliğine ağır bir müdahale teşkil eden bir tedbirin yalnızca belirli suçların önlenmesi bakımından mümkün olması gerekir.

Uygulanacak tedbir bakımından 3 farklı tedbirin düzenlenmiş olduğunu ifade edebiliriz. Bunlar;

- Telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi ve kayda alınması,
- İnternet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen verilerin tespit edilmesini,
- Sinyal bilgilerin değerlendirilmesi.

"Telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi ve kayda alınması ve sinyal bilgilerinin değerlendirilmesi" tedbirleri bakımından 2005 tarihli Yönetmelikte[961] bir düzenleme yapılmışken, "internet kaynakları arasındaki veri trafiği ile iletilen verilerin tespit edilmesi" tedbiri bakımından herhangi bir tanımın bulunmadığını belirtebiliriz.

Bu çerçevede;

iletişimin tespiti, İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri (Yönetmelik m.3/i),

[960] Özbek, Polis Hukuku, s. 98.
[961] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında 10.11.2005 tarihli ve RG 25989 sayılı Yönetmelik.

iletişimin dinlenmesi ve kayda alınması, telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri (Yönetmelik m.3/h),
Sinyal bilgisi, bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi kapsamaktadır (Yönetmelik m. 3/p).

Sinyal bilgilerinin değerlendirilmesi ise, iletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzerine gerçekleştirilen değerlendirme işlemler şeklinde tanımlanmıştı[962]. Örneğin sinyal bilgilerinin değerlendirilmesi ile ilgilinin yerinin tespiti amacıyla cep telefonunun hangi baz istasyonunda sinyal verdiği tespit edilebilir[963].

Çalışmamız bakımından önem teşkil eden tedbirin *"internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen verilerin tespit edilmesi"* olduğundan, çalışmanın devamında bunun üzerinde durulacaktır. Bu tedbir bakımından doğrudan bir tanım yapılmadığından, tedbir yürürlükteki kanunlardan yararlanmak suretiyle açıklanmaktadır[964]. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkına Kanun'nda düzenlenmiş olan tanımlar gereği, "*trafik bilgisi"*, taraflara ilişkin IP adresi, port bilgisi, verilen hizmetlerin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri olarak tanımlanmıştır (m. 2/1-j). "*Verinin"* ise, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer olarak tanımlandığını belirtebiliriz (m. 2/1-k).

Bunun neticesinde, veri trafiği tespitinin, taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerinin tespiti olduğu ifade edilmektedir[965]. Verinin de bilgisayar üzerinden işlem yapılabilen her türlü değeri kapsadığı dikkate alındığı takdirde, bilgi teknolojisi sistemlerinde metin veya sesli mesajların, anlık mesajlaşma

[962] Bkz; Danıştay 10. Dairesinin 09.03.2017 tarihli ve Esas No: 2012/1001; Karar No: 2017/1361 sayılı kararı ile Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin iptaline karar verilmiştir.
[963] Özbek, Polis Hukuku, s. 101.
[964] Özbek, Polis Hukuku, s. 101.
[965] Yetim, Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği), Seçkin Yayıncılık, Ankara, 2016, s.59.

uygulamalarından kaynaklanan verilerim, e-postaların, sosyal medya uygulamalarından elde edilen tüm verilerin tamamının bu tedbir tarafından kapsandığı kabul edilmekte olup[966], örneğin WhatsApp veya benzeri yazılı ve sesli mesajlaşma uygulamaları üzerinden yapılan konuşmaların kimler arasında ve ne kadar süreyle gerçekleştiğinin ve konuşmaların içeriğinin ne olduğunun tespitine de izin verildiği belirtilmektedir[967]. Ancak bu yetkinin içeriğinin kanun koyucu tarafından açıkça tanımlanmamış olması eleştirilmekte ve kanunilik ilkesi açısından sakıncalı görülmektedir. İnternet üzerinden yapılan her türlü iletişime önleyici müdahalelerin önünü açan ve bu bağlamda internet kullanıcılarının kimlik ve diğer bilgi ve verilerini doğrudan polisin takdir yetkisi kapsamında doğrulama ve aramaya tabi tutan bu hüküm Anayasa'ya aykırı olarak değerlendirilmektedir[968].

Burada iletişimin tespitinin çok ötesinde ve daha geniş kapsamlı bir tedbirin uygulamaya konulduğu öğretide haklı şekilde dile getirilmiştir[969]. Ancak online aramadan farklı olarak söz konusu verilerin internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiğiyle iletilmiş olması koşulu arandığı göz ardı edilmemelidir. Bir başka ifadeyle, bilgi teknolojisi sisteminde telekomünikasyon yoluyla yapılan iletişime veya internet trafiğine konu edilmemiş veriler (örneğin cep telefonuyla çekilmiş fakat hiçbir şekilde paylaşılmamış bir fotoğraf, doğrudan bilgisayarda hazırlanmış bir Word dosyasında yer alan uyuşturucu ağı listesi veya sesli notlar vb.), mevcut düzenlemenin kapsamı dışında kalmaktadır. Online arama tedbiri ise bu verileri de kapsayacak biçimde en geniş şekilde verilerin elde edilmesini içerir. Bu gerekçelerle yürürlükteki PVSK Ek m.7/2'nin online aramanın tam bir karşılığı olmadığı, tedbirin kapsamına giren faaliyetlerin yalnızca bir kısmının bu madde kapsamında düzenlenmiş olduğu kabul edilebilir.

Ayrıca Devlet Denetleme Kurulu'nun 2010 yılında yayınladığı rapora da kısaca değinmekte fayda var, zira bu raporda önleyici amaçlı iletişimin denetlenmesi bakımından önemli sorunlara değinilmiştir[970]. Bu çerçevede, önleyici amaçla iletişimin denetlenmesinde adli yöntemdeki gibi ikincillik ilkesinin ve son çare prensibinin bulunmaması, tedbirin uygulanması için objektif kişi belirlemesi

[966] Candide Şentürk Akaner, Bir Koruma Tedbiri Olarak Online Arama Ve Türk Hukukunda Uygulanabilirliği, 1. Baskı, 2022, Seçkin, s. 141.
[967] Özbek, Polis Hukuku, s. 102.
[968] Özbek, Polis Hukuku, s. 102, 103.
[969] Şentürk Akaner, s. 141.
[970] Kızılırmak, s. 118.

yapılmadığından toplumun bir kesiminin veya tamamının mahkeme kararıyla önleme amacıyla iletişiminin tespit edilmesinin önünde bir engel olmaması, önleme dinlemesinin uygulanması için herhangi bir şüphe seviyesinin veya yoğunluğunun aranmaması ve terör örgütü faaliyeti çerçevesinde yöntemin uygulanma süresinin uzatılmasında keyfiliği önleyici bir güvencenin getirilmiş olmaması eleştirilmektedir[971].

Gerçekten de *"suçların işlenmesinin önlenmesi amacıyla"* ifadesiyle suç işleme kuşkusu altında bulunmayan kişilerin dahi iletişiminin denetlenebilmesinin yolunun açıldığına yönelik eleştirilerin yerinde olduğunu düşünmekteyiz[972]. Bu bağlamda denetimin uygulanması bakımından en azından makul sebeplerin veya genel yaşam tecrübesine uygun olarak, olaylara dayalı somut tehlikenin aranması gerekir[973].

c. Teknik Araçlarla İzleme ve Diğer Kamu Kurum ve Kuruluşlarından Veri İsteme Yetkisi (Ek Madde 7/6)

Polise istihbarat faaliyetleri kapsamında teknik araçlarla izleme ve kamu kurum ve kuruluşlarından veri isteme yetkisi tanıyan PVSK ek 7. maddenin 6. fıkrasına göre, *"istihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir."*

Öncelikle ifade edilmelidir ki, teknik araçlarla izleme hem adli hem önleyici amaçla uygulanabilen bir tedbirdir[974]. Teknik araç, insanın görme ve işitme duyusunun algılama yeteneğinin sınırlarını aşmaya yardım eden her türlü teknik ekipman olarak tanımlanır[975].

---

[971] "Bilgi Teknolojileri ve İletişim Kurumunun 2006 - 2007 ve 2008 Yılları Faaliyet ve İşlemleri" Hakkında Hazırlanan 17/02/2010 tarih ve 2010/4 sayılı Denetleme Raporu; bilgi için bkz.: Kaymaz, İletişimin Denetlenmesi, s.527-528.
[972] Kızılırmak, s. 118.
[973] Altıparmak, s.63; Centel, s. 184; Taşkın, s. 498.
[974] Kızılırmak, s. 122.
[975] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 580.

Bu kapsamda kişinin kamuya açık yerlerdeki faaliyetleri, iş yeri ve özel olarak kullanılan otomobil teknik araçlarla gizli şekilde izlenebilir[976]. Ses kaydının alınması için mini mikrofonların, dinleyicilerin vb. araçların kullanılması mümkünken, görüntü kayıtları bakımından video kameraları, fotoğraf makineleri, gece görüşü sağlayan kızıl ötesi araçlar tercih edilebilmektedir. Teknolojinin gelişmesiyle birlikte, günümüz teknik araçların geliştiği ve bazılarının ses veya görüntü kaydetme işlevine sahipken, bazılarının sadece "iletim" işlevine sahip olduğu belirtilmektedir[977].

Bu tür teknik araçların konutun izlenmesinde kullanılması söz konusu olamaz. Bu bağlamda "kamuya açık yerlerin" izlenmesine olanak tanınırken, konutun bunun dışındaki yerleri kapsadığı kabul edilir. Dolayısıyla konutun dışından da içinden de teknik araçlara izlenmesi madde kapsamında değildir[978].

"Teknik araçlarla izleme" tedbiri ile "online arama" tedbiri arasındaki benzerliklerden biri, her iki tedbirin de gizli tedbirler olması ve her ikisinin de "teknik araçların" kullanımını içermesidir. Yukarıdaki tanım bağlamında, teknik araçların işlevlerinden birinin iletim olması sebebiyle, online arama bakımından bilgi teknolojisi sistemine nüfuz etmek için gereken arama yazılımını kapsayabileceği ifade edilebilir. Ancak bu hususların dışında iki tedbirin arasında başka benzerlik bulunmadığı, bunun ötesinde online arama tedbirin daha geniş kapsamlı olduğu ve çok daha müdahaleci nitelikte olduğu vurgulanmalıdır. Teknik araçlarla izleme tedbirinin konuta yönelik gerçekleştirilememesi söz konusuyken, hakkında online arama tedbiri uygulanan kişinin bilgi teknolojisi sistemine gizlice erişilerek sistemde depolanmış tüm verilere ulaşmak mümkündür. Sonuç olarak, PVSK ek madde 7/6 online arama için yetkilendirme temeli olarak kabul edilemez.

2. 2803 Sayılı Jandarma Teşkilat Görev ve Yetkileri Kanununda Jandarmanın Yetkileri

a. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesine İlişkin Yetkileri (JTK Ek Madde 5/1)

5397 sayılı kanun ile jandarmaya da telekomünikasyon iletişimini izleme yetkisi verilmiştir.

---

[976] Gökçen, Balcı, Alşahin, Çakır, Ceza Muhakemesi Hukuku, s. 544.
[977] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 580.
[978] Öztürk/Tezcan/Erdem, Ceza Muhakemesi Hukuku, s. 580; Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 629.

JTK ek m.5 gereği, *"Jandarma, bu Kanunun 7 nci maddesinin (a) bendine ilişkin görevleri yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, [mülga]250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya istihbarat başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir, kayda alabilir. (...) Bu işlemler, 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7'nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır."*

Söz konusu hükümde Jandarma'nın JTK' nın 7. maddesinin (a) bendine ilişkin görevlerine atıfta bulunulduğundan, ilgili hükmün de burada belirtilmesi gerekir. JTK m. 7'de jandarmanın mülki, adli ve askeri görevleri sayılmış olup, hükümde belirtilen 7. maddenin (a) bendinde sayılan görevleri, jandarmanın mülki görevlerini kapsamaktadır.

Buna göre, *"Jandarmanın sorumluluk alanlarında genel olarak görevleri şunlardır: a) Mülki görevleri; Emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak, ceza infaz kurumları ve tutuk evlerinin dış korunmalarını yapmak, (b) ve (c) bentlerinde [adli ve askeri görevler] belirtilen görevler dışında kalan ve diğer kanun ve nizam hükümlerinin icrası ile bunlara dayalı emir ve kararlarla Jandarmaya verilen görevleri yapmaktır".*

Bu düzenlemenin sonucunda, jandarma aynı polis gibi mülki görevleri kapsamında ve sadece belirtilen suçların önlenmesi bakımından yetkisini kullanabilir. Ancak ilk bakışta jandarmanın söz konusu yetkisinin polisin yetkisinin olduğu gibi doğrudan bir istihbari faaliyete yönelik olmadığı düşünülebilir[979]. Zira PVSK ek m. 7'deki benzer düzenlemede polisin faaliyetinin istihbari nitelik taşıdığı açıkça belirtilmişken, JTK ek m. 5'te buna yönelik herhangi bir ifade kullanılmamıştır. Ancak JTK Ek m. 5/7'de "Jandarma Genel Komutanlığı İstihbarat Başkanlığı" geçmektedir. Ayrıca Ek m.5/8' de ise, TBMM Güvenlik ve İstihbarat Komisyonu'na rapor

[979] Kızılırmak, s. 125 vd.

sunulacağı düzenlenmiştir. Bunun ötesinde, 5397 sayılı kanunun 2. madde gerekçesinde hem jandarmanın istihbarat faaliyetinde bulunma yetkisinin düzenlenmiş olduğu ifade edilmektedir, hem Jandarma Genel Komutanlığı İstihbarat Başkanlığı'nın neden yetkilendirildiği açıklanmaktadır: *"Yapılacak telefon dinlemelerine, bunların işaret, sinyal ve yer bilgilerine ulaşılmasına hâkim karar verecektir. Ancak bu tür işlemler özel bir eğitim, disiplin gerektirdiğinden bu faaliyetler bu konuda görevlendirilmiş ve uzmanlaşmış Jandarma Genel Komutanlığı İstihbarat Başkanlığı görevlilerince yerine getirilecektir. Tüm jandarma birimlerinin bu konuda görevlendirilmesinin sakıncaları göz önünde tutularak görevlendirilecek birimler sınırlı tutulmuştur."*[980]

Önemle ifade edilmelidir ki, Jandarma ek m.5'te belirtildiği şekilde iletişimin denetlenmesi yetkisini yalnızca kendi sorumluluk alanında kullanabilecektir.
PVSK ek m. 7'den farklı olarak, burada tedbir olarak yalnızca telekomünikasyon yoluyla yapılan iletişimin tespit edilmesi, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ile kayda alınmasının düzenlenmiş olduğunu görmekteyiz. Bu surette gerçekleşebilen iletişimin denetlenmesinin online arama için gereklilikleri karşılayıp karşılamaması incelenmelidir.

Çalışmamızın ilk bölümünde online arama ile telekomünikasyon yoluyla yapılan iletişimin denetlenmesi bakımından, her iki tedbirin gizli gerçekleştirilen birer tedbir olduklarını, ancak iletişimin denetlenmesinin kapsadığı verilerin online aramanın aksine daha sınırlı ve devam eden iletişim sürecine yönelik olduğunu belirtmiştik.

Online arama ile kullanıcının bilgisi dışında sisteme sızdırılan yazılım ile internet bağlantısı kurulması halinde soruşturma makamlarına iletilen verilerin telekomünikasyon olarak kabul edilebileceği düşünülebilir[981]. Bu durumda hakkında tedbir uygulanan kişinin sadece interneti kullanmasından kaynaklı telekomünikasyon sürecini başlattığı varsayılabileceği, bunun ilgili kişinin iradesiyle gerçekleşmesinin gerekli olmadığı, yalnızca bu kişi tarafından sisteminin bilinçli olarak işletilmesinin veya çalışır durumda tutulmasının sağlanması gerektiği ifade edilmektedir[982].

Öte yandan, ele geçirilen verinin artık iletim akışının bir parçası olmayıp halihazırda bilgi teknolojisi sisteminde depolanmış olmasının, yazılım nedeniyle veri

[980] Dönem: 22 (tbmm.gov.tr), Erişim tarihi: 01.06.2024.
[981] Bayraktar, D.E.Ü. Hukuk Fakültesi Dergisi, s. 442; Hofmann, NStZ, 2005, S. 123 f.
[982] Hofmann, NStZ, 2005, S. 123 f.

iletiminin JTK anlamında telekomünikasyon olmadığı anlamına gelebileceği savunulmaktadır[983]. Zira telekomünikasyon, *"her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması anlamına gelmektedir"*[984]. Fikrimizce de bu yerinde bir düşüncedir, nitekim bilgi teknolojisi sisteminde önceden depolanmış verilerin halihazırda telekomünikasyonun bir bileşeni olarak değerlendirilmesi, kanun koyucunun amacı dışında olacaktır.

Ayrıca online arama tedbirinde, şüpheli ile üçüncü bir taraf arasındaki herhangi bir telekomünikasyonun izlenmediğinin belirtilmesi gerekir. Nitekim burada üçüncü bir taraf olarak devlet, izlenecek iletişim sürecine katılmaz[985], ancak bağlantıyı kendisi kurar ve telekomünikasyon hattı üzerinden halihazırda depolanmış iletişim verileri olsun veya olmasın, bunları soruşturma yetkililerine aktarmak üzere bunlara erişim sağlar[986].

Sonuç olarak, JTK m. 5/1 online arama için yetkilendirme temeli olarak kabul edilemez.

b. Teknik Araçlarla İzleme ve Diğer Kamu Kurum ve Kuruluşlarından Veri İsteme Yetkisi (JTK Ek Madde 5/5)

Jandarmaya önleyici amaçla teknik araçlarla izleme ve diğer kamu kurum ve kuruluşlarından bilgi isteme yetkisi tanıyan JTK ek m.5/5 gereği, *"Bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir".*

JTK m. 5/5 hükmü de online arama için yasal dayanak olamayacaktır. Gerekçemiz PVSK ek m. 7/6 kapsamında yaptığımız açıklamalarla örtüşmektedir[987].

---

[983] Kaymaz, s. 47 vd.; Bayraktar, D.E.Ü. Hukuk Fakültesi Dergisi, s. 443.
[984] 10.11.2005 tarihli ve 25989 sayılı RG' de yayımlanan Yönetmeliğin 3/1 maddesi.
[985] Kaymaz, s. 53.
[986] Bayraktar, D.E.Ü. Hukuk Fakültesi Dergisi, s. 443, 444; Hofmann, NStZ, 2005, S. 123 f.
[987] Bkz. Üçüncü Bölüm I B 1

3. 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda (MİT K.) Milli İstihbarat Teşkilatının (MİT) Yetkileri

Milli İstihbarat Teşkilatı'na konumuz bağlamında sadece önleyici amaçlarla veya istihbarat yöntemleri kullanılarak elde edilen verilerin online arama tedbiri kapsamına girip girmediği sorusuna cevap vermek amacıyla sınırlı ölçüde değinilecektir.

Kısaca MİT'in görevlerine değinmek gerekirse, MİT K 4/1-a maddesi uyarınca, Milli İstihbarat Teşkilatı, Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasa düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler bakımından milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmakla görevli olduğunu ifade edebiliriz[988].

Bunun dışında MİT K m. 4 gereği, MİT'in örneğin milli güvenlik siyasetiyle ilgili planları hazırlama, kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için tekliflerde bulunma, her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplama, kaydetme, analiz etme gibi çeşitli görevlerinin düzenlenmiş olduğuna dikkat çekebiliriz.

a. MİT Kanunu Madde 6/1 Kapsamındaki Yetkiler

MİT'e, kendisine verilen görevleri yerine getirmesi için belirli yetkiler verilmiş olup, bunlar MİT K m. 6 da düzenlenmiştir. Bu yetkiler şu şekildedir:

"Madde 6 – (Değişik birinci fıkra: 17/4/2014-6532/3 md.)[989] Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

a) Yerli ve yabancı her türlü kurum ve kuruluş, tüm örgüt veya oluşumlar ve kişilerle doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.

b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi,

[988] Yenisey/Nuhoğlu, Ceza Muhakemesi Hukuku, s. 292.

[989] Maddede yer alan (c) ve devamındaki yetkiler kanuna 17.04.2014 tarih ve 6532 sayılı kanun ile eklenmiştir. (R.G. no: 28983, 26.04.2014).

belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

c) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318, 319, 324, 325 ve 332 nci maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilir, bunlardan örnek alabilir.

d) Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir.

e) İstihbari faaliyetler için görevlendirilenlerin kimliklerini değiştirebilir, kimliğin gizlenmesi için her türlü önlemi alabilir, tüzel kişilikler kurabilir. Kimliğin oluşturulması veya tüzel kişiliğin kurulması ve devam ettirilmesi için zorunlu olması durumunda gerekli belge, kayıt ve dokümanlar ile araç ve gereçler hazırlayabilir, değiştirebilir ve kullanabilir.

f) Yabancıların ülkeye giriş ve çıkış ile vize, ikamet, çalışma izni ve sınır dışı edilmesi gibi konularda, ilgili kurum ve kuruluşlardan talepte bulunabilir.

g) Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir.

h) Yabancı unsurların ülkenin ve vatandaşların iletişim güvenliğini tehdit eden faaliyetlerinin engellenmesine yönelik çalışmalar yapabilir, ilgili kurum ve kuruluşlardan talepte bulunabilir.

i) MİT'te görev alan veya alacak kişilerin güvenilirliklerini ve uygunluklarını belirlemek için yalan makinası uygulaması dâhil test teknik ve yöntemlerini kullanabilir.

j) MİT mensupları görevlerini yerine getirirken ceza ve infaz kurumlarındaki tutuklu ve hükümlülerle önceden bilgi vermek suretiyle görüşebilir, görüşmeler yaptırabilir, görevinin gereği terör örgütleri dâhil olmak üzere millî güvenliği tehdit eden bütün yapılarla irtibat kurabilir."

Çalışma konumuz olan online arama "*Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplama yetkisini düzenleyen"* MİT K m. 6/1-g'nin kapsamına girebileceği izlenimi verse de yukarıda da belirttiğimiz gibi, online arama ile telekomünikasyon kanalları dışında da elde edilen veriler kapsanmaktadır.

b. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesine İlişkin Yetkileri (MİT K. Madde 6/2)

Yukarıda da incelediğimiz gibi, polis ile jandarma için geçerli olan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi yetkisi MİT'e de verilmiştir. MİT K. M.6/2 gereği,

"Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, MİT tarafından kurulan merkez veya 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. (Değişik son cümle: 4/5/2007-5651/12 md.) 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesinin altıncı fıkrasının (a) bendinin (14) numaralı alt bendi kapsamında yapılacak dinlemeler de bu merkezler üzerinden yapılır."

PVSK ve JTK' deki düzenlemelere benzer şekilde MİT K.' de MİT' e telekomünikasyon yoluyla yapılan iletişimin denetleme yetkisinin tanındığını görmekteyiz. MİT' e tanınan yetkilerin arasında ayrıca casusluk faaliyetlerinin ortaya çıkarılması ile devlet sırrının ifşasının tespiti de sayılmıştır[990].

Bu noktada belirtmelidir ki, PVSK gereği polise tanınmış olan yetkilerden farklı olarak MİT'e *"internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen verileri"* denetleme yetkisi tanınmamıştır. Buna karşın MİT

[990] Kızılırmak, s. 131.

Kanunu'nda yer alan ve yukarıda belirtilen bazı görev ve yetkilerin bu faaliyetin yürütülmesine olanak sağladığı varsayılabilir. MİT K. m.4/1-i' deki *"her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek"* hükmü ile, m. 6/1-g' deki *"Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir"* hükmünün internet üzerinde denetim yetkisi verdiği söylenebilse de, internet ağının PVSK'de olduğu gibi düzenlenmesi bu konuda belirlilik ilkesi anlamında açıklık yaratacağı ifade edilmektedir[991].

Bunun ötesinde, PVSK ve JTK ile bağlantılı olarak daha önce açıkladığımız gibi, MİT Kanunu'nun 6/2 maddesi, telekomünikasyon yoluyla iletişimin denetlenmesi yalnızca sınırlı verileri kapsadığından ve devam eden iletişim sürecine yönelik olduğundan, online arama için bir yetki teşkil edemez.

C. Adli Amaçlı Düzenlemelerinde Online Araman Görünümü

1. CMK m. 135 İletişimin tespiti, dinlenmesi ve kayda alınması

CMK m. 134 uyarınca, telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi ile mobil telefonun yerinin tespiti düzenlenmiştir.

Her ne kadar online arama tedbirinin gizlilik ve teknik araçlarla bilgi edinme açısından telekomünikasyon yoluyla iletişimin denetlenmesine benzeyeceği düşünülebilse de, çalışmamızın ilk bölümünde online aramanın alternatif koruma tedbirleri ile mukayesesinde ve üçüncü bölümünde PVSK, JTK ve MİTK uyarınca önleyici amaçlı telekomünikasyon yoluyla iletişimin denetlenmesinde online arama ile halihazırda devam eden telekomünikasyon yoluyla yapılan iletişime müdahale söz konusu olmadığından, bu tedbir ile örtüşmediği tespit edilmiştir. Burada tekrardan kaçınmak için kendimizi CMK m. 135'in online arama için bir yetki temeli teşkil edemeyeceğini belirtmekle sınırlayacağız.

[991] Kızılırmak, s. 132.

2. CMK m. 134 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

Online arama tedbirinin, bilişim sistemlerinde halihazırda var olan ve depolanan verilerin elde edilmesi nedeniyle Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri ile benzerlik gösterdiği düşünülebilse de her iki tedbir arasında temel farklılıklar olduğunu ifade edebiliriz.

İlk olarak, online arama tedbirinin bilişim sistemlerindeki geleneksel aramalara kıyasla doğası gereği gizli olduğu vurgulanmalıdır. Ceza Muhakemesi Kanunu'nun 134. maddesi uyarınca, bu tedbir, şüphelinin hazır bulunması ve soruşturma görevlilerinin aranacak bilgi sistemlerinin bulunduğu yerde fiziksel olarak bulunması ile karakterize edilir[992]. Bununla birlikte gerçekleştirilen arama işlemlerinin tutanağa geçirilmesi ve tedbirin muhatabı tarafından imzalanması gerekmektedir. Tutanak tutma ve imzalama koşulları hukuki güvence bakımından önemlidir, zira ancak bu surette hakkında tedbir uygulanan kişilerin hukuk güvenliği tesis edilebilir[993]. Ancak, online arama tedbiri söz konusu olduğunda, tedbirin gizliliği nedeniyle tedbirin uygulandığı kişinin tedbir hakkında bilgisi olmadığından ve tedbir tutanağının imzalanması mümkün olmadığından, bu koşullar yerine getirilememektedir.

Tedbirler arasındaki bir diğer önemli fark ise kendini tedbirlerin uygulandığı süre bakımından göstermektedir. Online arama tedbiri, bilgi teknolojisi sistemlerinin uzun bir süre boyunca izlenmesini mümkün kılmaktadır. Bu, sisteme teknik araçlarla sızıldıktan sonra, sistemin kararın izin verdiği ölçüde uzun bir süre boyunca izlenebileceği anlamına gelir. CMK m. 134 uyarınca bu mümkün değildir. CMK m. 134/2 gereği, bilişim sistemlerine şifrenin çözülememesinden dolayı girilememesi halinde, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için söz konusu araç ve gereçlere elkonulması halinde dahi, elkonulan cihazlar gecikme olmaksızın iade edilir. Zira CMK m. 134/2' nin istisna olarak anlaşılması gerektiği, kuralın ise bilişim sistemlerinin bulunduğu yerde anında arama yapılarak, bu sistemlerin kayıtlarından kopya çıkarılması ve bu kayıtların çözülerek metin haline getirilmesi

[992] Bayraktar, s. 449.
[993] Bayraktar, s. 446.

gerektiği vurgulanmaktadır[994]. Sonuç olarak burada uzun süreli bir izlemeden ziyade tek seferlik ve belirli bir süreyi kapsayan bir tedbir söz konusudur[995].

Sonuç itibariyle, online arama tedbirinin CMK m. 134 ile uyumlu olmadığını, online aramanın CMK m. 134 hükmüne dayanarak uygulanmasının hukuka aykırı olarak değerlendirilebileceği kanaatindeyiz.

Bunun ötesinde, eğer bilgi teknolojisi sistemi el koymadan önce şifrelenmişse, bu durumda şifrelemeyi çözmek mümkün olmayabileceğinden, dijital delil elde etmek için cihazlarda geleneksel bir arama yapılmasının uygun olmayacağı unutulmamalıdır.

II. Türk Hukukunda Uygulanabilirlik

Çalışmamızın bu bölümüne kadar yaptığımız inceleme, online arama tedbirinin Türk hukuk sisteminde düzenlenmediğini göstermektedir. Tedbirin Türk hukukunda uygulanabilirliğine ilişkin olarak öncelikle Avrupa Konseyi Siber Suçlar Sözleşmesi ışığında bir değerlendirme yapılacaktır. Akabinde, elde edilen delilin niteliği gösterilmek suretiyle içtihat kararları temelinde online arama tedbirinin Türk hukuk sistemindeki gerekliliği değerlendirilecektir.

A. Avrupa Konseyi Siber Suç Sözleşmesi Işığında Değerlendirme

Bilişim teknolojileri alanındaki hızlı gelişim ve internetin sunduğu kolaylıklar, hayatın her alanının bilişim sistemleri ile donatılmasına yol açmıştır. Bunun sonucunda siber suçlar olarak adlandırılan yeni suç tipleri ortaya çıkmıştır. Dahası, geleneksel suçların delilleri dahi bilişim sistemlerinde bulunabilmektedir[996].

Dijital delillerin yaygın ve uluslararası nitelikte olması ve önemli bireysel ve toplumsal sonuçlar doğurması hem uluslararası düzeyde hem de ulusal sınırlar içinde yeni yaklaşımların ve iş birliğinin ortaya konmasını gerektirmiştir[997].

---

[994] Dülger, Ceza Muhakemesi Hukuku, s. 474.
[995] BT-Drucksache, 18/12785, s. 54.
[996] Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", Fasikül Hukuk Dergisi, Cilt 2, Sayı 9, ss.23, 24.
[997] Yılmaz, Türk Ceza Hukuku Sisteminde Siber Suçlar, Adalet Yayınevi, Ankara, 2016, s.164.

Bu bağlamda Avrupa Konseyi tarafından yürütülen çalışmalar sonucunda Avrupa Konseyi Siber Suç Sözleşmesi Haziran 2001'de hazırlanmış, Avrupa Konseyi Bakanlar Komitesi tarafından 8 Kasım'da onaylanmış ve 23 Kasım 2001 tarihinde Budapeşte'de Taraf Devletlerin imzasına açılmıştır. Sözleşme 1 Temmuz 2004 tarihinde yürürlüğe girdikten sonra, bilişim sistemleri çerçevesinde suçlarla mücadeleye yönelik ilk uluslararası anlaşma olmuştur[998].

Dört bölümden oluşan Sözleşme'nin birinci bölümü tanımları, ikinci bölümü maddi ve usul hukukuna ilişkin ulusal düzeyde alınacak tedbirleri, üçüncü bölümü uluslararası iş birliğini ve dördüncü bölümü ise diğer hükümleri düzenlemektedir[999]. Ayrıca sözleşmeye ek olarak bir memorandum (explanatory report) düzenlenmiş olduğunu, burada sözleşmenin amacı ve gerekçesine yer verilmiş olduğunu görmekteyiz.

Sözleşmenin başlıca amaçları, taraf Devletler arasında hızlı ve etkili bir iş birliği mekanizması geliştirmek, uyumlaştırılmış mevzuat ve ilgili tedbirlerin kabul edilmesini sağlamak ve toplumu sanal ortamda işlenen suçlardan korumaktır[1000].

Sözleşmeye taraf olan ülkelere hem maddi hukuk hem de usul hukuku alanında birtakım yükümlülükler getirilmiş ve bu doğrultuda Üye Devletler bilişim suçlarına ilişkin yasal düzenlemeleri yerine getirmeyi ve muhakeme işlemlerine ilişkin eksikliklerini Sözleşmeye uygun olarak gidermeyi taahhüt etmişlerdir[1001].

Türkiye Avrupa Siber Suç Sözleşmesini 10.11.2010 tarihinde imzalamış, 22.04.2014 tarih ve 6533 sayılı *"Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun"* ile onaylanmış ve sözleşme 01.01.2015 tarihinde yürürlüğe girmiştir[1002]. Avrupa Siber Suç Sözleşmesi, siber suçlarla etkin mücadele ve Türkiye'nin bu alandaki güvenilirliği açısından son derece önemli değerlendirilmektedir[1003].

Konumuz bakımından önem teşkil eden maddeler Sözleşmenin 14 ila 21. Maddeleridir, zira bunlar ceza muhakemesinin önemli bir unsuru olan arama ve

---

[998] Murat R. Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği." Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. 19/2 (Prof. Dr. Nur Centel'e Armağan), 2013, s.1241; Duran, "Ceza Muhakemesi Kanunu'nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK m.134)", Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi, 2019, Cilt: 14, Sayı: 173, ss.173-241.

[999] SEV 185 - Übereinkommen über Computerkriminalität (coe.int),Erişim tarihi: 01.06.2024:
Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayıncılık, 8.Baskı, s.201.

[1000] Dülger, s.200-201; Başlar, Ceza Yargılamasında Elektronik Delil, Ankara 2016, Yetkin s. 115.

[1001] Dülger, Bilişim Suçları, s.201.

[1002] Full list - Treaty Office (coe.int), Erişim tarihi: 01.06.2024:

[1003] Dülger, Bilişim Suçları, s.580.

elkoyma tedbirlerinin elektronik ortamda uygulanmasını ele almaktadır[1004]. Bu çerçevede;

- 16. madde *"kaydedilmiş bilgisayar verilerinin süratli bir biçimde korunmasını",*
- 17. madde *"trafik verilerinin süratli bir biçimde korunması ve kısmen açıklanmasını",*
- 18. madde *"Verilerin teslim edilmesine yönelik emir",*
- 19. Madde *"kaydedilmiş bilgisayar verilerinin aranması ve bunlara el konulmasını",*
- 20. madde *"trafik verilerinin gerçek zamanlı toplanmasını",*
- 21. Madde *"içerik verilerinin gerçek zamanlı toplanmasını"* düzenlemektedir.

Ancak ifade edilmelidir ki, yukarıda sıraladığımız tedbirlerden arasında yer alan 16. Madde ile düzenlenmiş olan "*kaydedilmiş bilgisayar verilerinin süratli bir biçimde korunması"* ile 17. Maddede yer alan *"trafik verilerinin süratli bir biçimde korunması ve kısmen açıklanması"* tedbirlerinin Ceza Muhakemesi Hukukumuzda muadil düzenlemeleri bulunmamaktadır[1005].

Bilişim sistemlerinde arama ve elkoyma ile ilgili olarak, CMK m. 134 hükmünün Sözleşmenin 19. Maddesinde öngörülen *"kaydedilmiş bilgisayar verilerinin aranması ve bunlara el konulması"* tedbirini iç hukukumuza aktardığı belirtilmektedir. Ancak CMK m. 134'ün Sözleşme ile uyumlu olmadığı, CMK m. 134' deki tedbirin kapsamının Sözleşmenin 19. Maddesinden farklı olarak daha dar olduğu, Sözleşme hükmünün elektronik ortamdaki delillerin geleneksel delillerden farklı ve has has olduğunu belirttiği, söz konusu delillerin elde edilme şekli ve muhafaza yöntemlerine ilişkin CMK da yer almayan özellikler gibi bazı eksiklikler içerdiği belirtilmektedir[1006].

Sonuç olarak, Türkiye'nin Siber Suç Sözleşmesi'ni imzalamış olması, Konsey üyesi ülkelerin çoğunun online arama tedbirine mevzuatlarında açıkça yer vermesi ve

[1004] Keskin, Serap, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi." İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt:59, Sayı: 1- 2, 2001, s.156.; Başlar, s.97

[1005] Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri" 2015, s.85, GSI_Articletter_2015_Summer_Article6.pdf (goksusafiisik.av.tr), Erişim tarihi: 01.06.2024.

[1006] Duran, s. 177; Baştürk, s. 29.

günümüzde bilgi teknoloji sistemleri ile bağlantılı olarak işlenen suçlar ve bunlarla mücadelede etkin bir rol alabileceği nedeniyle bu tedbirin Türk hukukunda da düzenlenmesi gerektiği kanaatindeyiz[1007].

B. Dijital Delil Perspektifinden Yargı Kararları Işığında Değerlendirme

1. Dijital Delil

Dijitalleşme ile yeni iletişim seçenekleri ve teknolojileri, bir bütün olarak toplumun gelişimi üzerinde önemli bir etkiye sahiptir. İletişimdeki şifreleme teknolojileri neticesinde, geleneksel telekomünikasyon denetimi yoluyla değerlendirilebilir bulguların elde edilmesi zorlaşmıştır.

Bu çerçevede uzaktan erişim yoluyla delil elde etmenin bir aracı olarak online arama tedbirinin önemi ortaya çıkmaktadır[1008]. Bilgi teknolojisi sistemlerinin suç amaçlı olarak geliştirilmesi ve kötüye kullanılması, soruşturma yetkilerinin genişletilmesi için bir gerekçe olarak kabul edilmektedir. Bu surette online aramanın, cezai soruşturma ve kovuşturma düzeyindeki güvenlik zorluklarının ve boşluklarının üstesinden gelmeye yönelik bir tedbir olduğunu ifade edebiliriz.[1009]

Hayatın neredeyse her alanında kullanımı giderek artan bilişim sistemleri sadece suça değil, delillere de yeni bir boyut kazandırmıştır. Bilişim sistemleri suçu aydınlatmak ve suçlulara ulaşmak bakımından önemli bir araç haline gelmiştir. Bunun sonucunda, online arama tedbirinde olduğu gibi, bir elektronik araç olan bilgi teknolojisi sistemleri aracılığıyla elde edilen dijital deliller (e-delil) [1010] ceza muhakemesinde önemli bir rol almaya başlamıştır.

Öğretide dijital delilin farklı tanımları vardır. Bir görüşe göre dijital delil, *"elektronik ortamda bulunan ve bir suçun oluşumuyla ilgili olarak bir iddianın gerçekleştiğine veya aksini ispatına veya suçun kastına veya saiki gibi önemli elementlerle dair bilgi veren ve dijital ortamlarda depolanan veya gönderilen veridir"*[1011]. Diğer bir tanıma göre dijital delil, elektronik bir araç nezdinde saklanan

[1007] Şentürk Akaner, s. 175.
[1008] Köker, Nilüfer, Çeviri: Prof. Dr. Prof. h.c. Arndt Sinn, "Kaynak Telekomünikasyon Denetimi ve Online Arama Yoluyla Yeni Gizli Soruşturma Tedbirleri", Fasikül Aylık Hukuk Dergisi, Haziran 2019, s. 115.
[1009] Öztürk/Tezcan/Erdem, Dijital CMK, s. 545.
[1010] Değirmenci, Olgun, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin, 2014, s. 31 vd.; Öztürk/Tezcan/Erdem, Dijital CMK, s. 443.
[1011] Tanrıkulu, s. 47.

ya da bu araçlar aracılığıyla dolaşımı sağlanan ve muhakeme bakımından önem teşkil eden bilgi ve veriler şeklinde ifade edilmiştir[1012].

Dijital delilin tanımlanmasında veri kelimesine atıfta bulunulduğundan, dijital delilin net bir şekilde açıklanabilmesi için veri kelimesine de değinmek gerekir. Bilişim sistemleri aracılığıyla işleme tabi tutulabilen, bu işlemler çerçevesinde birtakım sonuçlar elde edilebilen, depolanabilen ve başka bilişim sistemlerine aktarılabilen her türlü bilgi, veridir[1013]. Diğer bir görüş ise veriyi bilgisayar aracılığıyla herhangi bir işlem veya açıklama bakımından harf, kod, rakam ya da sayı gibi unsurları ortaya çıkarmak üzere yararlanılan genel bir tabir olarak açıklamıştır[1014].

Bilişim sistemlerinde delil aramanın amacı bu verileri elde etmek ve maddi vakıalara ilişkin verileri dijital delil olarak hükme dahil etmektir. Bu noktada, tüm verilerin dijital delil olarak kabul edilmeyeceği vurgulanmalıdır. Dijital verilerin yargılama ile ilgili olan kısımları belirli koşulları yerine getirmeleri halinde dijital delil olarak kabul edilebilir[1015].

Dijital delilin maddi gerçeğe ilişkin olması gerekliliğinin yanı sıra, gerçeğin ortaya çıkarılmasına elverişli olması da gerekmektedir. Ayrıca dijital deliller hukuka uygun olarak elde edilmeli, bütünlüğü bozulmamış, zarar görmemiş ve güvenilir olmalıdır. Dahası, dijital deliller mantıksal ve bilimsel kurallara uygun olmalı ve gerçekliği konusunda şüpheye yol açmamalıdır[1016].

Belirtmek gerekir ki, dijital delillerin bulunabileceği kaynaklar somut niteliğe sahip olabilse de yargılama açısından önem teşkil eden bu kaynakların içerisindeki soyut verilerdir[1017]. Dijital delillerin söz konusu soyut niteliği, delillerin araştırılması ve muhafazası bakımından bazı önemli zorlukları da beraberinde getirmektedir. Günümüzde bilişim aygıtları (veri taşıyıcıları) çok yüksek boyutlardaki verileri depolayabilir hale gelmiştir. Bunun sonucunda dijital delilin tespitinin ilk anda yapılabilmesi her zaman mümkün olmayabilir[1018].

Bir diğer önemli husus ise, bilişim aygıtlarının ve bunların içindeki verilerin değiştirilmeye veya silinmeye müsait hassas yapılar olmalarıdır. Bu nedenle özellikle

[1012] Dülger, Bilişim Suçları, s. 668.
[1013] Dülger, Bilişim Suçları, s.77.
[1014] Gün, Nagihan, "Türk Ceza Hukukunda Bilişim Suçları", Çankaya Üniversitesi, 2020, s.29.
[1015] Dülger, Bilişim Suçları, s. 604; Başlar, s. 67.
[1016] Karagülmez, s. 509; Dülger, Bilişim Suçları, s. 605, 606.
[1017] Dülger, Bilişim Suçları, s. 603.
[1018] Mesut Orta, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması: Adli Bilişim, Ankara, Yetkin Yayınları, 2015.

dijital delillerin elde edilmesi ve muhafazası aşamalarında bunların uzmanlığı bulunan kişiler tarafından yapılması önemlidir[1019]. Aksi takdirde bu hassas ve tahrip edilebilirliği yüksek olan dijital deliller elde edildiği aşamada yapılan hatalar sebebiyle hukuka aykırı delil teşkil edebilir.

Bunun ötesinde dijital delilin kopyalanabilir özelliği bulunmaktadır. Ancak bu özelliği ile dijital delilin manipüle edilmeye de müsait bir yapıya sahip olduğu ifade edilebilir. Bu nedenle dijital delilin yargılamada ileri sürülebilmesi için aslına uygun olduğunun ispatı gereklidir[1020]. Bu bakımdan önemli olan, dijital delilin birebir kopyalanmış olması ("forensic image") ve bu kopyaların hâkim veya mahkeme huzuruna getirilmesine kadar geçen süreçte de aslına uygunluğunu ortadan kaldıracak herhangi bir olumsuz müdahaleye maruz bırakılmamış olmasıdır[1021].

Bu bağlamda, örneğin hafızası tam olarak kullanılmayan bir veri taşıyıcısını kopyalayıp muhafaza ederken, "imajı" ve "HASH değeri" alınarak ve zaman damgası kullanılarak veri "mühürlenmelidir". Bu, kopyalama işleminden sonra kopyalanan veride değişiklik veya ekleme yapılması riskini ortadan kaldırır[1022].

Dijital verilerin delil olarak kullanılabilmesi için öncelikle delillerin genel özelliklerine sahip olması gerekmektedir. Ayrıca kendine has özellikleri nedeniyle adli bilişim uzmanları ve kolluk kuvvetleri tarafından yapılan işlemlerin doğruluğu ve güvenilirliği konusunda olası şüphelerin sürecin başından son anına kadar giderilmesi gerekmektedir[1023]. Bu bağlamda delillerin kaynağı, elde edilme şekli, saklanması, bir yerden başka bir yere taşınması, raporlanması ve sunulması güvenilir olmalıdır[1024]. Aksi takdirde elde edilen veriler suçun ispatında kullanılamaz.

Dijital deliller, beş duyu ile doğrudan algılanamayan gayri maddi verilerden oluşmaktadırlar. Dolayısıyla bu delillerin anlaşılabilmesi için geleneksel delillerden farklı olarak özel teknik yazılım kullanmak suretiyle özel prosedürlere başvurulur[1025]. Bu şekilde deliller raporlanıp algılanabilir hale getirilir ve nihayet ceza muhakemesinde değerlendirmeye alınabilir. Raporlama sürecindeki teknik terimlerin anlaşılabilir ve basit bir dille aktarılması önemlidir. Öngörülen usullere uygun olarak

[1019] Öztürk/Tezcan/Erdem, Dijital Ceza Muhakemesi Hukuku, s. 444; Başlar, s. 89; Orta, s. 240, 241.
[1020] Göksoy, s. 96; Karagülmez, s. 509.
[1021] Karagülmez, s.509.
[1022] Dülger, Ceza Muhakemesi Hukuku, s. 477; Öztürk/Tezcan/Erdem, Dijital CMK, s. 444.
[1023] Doğan Gedik, "Bilişim Suçlarında IP Tespiti ile Ekran Görüntüleri Çıktılarının İspat Değeri", Bilişim Hukuku Dergisi, cilt 1, sayı 1, 2019, s.70.
[1024] Gedik, s. 70.
[1025] Uğraş, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", Türkiye Barolar Birliği Dergisi, 2021 Sayı 154, s. 100, 101.

hazırlanan bilimsel raporun güvenirliğine ilişkin şüphe bulunmadığı takdirde, dijital delillerin de diğer kabul gören deliller gibi delil olma değeri olabilecektir[1026].

2. Yargıtay İçtihadı Işığında Değerlendirme

Türk hukukunda online arama tedbirine ilişkin yasal zemin bulunmaması sebebiyle, mevcut yasal çerçevede bu tedbire en yakın koruma tedbirleri ve bunlara ilişkin uygulama örneklerinin incelenmesinde fayda bulunmaktadır. Yargıtay kararlarına değinmek suretiyle bu konuya açıklık getirilmeye çalışılacaktır.

Yargıtay nezdinde FETÖ/PDY yargılamalarında "*ByLock"* uygulamasının kullanımına ilişkin online arama ile ilgili olabilecek kararlar verdiğini gözlemlemekteyiz.

Bu bağlamda, Yargıtay 16. Ceza Dairesinin, 24.04.2017 tarih 2015/3 Esas ve 2017/3 Karar Sayılı kararında[1027], ByLock uygulamasının kullanılması suretiyle örgüt içi haberleşmeye dayalı olarak ilgili sanıklar aleyhine delil elde etmek amacıyla geçmişte gerçekleşen mesajlaşma ve iletişim içeriklerinin tespiti için CMK m. 134 kapsamında kopyalama ve el koyma işlemlerinin yapılmasının zorunlu olduğu ifade edilmiştir. ByLock'un delil niteliğine ilişkin "…*Elektronik deliller, klasik delillerden farklı olarak soyut bir yapıya sahiptirler. Şüphesiz ki, elektronik delillerin içerisinde yer aldığı somut bir donanım aygıtı bulunmakta ise de ceza yargılaması bakımından esas delil teşkil edenler bu donanım aygıtının kendisi değil, içerisinde yer alan dijital nitelikteki delillerdir"* şeklinde hukuki değerlendirme de bulunan 16. Ceza Dairesi; ByLock iletişim sistemindeki veri tespitlerinin hangi koruma tedbiri kapsamında incelenmesi gerektiği yönündeki ifadeleri bakımından ise, CMK m. 135 açısından, "*İletişimin dinlenmesi ve kayda alınması ise, halen ve gelecekte yapılacak görüşmelerin dinlenme ve kayda alınmasına yönelik işlemleri kapsamaktadır"; "…Telekomünikasyon yoluyla yapılan iletişimin dinlenmesinden, yapılan konuşmaların, iletişimin gerçekleştiği hat, sistem veya ortama girilmek suretiyle canlı olarak işitilmesi anlaşılmalıdır. Telefon dışındaki diğer telekomünikasyon araçlarıyla yapılan denetim ise genelde kaydetme şeklinde gerçekleşmektedir. Örneğin iletim anında faks mesajının ele geçirilmesi kaydetme şeklinde gerçekleşir. İnternet üzerinde*

[1026] Göksoy, Resul, Ceza Muhakemesinde Dijital Delilerin Elde Edilmesi ve Güvenilirliğinin Sağlanması, Ankara, Seçkin Yayıncılık, 2019, s. 177.
[1027] Yargıtay 16. Ceza Dairesinin, 24.04.2017 tarih 2015/3 Esas ve 2017/3 Karar Sayılı Kararı için bkz Yargıtay Ceza Genel Kurulu E. 2017/16-956 (kazanci.com.tr), Erişim tarihi: 01.06.2024.

gönderilen mesaj veya diğer verilerin araya girmek suretiyle ele geçirilmesi ise, bu verilerin birer kopyalarının üretilmesi şeklinde gerçekleşmektedir ki bu da kaydetme kapsamına girer";

"CMK'nın 135 inci maddesinin birinci fıkrasına göre yapılan iletişimin dinlenmesi ve kaydı, geçmişe değil, geleceğe dönük olarak yapılabilir. Diğer bir ifadeyle geçmişte gerçekleşen iletişimin dinlenebilmesi veya kayda alınabilmesi mümkün değildir. Ancak internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından, bu iletişim kayıtları hakkında CMK'nın 134 üncü maddesinin birinci fıkrası gereğince arama, kopyalama ve elkoyma koruma tedbirleri uygulanabilir";

"Ceza yargılamasında delil olarak kullanılabilecek elektronik deliller arasında SMS, MSN Messenger, Gtalk gibi iletişim kayıtlarının yanı sıra, bu nitelikteki gizli, şifreli veya silinmiş dosya ve klasörleri de saymak mümkündür" demek suretiyle bilgi teknolojisi sistemleri üzerinde şüpheli veya sanığın internet ortamında çeşitli programlar veya sosyal iletişim siteleri yada belirli yapılarca kullanılan Bylock gibi uygulamalar vasıtasıyla gerçekleştirdiği iletişime yönelik kayıtların aranmasının, CMK m. 135' den ziyade, CMK m. 134 uyarınca gerçekleştirilebileceğine hükmetmiştir. Özetle 16. Ceza Dairesi, bilgilerin bir bilgisayardan elde edildiğini tespit etmek suretiyle, ByLock programının bulunduğu sunucuya ve içerdiği bilgilere Ceza Muhakemesi Kanunu'nun 134. maddesini uygulamıştır.

Yargıtay Ceza Genel Kurulu 26.09.2017 tarih 2017/16-956 Esas ve 2017/370 Karar Sayılı kararda[1028] da yine FETÖ/PDY yargılamasına ilişkin ByLock uygulamalarının hangi koruma tedbiri kapsamında incelenmesi gerektiği yönündeki ifadeleri bakımından, incelemenin CMK m. 134 uyarınca yapılabileceğini belirtmiştir. Ceza Genel Kurul ayrıca *"Avrupa Konseyi Siber Suç Sözleşmesi, 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";*

"Avrupa Konseyi Siber Suç Sözleşmesi bilgisayar sistemlerinin birbirlerine bağlanabilme özelliklerinden dolayı verilerin, doğrudan aramanın yapıldığı bilgisayarda değil, bilgisayarın doğrudan ya da internet gibi iletişim sistemleri üzerinden dolaylı şekilde bağlantılı olduğu başka bir sistemde bulunabileceğini, bu

[1028] Yargıtay Ceza Genel Kurulu 26.09.2017 tarih 2017/16-956 Esas ve 2017/370 Karar Sayılı karar için bkz Yargıtay Ceza genel Kurulu E. 2017/16-956 (kazanci.com.tr), Erişim tarihi: 01.06.2024.

durumda aramanın verilerin gerçekte bulunduğu yeri içine alacak biçimde genişletilebileceğini ya da verilerin bulundukları yerden getirilebileceğini kabul etmektedir";

"Elektronik delillerin bulunabileceği kaynaklar arasında, uzak veri saklama yerleri ve İnternet Servis Sağlayıcıları (ISS) bulunmaktadır. Bir diğer kaynak ise farklı yerlerde hatta ülkelerde yer alan bilişim sistemleri olabilmekte, verinin bir bölümü ele geçtiğinde tek başına anlam ifade etmemesine rağmen diğer parçaları da ele geçirildikten sonra veriler bir arada fikir bütünlüğü oluşturabilmektedir" ,

" Bilgisayar kütüklerinin sadece hard disk şeklinde anlaşılmaması gerekir. Bilgisayar kütükleri, internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP no'larını ve diğer erişim bilgilerini depoladıkları veri tabanlarını da ifade etmekte, bir bilgisayar aracılığıyla ağ üzerinden ulaşılabilen ortak paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçlarını da kapsamaktadır";

"Şüpheli veya sanığın internet ortamında çeşitli programlar ya da sosyal iletişim siteleri (Msn Messenger, Facebook, Twitter vb.) vasıtasıyla gerçekleştirdiği iletişime ilişkin kayıtların aranması, CMK'nın 135 inci maddesinin birinci fıkrasına göre değil, aynı Kanunun 134'üncü maddesinin birinci fıkrasına göre yapılabilir. Zira CMK'nın 135 inci maddesinin birinci fıkrasında düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbiri, teknik araçlarla iletişimin dinlenmesini ve kayda alınmasını kapsamaktadır" diyerek ByLock uygulamalı telefonlarda bulunan geçmişte gerçekleştirilmiş görüşmelerin ve kayıtların CMK m. 134 uyarınca "arama, kopyalama ve elkoyma" tedbirleri ile elde edilebileceğine karar vermiştir.

Ancak bu noktada, Ceza Muhakemesi Kanunu'nun 134. Maddesi uyarınca, söz konusu telefonların şifresinin veya ByLock uygulamasının şifresinin çözülmesi ve böylece iletişimin içeriğine erişimin sağlanması halinde başarıya ulaşılabileceği vurgulanmalıdır. ByLock uygulamasının şifresinin çözülememesi halinde haberleşme içeriklerine erişilemeyeceğinden, ByLock uygulamasının cep telefonuna yüklenmesinin Yargıtay'ın yerleşik içtihatları anlamında FETÖ/PYD örgütüne üyelik için yeterli sayılamayacaktır[1029].

[1029]Yargıtay 16. Ceza Dairesi, 24.04.2017 tarih 2015/3 Esas ve 2017/3 Karar Sayılı karar; Yargıtay 16. Ceza Dairesi, 20.06.2018 tarih ve 2018/1028 Esas, 2018/1959 Karar Sayılı kararı.

Bu bağlamda, gizli erişime izin vererek şifreleme sorununun üstesinden gelebildiği ve cep telefonuna fiziksel olarak el konulmasını gerektirmediği için online aramanın önemi ortaya çıkmaktadır.

Bu noktada ifade edilmelidir ki, Federal Almanya Anayasa Mahkemesi, online arama teknik yönteminin uluslararası terörizmle mücadeleye karşı savunmaya uygun olduğuna ve prensip olarak Anayasa'daki temel haklarla uyumlu olduğuna karar vermiştir[1030]. Nitekim bilgi teknolojisi sistemlerinin suç amaçları için geliştirilmesi ve kötüye kullanımı, soruşturma yetkilerinin genişletilmesi açısından temel sebep olarak gösterilmektedir[1031]. Dijitalleşme ile artık suç tipleri de değişmekte ve bilişim sistemleri ile internet üzerinden çeşitli hukuka aykırı eylemler "online" olarak gerçekleşmektedir.

Bu bağlamda karanlık ağ olarak bilinen "darknet" konusu da önem teşkil etmektedir. Darknet, internetin ikinci, gizli bölümü olarak adlandırılan Deep Web'in ("derin ağ") karanlık yüzü olarak nitelendirilen bir şifreli ağdır[1032]. Darknete erişim sağlamak için, darknet 'in çalıştığı Tor, 12P ve FreeNet gibi özel olarak tasarlanmış tarayıcılara ihtiyaç duyulur. Bu nedenle Internet Explorer, Chrome veya Yahoo gibi bilinen sıradan tarayıcılarla erişim sağlanması mümkün değildir[1033]. Herkese açık internette iletişim izlenebilirken, Tor tarayıcısı gibi uygulamalar darknet üzerine anonim kalmayı sağlar[1034].

Darknet 'in amacı, kullanıcılarının tespit edilme endişesi yaşamadan anonim kalarak istedikleri konuda veri alışverişinde bulunabilmeleri. Ancak bunun sonucunda darknet ile uyuşturucu, insan ve silah kaçakçılığı, kiralık katillik ve çocuk pornografisi gibi yasa dışı faaliyetlere zemin oluşturulmakta, darknet üzerindeki faaliyetlerin neredeyse 60%'ının suç olarak kabul edilebileceği belirtilmektedir[1035]. Karanlık ağda, anonimlik ve takip edilemezlik vaadiyle suçlulara ve suç eğilimli insanlara hitap eden bir ortamın yaratıldığı eleştirilmektedir[1036].

[1030] BVerfG NJW 2016, 1781 Rn. 208 ff; KK-StPO/Henrichs/Weingast §100 b; Rn. 4.
[1031] Öztürk/Tezcan/Erdem, Dijitial CMK s. 545, 546.
[1032] Momsen/Bruckmann, s. 27.
[1033] Öztürk/Tezcan/Erdem, Dijital CMK, s. 548.
[1034] Sönmez, Göktuğ/Çelik, Emine, Anonimlik ve İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri, Yıl: 22, Cilt:22, Sayı: 1, Haziran 2020, s. 71.
[1035] Momsen/Bruckmann, s. 27.
[1036] Arndt Sinn, Ermittlungen im Darknet/Karanlık Ağ'da Soruşturma, Fasikül Cehamer Aylık Hukuk Dergisi, Yıl 10, Sayı 104, Temmuz 2018, Seçkin, s. 7; Köker, Nilüfer, Çeviri: Karanlık Ağ'da Soruşturma/Ermittlungen im Darknet, Fasikül Cehamer Aylık Hukuk Dergisi, Yıl 10, Sayı 104, Temmuz 2018, Seçkin, s. 17.

Soruşturma makamları darknet kullanan suçluların anonimliğini deşifre etmekte ve yasadışı faaliyetlerini ortaya çıkarmakta zorlanmaktadır[1037]. Bu zorlukların online arama tedbiri ile aşılabileceğine inandığımız için, darknet üzerinden işlenen suçlarla mücadele etmek amacıyla online arama tedbiri için yasal bir zemin oluşturulması gerekmektedir[1038].

Bununla birlikte özellikle organize suç ve uluslararası terörizm ile mücadelede geleneksel arama ve elkoyma tedbirlerinin şifrelenmiş bilişim sistemlerine erişim sağlayamadıkları hallerde, online aramanın etkili bir koruma tedbiri olabileceği kanaatindeyiz. Başka bir ifadeyle, bilişim sistemlerinden kaynaklanan suçlarla mücadelede, özellikle de organize suçlarla ilgili olarak, teknoloji tabanlı ve teknoloji destekli tedbirlerin kullanılması gerektiğini düşünmekteyiz[1039].

Ancak online arama tedbiri temel hak ve özgürlüklere ciddi bir müdahale teşkil ettiğinden, yasallaştırılmasına ilişkin koşulların katı bir şekilde düzenlenmesi zaruridir. Bu, devletin bir "gözetim devleti" haline gelmesini önlemek ve hukukun üstünlüğünden sapmayarak özgürlük ve güvenlik arasındaki dengeyi sağlamak için gereklidir. Ceza yargılamasının temel amacının, maddi gerçeği ortaya çıkarırken, kişisel hak ve özgürlüklere saygı ile toplumsal düzenin korunması arasında bir denge kurmak olduğu unutulmamalıdır.

III. Türk Hukuku Bakımından Öneriler

Çalışmanın bu bölümünde, tarafımızca Türk hukukuna kazandırılması önerilen online arama tedbirinin yasal çerçevesi bakımından öneriler sunulmaya çalışılacaktır. Öncelikle genel olarak düzenleme kaleme alınırken müdahalenin yoğunluğu başta olmak üzere dikkat edilmesi gereken teknik hususlara değinilecek, ardından tedbirin

[1037] Sinn, Ermittlungen im Darknet, s. 10; Köker, Çeviri: Karanlık Ağ'da Soruşturma, s. 19; Öztürk/Tezcan/Erdem, Dijital CMK, s.548.
[1038] Öztürk/Tezcan/Erdem, Dijital CMK, s.549.
[1039] Aynı yönde bkz. Şentürk Akaner, s. 185; Aksi yönde bkz. Erdem, Dilek Özge, Dijital Delillerin Elde Edilme Yöntemi Olarak Alman Ceza Muhakemesinde (Alman CMK §100b) Online (Çevrimiçi) Arama Tedbiri ve Tedbirin Türk Hukukunda Uygulanabilirliği, CHD Ağustos 2023, Sayı: 52, s. 391.

uygulanma esasları konusunda Türk kanun koyucusuna somut önerilerde bulunulmaya çalışılacaktır.

A. Müdahalenin Yoğunluğu Bakımından

Geleneksel arama ve elkoyma tedbirleri ile telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinden farklı olarak, online arama tedbirinin en önemli avantajı şifrelenmiş verilere erişim imkânı sağlamasıdır. Şifreli veriler konusunda geleneksel tedbirlerin yetersizliği sorununu aşmasının yanı sıra, gizlice ve uzunca bir süre uygulanabilir olması tedbire, suçla mücadelede etkin bir rol kazandırmaktadır. Özellikle organize suç örgütleri tarafından günümüzde şifreli mesajların kullanımı neredeyse kural haline geldiğinden, geleneksel delil elde etme yöntemleri kullanılarak örgütlü suçlarla mücadele edebilmek gerçekçi görünmemektedir. Keza dijital çağın sunduğu RAM kapasitesindeki iyileşme ve bulut bilişim sistemleri gibi harici depolama alanlarında depolanan verilere de erişim ancak online arama ile sağlanabilir.

Bununla birlikte online arama, hayatın sır alanı dahil olmak üzere temel hak ve özgürlüklere ağır müdahale teşkil eden bir nitelik taşımaktadır. Zira hakkında tedbir uygulanan kişinin kullanıcısı olduğu bilgi teknolojisi sistemlerinde bulunan tüm verilere erişim imkânı sağlamaktadır. Bir kimsenin, onu diğer insanlardan ayırt edici olan tüm özellikleri ve davranış modelleri de dahil olmak üzere tüm kişiliğini profillemeye yarayacak her türlü verisine erişme imkânı sunan bu tedbir, katı uygulanma koşullarına bağlanmalıdır. Casus yazılım tedbirin yöneltildiği bilgi teknoloji sisteminde yer alan verileri sistemde yalnızca pasif şekilde kalarak incelemelidir. Hakkında tedbir uygulanan sitemdeki herhangi bir fonksiyonun aktifleştirilmesine (örneğin bilgisayarın kamerasına erişip, elektronik cihazın bulunduğu mekânın optik kaydının alınmasına) imkân vermeyecek şekilde yazılım programlanmalıdır.

B. Tedbirin Teknik Özellikleri Bakımından

Devletin kendisi, bilişim teknolojileri sistemlerinin tüm versiyonlarına, bir başka ifadeyle tüm işletim sistemlerine (iOS, Microsoft vd.) uygun yazılım geliştirmelidir. Zira casus yazılımı kendisi geliştirmezse, bunu üçüncü kişilerden temin etmesi gerekecektir. Casus yazılımı üçüncü kişilerden, hele ki karanlık ağda faaliyet gösteren kimselerden temin etmesi halinde, bu durum bilişim güvenliği konusunda

devletin yükümlülükleri ile ciddi çelişki doğuracaktır. Bu tür ortamlardan temin edilecek yazılımların güvenlik açıklarından istifade ederek tersine casusluk riski barındırmasının yanı sıra söz konusu kara borsa faaliyetlerinin güçlenmesine dolaylı yoldan yapacağı katkı da göz önünde bulundurulmalıdır.

Dürüstlük kuralının bir uzantısı olarak devletin güven sorumluluğunu ihlal etmeden başvurulması gereken bir tedbirdir. Devlet, tedbirin uygulanması sırasında adeta "beyaz şapkalı bir hacker" gibi davranmalıdır. Bir başka ifadeyle, sisteme sızarken etik değerlerini kaybetmeden, yalnızca pasif şekilde gözlem yapmak ve delil elde etmek amaçları doğrultusunda hareket etmelidir. Casus yazılım bakımından asgari kalite standartları oluşturulmalıdır. Kötüye kullanım risklerini minimize etmek için belirlenmesi gereken bu asgari standartların bağımsız ve tarafsız bir otorite tarafından denetlenmesi düşünülmelidir. Almanya'da kaynak telekomünikasyon denetimi tedbirinde yaşanan tedbirin amaçları bakımından sınır aşımı örnekleri gibi olumsuz tecrübelerin online arama bakımından tekrarlanmaması adına gerekli hassasiyet gösterilerek müdahalenin teknik sınırlarının yasayla sıkı şekilde belirlenerek temel hak ve özgürlüklerin etkili biçimde korunması sağlanmalıdır.

Gerek yazılımın geliştirilmesinde gerekse geliştirilmiş olan yazılımın bilgi teknoloji sistemlerine sızdırılması bakımından uzmanlaşmış personel yetiştirilmesi gerekmektedir. Zira yalnızca bir yazılım geliştirmek, online arama tedbirinin başarıya ulaşması için tek başına yeterli değildir. Bilgi teknoloji sistemlerine sızma yöntemlerinden, en sonuç odaklı olanı güvenlik açıklarından faydalanmak olduğundan, buna yönelik bir faaliyeti gerçekleştirebilecek kapasitede eleman temin etmek zaruridir.

Bununla birlikte günümüzde tüm işletim sistemleri devlet dışı aktörler tarafından kullanıcılara sunulduğundan, tedbirin uygulanması konusunda yetkili uzman personelin mümkün olan en hızlı şekilde sisteme sızması gerekmektedir. Aksi takdirde, güvenlik açıklarının kapatılmasına yönelik güncellemeler tedbirin sonuçsuz kalmasına yol açabilecektir.

Öte yandan, etik bir başka çelişki de devletin vatandaşlarını bilgi teknoloji sistemlerinde yer alan açıklar konusunda uyarma yükümlülüğüne sahip olmasıdır. Bu etik çelişkinin online arama lehine bozulmasına gerekçe olarak yine devletin suçu ve suçluyu önlemek yönündeki yükümlülüğü gösterilebilir. Esasen devlet, bilgisi dahilindeki sistem açıkları konusunda vatandaşlarını uyarma yükümlülüğünü ihmal etmekle birlikte, daha ağır tehdit altında olan başka temel hak ve özgürlüklerini

koruma vazifesini yerine getirmektedir. Bu durum, tedbirin anayasal güvence altındaki ölçülülük prensibini ihlal etmediği şeklinde yorumlanabilir.

Suçla mücadele amacıyla geliştirilen bir yazılımın suça ve suçluya hizmet edecek hale gelmesi herhalde düşünülebilecek en ağır senaryodur. Bu sebeple, devlet tarafından geliştirilecek yazılımın üçüncü kişiler tarafından ele geçirilmesi ve kötüye kullanılması konusunda maksimum düzeyde güvenlik önlemlerinin alınması da devletin bir yükümlülüğü olarak görülmelidir. Ayrıca online arama tedbiri için kullanılmak üzere geliştirilen casus yazılım ile bilgi teknoloji sistemlerine sızan personelin de yetkisinin sınırlarını aşıp aşmadığı konusunda bir denetim mekanizması oluşturulması gereklidir.

Online arama araçlarının teknik özellikleri ve veri koruma konusundaki gereksinimler nedeniyle, tedbirin oldukça karmaşık olduğu ve her bir uygulamanın somut soruşturma bakımından özel olarak tasarlanması gerekmektedir. Bu durum, çok sayıda uzmanlaşmış personele ihtiyaç doğurmaktadır. Bu gerekçelerle, online arama geleneksel teknik araçlarla izleme tedbirlerine bir alternatif değildir. Bu geleneksel yöntemlerden sonuç alınmaması veya sonuç alınma ihtimalinin açıkça düşük veya imkânsız olması gibi çok istisnai durumlarda online arama tedbirine başvurulması düşünülmelidir.

C. Tedbirin Bağlantılı Olduğu Temel Haklar ve İlkeler Bakımından

Online arama tedbiri, içerisinde bulunduğumuz dijital çağ bakımından her ne kadar gerekli ise de temel hak ve özgürlükler bakımından çeşitli riskleri de beraberinde getirmektedir. Bu soruna çalışmanın ilk bölümünde değinilmiş olmakla birlikte, ilgili temel hak ve özgürlükler bağlamındaki somut önerilere bu başlık altında yer verilecektir.

❖ Her şeyden önce bir hukuk devletinin, ülkesinde yaşayan herkese sağlaması gereken asgari güvenceleri ihlal edecek şekilde online arama tedbirinin uygulanmaması gerektiği açıktır. Bu noktada ifade etmek gerekir ki her ne kadar ceza muhakemesi hukukunda kural olarak kıyas mümkün ise de online arama tedbiri gibi temel hak ve özgürlüklere ciddi bir müdahale teşkil eden bir tedbiri kıyasen uygulamak kabul edilemez. Kanunilik ilkesinin bir gereği olarak, online arama tedbirinin tüm

koşullarıyla birlikte kanunla düzenlenmesi kaçınılmazdır[1040]. Tedbirin uygulanma koşulları, usul ve esasları da tüm detaylarıyla kanunda düzenlenmeli; bunlar yönetmelik gibi idari düzenleyici işlemlerle belirlenmemelidir.

❖ Online aramanın, soruşturmanın amaçları dışında kullanılması, soruşturma makamlarının, hakkında tedbir uygulanan kişinin soruşturmayla ilgisi olmayan ve hayatın sır alanına ait olan bilgilerinin kamuoyu ile paylaşılması şeklinde soruşturma gizliliğini ağır biçimde ihlal edecek bir tutum sergilemeleri, vazgeçilmez olan insan haysiyetinin korunması ilkesi ile bağdaşmaz. Zira Federal Alman Anayasa Mahkemesi tarafından da vurgulandığı gibi günümüzde dijital mahremiyet insan onurunun bir parçasını oluşturur. Online arama tedbirinin, sert çekirdekli olan işkence yasağın ihlal edecek şekilde uygulanması kesinlikle kabul edilemez.

❖ Hakkında online arama tedbiri uygulanan şüpheli veya sanığa adil yargılanma hakkının gerektirdiği asgari güvencelerin mutlaka sağlanması gerekmektedir. Temel hak ve özgürlüklere ağır müdahale oluşturan tedbirin, usulî güvencelerle desteklenmesi gözetilmelidir. Bu bakımdan, tedbire başvurulması mutlaka hâkim kararı (hatta belki ağır ceza mahkemesi tarafından oy birliği ile verilecek bir karar dahi düşünülebilir) veya en azından gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından tedbir kapsamındaki girişimler bakımından mutlaka bir hâkim denetimi öngörülmelidir. Belirli süreler içerisinde hâkim onayından geçmeyen işlemlerin, derhal sona erdirilmesi; o ana kadar elde edilen delillerin gecikmeksizin yok edilmesi gibi güvenceler yasada açıkça düzenlenmelidir.

Kimi hukuk sistemlerinde gizli soruşturmacı tedbiri bakımından, kararın verilmesi sırasında şüphelinin pasif haklarının korunması amacıyla hakkında gizli soruşturma tedbiri uygulanacak kişiyi tanımayan ve kimliğini bilmeyen "güvenilir bir avukat" görevlendirilmektedir[1041]. Türk hukuku bakımından öğretide bu yöndeki öneriler[1042] göz önünde bulundurularak, online arama açısından da benzer bir düzenleme yapılması düşünülebilir.

❖ Ölçülülük ilkesi gözetilmek suretiyle, online arama tedbirine, örneğin yalnızca örgütlü suçlarla mücadele çerçevesinde başvurulması öngörülebilir. Örgütlü

[1040] Şentürk Akaner, s. 175.
[1041] Yenisey/Nuhoğlu, s. 482 – 483.
[1042] Erden Tütüncü, Efser. "Dürfen verdeckte Ermittler im türkischen Strafprozessrecht während der Erhebung von Beweismitteln Ton- und/oder Videoaufzeichnungen machen?", Zeitschrift für Internationale Strafrechtswissenschaft, s. 139.

suçlarla mücadele bakımından mevzuatımızda halihazırda mevcut olan gizli soruşturma yöntemlerinde olduğu gibi online arama tedbiri de sıkı uygulama koşullarına bağlanmalıdır. Hatta bahse konu tedbirlerle kıyaslandığında, online arama temel hak ve özgürlüklere daha ağır bir müdahale teşkil ettiğinden, söz konusu tedbirlere nazaran çok daha ağır koşullara bağlanması gerekmektedir. Ayrıca örgütlü suçlarla mücadele kapsamında başvurulabilen özel tedbirler arasındaki öncelik-sonralık sıralamasında en son başvurulması gereken tedbir olduğunun yasada açıkça belirtilmesi, uygulamada ölçülülük ilkesini ihlal etme riski bulunan pratiklerin de önüne geçecektir. Bu gibi yasal güvencelerin temini sayesinde, ölçülülük ilkesini ihlal etmeden online arama tedbirine başvurulabilir.

❖ Özel ve aile hayatına saygı hakkı kapsamında online arama tedbiri irdelendiğinde, tedbirin niteliği itibariyle hayatın sır alanına müdahaleyi beraberinde getirdiği açıktır. Bu sebeple, online aramanın ancak kuvvetli suç şüphesinin varlığı ve başka surette delil elde imkânı bulunmayan, örgütlü suçlarla mücadelede başvurulan diğer gizli soruşturma tedbirlerinden sonuç alınamayan yahut sonuç alınmasının mümkün olmadığı açık olan çok istisnai hallerde uygulama alanı bulması düşünülmelidir. Öte yandan bu tedbiri uygulama yetkisine sahip olan kolluk personelinin, özel bir teknik ve etik eğitim almış personel olması gerektiği düşüncesindeyiz. Tedbirin uygulandığı somut soruşturmayla ilgisi olmayan özel ve aile hayatının bilhassa sır alanına ait verilerin -hâkim denetiminden geçirilmek suretiyle- derhal imha edilmesi zorunluluğu ile tedbirden elde edilmesi beklenen amaçlara ulaşılması veya ulaşılma imkanının ortadan kalkması durumlarında tedbire derhal son verilmesi zaruriyeti açıkça yasada güvence altına alınmalıdır. Ancak bu düzenlemelerin yasada açıkça yer alması da tek başına yeterli olmayacaktır. Kolluğun bu konuda uzmanlaştırılması zorunludur.

Ayrıca online arama tedbirine başvurulabilecek olan suçlar bir katalog halinde yasada düzenlenmeli, bu kataloğun diğer gizli soruşturma tedbirlerinde yer alan suç kataloglarına nazaran daha dar kapsamlı olması da düşünülmelidir.

❖ Kişisel verilerin korunmasını isteme hakkının ceza muhakemesi bakımından geçerli olmadığı söylenemez. Şöyle ki "istisnalar" başlıklı KVKK m. 28'in 1'inci fıkrasının ç bendinde *"Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen*

önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi" halinde bu kanun hükümlerinin uygulanmayacağına dair düzenleme bulunmaktadır. Ancak bu düzenleme, soruşturma ve kovuşturma makamlarına ölçüsüz bir müdahale yetkisi verildiği şeklinde yorumlanmamalıdır. Zira yukarıda belirtildiği üzere, soruşturma ve kovuşturma makamları hukuk devleti, insan haysiyetinin korunması gibi bir dizi yükümlülük sahibidir. Tüm bunlar bir arada değerlendirildiğinde, ancak ilgili soruşturmanın amaçları doğrultusunda ve ölçülü şekilde online arama tedbirine başvurulması mümkündür. Türk yasa koyucu, ceza muhakemesi makamları arasındaki kişisel veri işleme ve yayma faaliyetleri bakımından bir düzenleme getirmemiş bulunduğundan, uygulamada bu faaliyetler KVKK m. 28'in "fazlasıyla geniş yorumlanması" sonucunda denetimsiz kalmış vaziyettedir. Kanaatimizce bu konuda Alman yasa koyucu örnek alınmak suretiyle, ceza muhakemesi makamlarının kendi aralarındaki kişisel veri paylaşımı konusunda sıkı koşullara bağlanması gerekmektedir.[1043]

D. Tedbirin Hizmet Ettiği Amaç Bakımından

Online arama, kişilerin temel hak ve özgürlüklerine ağır müdahale oluşturan bir tedbir olması sebebiyle uygulama alanının mümkün olduğunca sınırlı bir kapsamda belirlenmesi gerekmektedir. Bu sebeple tedbirin -en azından başlangıçta- yalnızca adli amaçlı olarak kullanılmasına cevaz verilmesi gerektiği düşüncesindeyiz. Önleyici amaçlarla online arama tedbirine başvurulması hususuna ise ihtiyatla yaklaştığımızı ifade etmek isteriz. Nitekim Türk hukukunda mevcut önleyici tedbirler (örn. PvSK Ek m. 7) bağlamında yasal düzenlemedeki belirsizliklerden ve hatalı uygulamalardan kaynaklanan sorunlara bir yenisinin eklenmemesi için online arama tedbirinin önleyici amaçlarla uygulanmasına dair bir yasal düzenleme getirilmek istenirse, bu tedbirin uygulanma koşulları, usul ve esasları hiçbir tereddüde yer vermeyecek şekilde açık yasal zemine kavuşturulmalıdır. Aksi takdirde, demokratik bir hukuk devletinde bireylere sağlanması gereken asgari standartlar tehlikeye düşebilir.

Alman Hukukunda da online arama tedbirinin önleyici amaçlı kullanılmasına yönelik yasal düzenlemeler mevcuttur. Ancak tüm bu düzenlemelerin çok sıkı koşullara bağlı tutulduğunu hatırlatmak isteriz. Ayrıca Federal Almanya Anayasa

[1043] Aynı yönde bkz. Erden Tütüncü, Efser/Taşçı Aydemir, Ece. "Kişisel Verilerin Ceza Muhakemesinde Korunmasına İlişkin Kısa Bir Değerlendirme", Fasikül Aylık Hukuk Dergisi, 2022/4 (Ekim-Kasım-Aralık) (Baskıda), s. 6 vd.

Mahkemesi'nin 27.02.2008 tarihli (Karar No. 1 BvR 370/07) kararında vurgulandığı gibi ancak "ağır basan bir hukuki menfaate yönelik somut bir tehlike olduğuna dair olgusal göstergelerin varlığı" gibi sıkı koşulların mevcudiyeti halinde online arama tedbirine önleyici amaçlı olarak başvurulabilmelidir.

Çalışmanın sınırlılıkları gereğince, önleme amaçlı online aramaya ilişkin açıklamalarımız bu kadarla sınırlı tutulacaktır. Bundan sonraki başlık altında yalnızca adli amaçlı online arama tedbirine dair normatif önerilerimize yer verilecektir.

E. Tedbirin Uygulanma Şartları Bakımından

Düzenleme kaleme alınırken, tedbirin bütün uygulanma şartları titizlikle ele alınmalıdır. Bu çerçevede şekli ve maddi koşullar hiçbir soru işaretine yer bırakmayacak şekilde açıklık ve belirlilik kriterlerine göre düzenlenmelidir.

1. Müdahalenin koşulları

Online arama tedbiri gereği, tedbire maruz kalan kişinin bilgisi dışında da, bu kişi tarafından kullanılan bir bilgi teknolojisi sistemine erişmek ve buradan veri elde etmek amacıyla teknik araçlar kullanılabilir.

Öncelikle online aramanın gizliliğe dayanan bir soruşturma yöntemi olduğunu ifade etmeliyiz. Her ne kadar Alman CMK m. 100b 'de açıkça gizlilik terimi kullanılmamış olsa da, "hakkında tedbir uygulanan kişinin bilgisi olmadan da" ibaresi online aramanın gizli bir tedbir olduğuna işaret etmektedir.

Bununla birlikte, suçun teşebbüs aşamasında kalması veya iştirak halinde işlenmiş olması, tedbirin uygulanması bakımından önem taşımamalıdır.

Alman Hukukunda düzenlenmiş olan online arama tedbirinde özellikle "bilgi teknolojisi sistemleri" kavramı tercih edilmiş olup, böylelikle bu sistemlerin kapsama alanı geniş tutulmuştur. Mevzuatımıza online aramanın getirilmesi durumunda, uygun kavram bakımından bilgi teknolojisi sistemleri ile "bilgisayarlar, bilgisayar programları ve kütükleri" (CMK m. 134) arasında tercih yapılması gerekir.

İki kavram arasındaki tercihimizi belirtmeden önce, kısaca "bilgisayarlar, bilgisayar programları ve kütüklerini" tanımlamak isteriz. Bilgisayar, "belleğine yüklenmiş program uyarınca aritmetik ve mantık işlemleri yapabilen, sonuca göre karar verip programdaki akışı değiştirebilen, çevresiyle etkileşimde bulunabilen, girdi ve sonuç verilerini belleğinde tutabilen aygıt, elektronik beyin olarak" tanımlanır.

Bilgisayar programı ise, 5846 sayılı Fikri ve Sanat Eserleri Kanunu gereği, "bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları" olarak tanımlanmaktadır. Bilgisayar kütükleri ise hard disk olarak açıklanmakta olup, internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP numaralarını ve diğer erişim bilgilerini sakladıkları veri tabanlarını kapsadığı, hatta daha geniş bir yorum ile taşınabilir ya da bulut formatında her türlü veriyi taşıyan ve depolayan sistem olarak anlaşılması gerektiği ifade edilir. Bilişim sistem ve teknolojilerin hızla geliştiğini, gittikçe daha fazla verinin farklı cihaz ve taşıyıcılarda kaydedilip işlendiğini ve bulut bilişim sistemlerine de talebin arttığını dikkate alırsak, bu yorumun isabetli olduğunu ifade edebiliriz.

Bu doğrultuda, içerisinde bilişim teknolojisi barındıran her türlü akıllı elektronik cihaz ve veri taşıyıcısını kapsaması sebebiyle, CMK m. 134 gereği kullanılmış olan "bilgisayarlar, bilgisayar programları ve kütükleri" ifadesinin online arama bağlamında da kullanılabileceğini düşünmekteyiz.

Teknik araç bakımından ise, düzenleme kaleme alınırken, Alman hukukundaki gibi teknik araçlarla online arama tedbiri ifadelerinin kullanılması düşünülebilir. Zira Türk öğreti ve uygulamasında kabul görmüş olan teknik araç terimi göz önünde bulundurulduğunda, online arama kapsamındaki "yazılım"ları da kapsamına aldığı kanaatindeyiz. Bu sebeple, teknik araç kavramının online arama tedbirinde de kullanılmasında bir sakınca bulunmadığı görüşündeyiz. Ayrıca kümülatif olarak aşağıdaki koşullar sağlanmalıdır:

a. Kuvvetli suç şüphesinin bulunması

Alman CMK m. 100b ile nitelikli suç şüphesi aranmaktadır. Ancak nitelikli suç şüphesi hukukumuza yabancı bir kavramdır. Bu nedenle tedbirin müdahaleci niteliği ile uyum sağlayabilecek, Hukukumuzda kabul gören ve uygulamada sorun teşkil etmeyecek bir suç şüphesinin aranmasının uygun olacağı kanaatindeyiz.

Hukukumuzun ciddi müdahaleci tedbirlerde aranan şüphe derecesini göz önünde bulundurduğumuzda, gerek CMK m. 135/1 gerekse CMK m. 140/1 gereği "somut delillere dayanan kuvvetli şüphe"nin arandığını görmekteyiz. Bu tedbirler yoluyla kişilerin özel yaşamlarına, haberleşme özgürlüklerine gibi temel hak ve özgürlüklere keyfi olarak müdahale edilmesi önlenmeye çalışılmaktadır. Alman CMK

m. 100b gereği ifade ettiğimiz gibi, şart koşulan şüphenin kesin olgusal maddi delillerle belirli bir somutlaştırma ve pekiştirme derecesine ulaşması beklenir. Alman hukuk sisteminde kuvvetli şüphe derecesi aranmamasına rağmen, Türk hukuk sisteminde bunun geçerli olamayacağı ve Türk ceza muhakemesi hukukunda tedbirin düzenlenmesi halinde somut delillere dayalı kuvvetli suç şüphesinin aranması gerektiği kanaatindeyiz, zira online arama telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ve teknik araçlarla izleme tedbirlerinden daha ağır bir müdahaledir.

b. Somut olayın ağırlığı

Düzenleme, katalog suçların halihazırda mevcut olan soyut ağırlığına bakılmaksızın, online arama yapılmasını gerektiren suçun da somut olayda özellikle ağır olması gerektiğini açıkça belirtmelidir.

c. İkincillik İlkesinin Uygulanması

Online aramaya, ancak "başka surette delil elde edilmesi olanağının bulunmaması halinde" başvurulabilmelidir. Bu tedbirin başta özel hayatın gizliliği, insan haysiyetinin korunması ve kişisel verilerin korunmasını isteme hakkı gibi temel hak ve özgürlüklere ağır müdahale oluşturduğu gerçeği, ölçülülük ilkesinin somut bir görünümü olarak ikinci derecede uygulanabilirlik koşuluna yer vermek suretiyle göz önünde bulundurulmalıdır.

2. Suç kataloğu

Düzenlemede tedbirin uygulama alanına giren suçlar katalog biçiminde sınırlayıcı olarak sayılmalıdır. Katalogda yer alması gereken suçlar bakımından öncelikle Alman CMK m. 100b/2 de "özellikle ağır suçların" yer aldığını, bu suçların telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri ile düzenlenmiş olan suç kataloğunda yer alan suçlardan daha ağır nitelikte ve dolayısıyla daha dar kapsamlı olduklarını ifade etmiştik. Özellikle ağır suçlar bakımından ise yasada öngörülen cezanın alt ve üst sınırlarının belirleyici, bu surette üst sınırı en az beş yıl hapis cezasını gerektiren suçların "özellikle ağır suç" başlığı altında değerlendirilebileceğini açıklamıştık.

Ancak cezaların ağırlığı bakımından Alman ve Türk hukuk sistemleri arasında ciddi farklılıklar olduğunu belirtmek gerekir. Zira Alman Ceza Kanunu'nda düzenlenen cezalar Türk Ceza Kanunu'na kıyasla çok düşüktür. Bu nedenle, üst sınırı en az beş yıl hapis cezası gerektiren suçların Alman kanun koyucu tarafından özellikle ağır suçlar olarak kabul edilmesi bizim Hukukumuz açısından kabul edilebilir değildir. Dolayısıyla suç kataloğunun dikkate alması gerektiği cezanın alt ve üst sınırlarını Alman Hukuk sistemiyle örtüşerek düzenlemek uygun olmayacaktır. Zira böyle bir durumda tedbirin uygulama alanının katalog suçlarla sınırlandırılmasına ilişkin güvencenin içi boşaltılmış olur ve deyim yerinde ise online arama uygulamada "rutin" bir soruşturma tedbirine dönüşebilir.

Türk Hukuk sisteminde cezaların çok yüksek olması sebebiyle, dile getirdiğimiz sorunların önlenmesi için suç kataloğunda yer alması gereken suçlar bakımından müdafinin görevlendirilmesi zorunluluğunu düzenleyen CMK'nın 150/3. maddesi gereği belirleyici ölçüt olarak alt sınırı en az beş yıl hapis cezası gerektiren suçların düzenlenmesi düşünülebilir. Bu ölçütün çağdaş ceza adaletini tam manasıyla temin etmek için uygun olduğu kanaatindeyiz. Aksi takdirde suç kataloğunun sınırlandırılması mümkün olamaz ve bunun sonucunda birçok suç sebebiyle online arama gerçekleştirilebilir.

3. Müdahalenin Muhatabı

Online aramanın kural olarak şüpheli hakkında düzenlenebileceği, istisnai durumlarda ise, başka kişiler hakkında da tedbirin uygulanabileceği düzenlenmelidir. Başka kişiler bakımından somut olgular şüphelinin başka kişinin bilgi teknolojisi sistemini kullandığını ve sadece şüphelinin bilgi teknolojisi sisteminde uygulanacak olan tedbir ile maddi olgunun araştırılması veya diğer şüphelilerin ortaya çıkarılmasının sağlanamayacağını göstermelidir.

Bunun ötesinde bu tedbire üçüncü kişilerin etkilenmesinin kaçınılmaz olması halinde de başvurulabileceği düzenlenmelidir. Zira şüpheli hakkında bilgi teknolojisi sistemlerinde yapılan aramalarda üçüncü kişilere ait bilgilerin de yer alacak olmasının, tedbirin uygulanmasına engel teşkil etmemesi gerekir. Bu durumda yalnız şüphelinin değil, soruşturmayla ilgisi olmayan üçüncü kişilerin de temel haklarına müdahale edileceği ileri sürülse de tedbirin niteliği ve yapısı gereği (örneğin sosyal medya üzerinden herhangi bir etkileşimin gerçekleşmesi durumunda) üçüncü kişilere ait verilerin elde edilmemesi imkansızdır.

Ayrıca online arama için telekomünikasyon hizmet sağlayıcıları gibi, bilgi teknolojisi hizmet sağlayıcıları bakımından bir iş birliği yapma yükümlülüğü getirilmemelidir.

4. Yükümlülükler

a. Teknik güvenlik önlemleri alma yükümlülüğü

Bilgi teknolojisi sisteminde yalnızca veri toplama için gerekli olan ve tedbirin sonunda teknik olarak mümkün olduğu ölçüde otomatik olarak eski haline getirilecek değişikliklerin yapılması teknik olarak sağlanmalıdır.

b. Rapor tutma yükümlülüğü

Teknik araçların kullanımında, tedbire maruz kalan kişinin haklarının etkili bir şekilde korunmasını ve mahkemede toplanan delillerin güvenilirliğini sağlamak için özel raporlama düzenlemeleri kaleme alınmalıdır. Bu doğrultuda kapsamlı belgelendirme özellikle bir tedbirden önceki adımları, uygulama sürelerini, teknik araçları ve elde edilen verilerin ayrıntılarını anlaşılır kılmalıdır.

c. Verileri silme yükümlülüğü

Tedbir yoluyla elde edilen kişisel verilerin, ceza soruşturması ve tedbirin herhangi bir yargısal denetimi için artık gerekli olmadığı hallerde, derhal silinmesi gerekir. Silme işlemi kayda geçirilmelidir.

d. Bilgilendirme yükümlülüğü

Tedbire maruz kalan kişiyi ve önemli ölçüde etkilenen kişileri alınan online arama tedbiri konusunda bilgilendirmek ve müteakiben başvurulabilecek kanun yollarını ve bunun için öngörülen süreyi belirtmekle gerekir.

5. Sınırları

a. İçerik bakımından

Online arama tedbiri ile tedbire maruz kalan kişinin bilgi teknolojisi sisteminde kaydedilmiş tüm verilere erişim sağlanabileceğinden, içerik bakımından sınırlamanın getirilmesi zaruridir.

İnsan onurunun dokunulmazlığı ilkesinden kaynaklanan özel hayatın mutlak koruma altındaki çekirdek alanına müdahaleyi önlemek için önlemlerin alınması elzemdir. Özel yaşamın çekirdek alanında kişiliğin gelişimi, duygu ve hisler gibi içsel süreçlerin yanı sıra son derece kişisel nitelikteki düşünce, görüş ve deneyimlerin devlet yetkililerinin bunu izleyeceği korkusu olmaksızın ifade edilmesi olasılığını içerir. Bir bilgi teknolojisi sistemine gizli erişim bağlamında, harekete geçen soruşturma yetkililerin çekirdek alana dahil edilebilecek kişisel verileri elde etme riski bulunmaktadır. Ancak bu kişisel verilerin mutlak korunması söz konusudur.

Bu nedenle, online aramanın Türk Hukukunda hüküm altına alınması halinde, çekirdek alanın korunması için muhakkak açık bir düzenleme getirilmeli ve böylelikle çekirdek alanla ilgili verilerin elde edilmesi engellenmelidir.

Bu bağlamda Alman CMK düzenlemesine paralel olarak;

- Online arama tedbirinin yalnızca özel hayatın çekirdek alanından bilgi elde edileceği varsayımına ilişkin olgusal göstergelerin bulunması halinde, tedbire başvurulamayacağı,
- Özel hayatın çekirdek alanına ilişkin verilerin elde edilmemesinin teknik olarak sağlanması gerektiği,
- Teknik önlemlere rağmen özel hayatın çekirdek alanına ilişkin verilerin elde edilmesi halinde, bunların ya derhal silinmeli ya da savcılık tarafından verilerin kullanılabilirliği ve silinmesine ilişkin bir karar için karar veren mahkemeye iletilmesi gerektiği hüküm altına alınmalıdır.

Burada Federal Anayasa mahkemesi tarafından iki aşamalı mekanizma olarak geliştirilen veri değerlendirme ve veri kullanımı düzeyindeki güvenceler aracılığıyla hakkında tedbir uygulanan kişinin koruma ihtiyaçlarının dikkate alınması önem teşkil etmektedir. Hukukumuzda online aramanın düzenlenmesi halinde, özel hayatın çekirdek alanını koruyacak düzenlemelerin bu doğrultuda tasarlanmasını önermekteyiz.

Bu çerçevede ilk aşamada, özel yaşamın çekirdek alanının etkilenebileceğine dair somut göstergelerin bulunması halinde, yasa koyucu çekirdek alanla ilgili verilerin elde edilmemesini sağlamaya çalışmalıdır. Bu bağlamda özellikle bilgi teknolojisi güvenlik önlemleri kullanılmalıdır.

İkinci aşamada ise, değerlendirme ve kullanım aşamasındaki güvenceler vasıtasıyla veri sahiplerinin koruma ihtiyaçlarının dikkate alınması ve bu tür bir erişimin etkilerinin en aza indirilmeye çalışılması gerekmektedir.
Burada bağımsız bir organ tarafından elde edilen verilerin denetlenmesinin, uygun bir usul tedbiri olarak önemli olacağını vurgulamak isteriz.

b. Yetki bakımından

Alman CMK m. 100e/2-1 gereği online arama tedbirine başvurulabilmesi için savcının Mahkemeler Teşkilatı Kanunu'nun 74a/4 (GVG) hükmü gereğince yetki bölgesinde bulunduğu eyalet mahkemesinin devlet güvenlik dairesine talepte bulunması gerekmektedir.

Tedbire karar vermeye yetkili daire, Eyalet Yüksek Mahkemesinin yetki bölgesinde bulunan, ceza yargılamasında görevli olmayan 3 hâkimden oluşan devlet güvenlik dairesine (Staatsschutzkammer) aittir.

Gecikmesinde sakınca bulunan hallerde ise karar vermeye yetkili dairenin başkanının da bu kararı vermeye yönelik yetkisi düzenlenmiş olup, bu durumda 3 gün içinde bu kararın mahkeme dairesi tarafından onaylanması gerekmektedir.

Türk hukukunda online arama konusunda bir yasal düzenleme yapılması halinde buna karar verme yetkisi bakımından sıkı koşullar belirlenmesi gerektiği kanaatindeyiz. Bu sebeple tedbire ancak ağır ceza mahkemesinin oybirliği ile karar verilebileceği gibi yüksek bir eşik belirlenmesi yerinde olur. Tedbirle müdahale edilen temel hak ve özgürlükler ile Alman Hukukunda da yetkinin üç hakimli devlet güvenlik dairesine verildiği göz önünde bulundurulduğunda en uygun çözüm bu gibi görünmektedir. İkincillik ilkesinin hâkim olduğu bir tedbir olduğundan gecikmesinde sakınca bulunması gibi bir durumun doğmayacağı kanaatindeyiz. İstisnai bir durumda gecikmesinde sakınca bulunan bir hal söz konusu olsa dahi bu durumda da Alman Hukuku örnek alınarak, ağır ceza mahkemesi başkanı tarafından karar verme yetkisi düzenlenebilir. Bu durumda dahi derhal kararın heyetin onaya sunulması yönünde düzenleme yapılmalıdır.

c. Zaman bakımından

Tedbirin uygulama süresi muhakkak açık bir şekilde düzenlenmelidir. Alman CMK m. 100e/2-4 uyarınca, online arama tedbiri en fazla bir ay ile sınırlı olmalıdır. Elde edilen soruşturma sonuçları dikkate alınarak, koşulların devam etmesi şartıyla,

her durumda bir aydan fazla olmamak üzere uzatmaya gidilme imkânı tanınmıştır. Kararın süresinin toplam altı aya uzatıldığı ve uzatmanın devam etmesinin talep edildiği hallerde kararın yüksek bölge eyalet mahkemesi tarafından verileceği düzenlenmiştir.

Ceza Muhakemesi Hukukumuzda düzenlenmiş olan telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinin uygulanma süresini incelediğimizde, CMK m. 135/4 gereği, *"tedbir kararı en çok iki ay için verilebilir. Bu süre, bir ay daha uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim yukarıdaki sürelere ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere uzatılmasına karar verebilir."*

CMK m. 140/3 uyarınca ise, *"teknik araçlarla izleme kararı en çok üç haftalık süre için verilebilir. Bu süre gerektiğinde bir hafta daha uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi hâlinde, hâkim yukarıdaki sürelere ek olarak her defasında bir haftadan fazla olmamak ve toplam dört haftayı geçmemek üzere uzatılmasına karar verebilir."*

Online arama tedbirinin temel hak ve özgürlüklere ciddi müdahaleci niteliği dikkate alındığında, CMK m. 140/3 uyarınca öngörülmüş sürelerin uygun olacağı kanaatindeyiz. Ancak online aramanın uygulanması için teknik koşulların oldukça zor, bir başka ifadeyle teknik araç olarak tanımlanan uygun yazlımın tedariğinin zor olması ve tedbirin kısa süreli olmasının kriminalistik açıdan istenen sonucu vermeyebileceği sebebiyle, tedbirin Alman CMK da öngörüldüğü gibi bir ay ile sınırlandırılması düşünülebilir.

Bu noktada, Alman Ceza Muhakemesi Kanunu'nda olduğu gibi, kararın toplam süresi altı ayı aştıktan sonra uzatma talep edilebilmesinin ve bu nedenle tedbirin uzun sürebilmesinin ölçülülük ilkesi açısından kabul edilemez olduğu kanaatinde olduğumuzu vurgulamak gerekir.

d. Kişi bakımından

Alman CMK m. 100d/5-1 uyarınca online arama mesleki gizlilik sebebiyle tanıklıktan çekinme hakkı olan kişilere uygulanamaz.

Alman CMK m. 100d/5-2 uyarınca ise, sanığın yakınlarının tanıklıktan çekinme hakkının bulunduğu düzenleme altına alınmıştır. Bununla birlikte mesleki gizliliğe tabi olan kişilerle bir mesleğin ortaklaşa icrası da dahil olmak üzere sözleşmeye dayalı bir ilişki durumunda, meslek öncesi faaliyetlere yardımcı olunması

veya başka bir yardımcı faaliyet icra edilmesi durumunda da tanıklıktan çekinme hakkının genel olarak bulunduğu ifade edilebilir.

Türk Hukukumuz açısından da kişi bakımından sınırlamanın önemli olduğunu, bu kapsamda tanıklıktan çekinme hakkı bulunan kişilere yönelik düzenleme getirilmesi gerektiğini vurgulamak isteriz.

Ceza Muhakemesi Kanunu'nun 135. Maddesinin 3. Fıkrası uyarınca bir düzenlemenin getirilmesinin uygun olabileceği fikrindeyiz.

6. Delil değerlendirilmesi

Online aramanın düzenlenmiş olduğu Alman CMK. m. 100b uyarınca elde edilen kişisel verilerin ceza yargılamasında değerlendirilmesine yönelik herhangi bir düzenleme yapılmamıştır. Yalnızca Alman CMK m. 100d/2-1 gereği özel hayatın çekirdek alanını ilgilendiren özel kişisel bilgilerin kullanılması mutlak olarak yasaklanmıştır.

Bununla birlikte Alman CMK m. 100d/5-2 uyarınca Alman CMK m. 52 ve m. 53a uyarınca tanıklıktan çekinme hakkı tanınan kişiler bakımından nisbi delil değerlendirme yasağı geçerlidir. Bu çerçevede bu karar ile elde edilen verilerden, temelde yatan güven ilişkisinin öneminin göz önünde bulundurulması suretiyle, söz konusu olayın gerçeklerinin araştırılması veya suçlanan kişinin nerede olduğunun tespit edilmesindeki menfaatle orantısız olmaması halinde yararlanılabilir.

Tedbire yönelik karar alınması sırasındaki (örneğin yetki aşımı veya eksikliği gibi) şekli eksiklikler elde edilen bilgilerin kullanılamaz hale gelmesine yol açabilir. Ancak burada esaslı ile basit eksikliklerin arasında bir ayrım yapılmalıdır. Bununla birlikte maddi koşullarda eksiklikler, olay özelinde değerlendirilmek suretiyle delil yasağı teşkil edebilir veya etmeyebilir. Uygulamada sorunlara yol açmamak için bunların açıkça düzenlemesinde fayda olduğunu düşünmekteyiz.

Tesadüfen elde edilen deliller bakımından; usulüne uygun olarak emredilen bir online arama sırasında asıl yargılamayla doğrudan ilgili olmayan ancak diğer yargılamaların gerçekleştirilmesine ve dolayısıyla başka soruşturmaların başlatılmasına sebep olabilecek tesadüfen bilgi elde edildiği hallerde, bu bilgiler Alman CMK m. 477/2 gereği kullanım ve yararlanma hükmüne uygun olarak diğer katalog suçların soruşturulması için aktarılabilir.

Türk Ceza Muhakemesi Kanunu'nun "tesadüfen elde edilen deliller" başlığını taşıyan 138. Madde gereği ise, *"(1) Arama veya elkoyma koruma tedbirlerinin*

uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir. (2) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir".

Online aramanın Türk hukukumuzda yer alması durumunda, tesadüfen elde edilen veriler bakımından CMK m. 138/2 hükmü ile paralel olarak, yalnızca düzenleme altına alınmış olan katalog suçlarından birinin işlendiği şüphesini uyandırabilecek bir delilin elde edilmesi halinde, bu değerlendirilebilmelidir. Online arama diğer gizli soruşturma tedbirlerine nazaran daha çok temel hak ve özgürlüklere müdahale teşkil ettiği için, tesadüfen elde edilen delilin ancak katalog suçu olması koşuyla muhafaza altına alınabileceği ve bu durumda hukuka uygun delil teşkil edebileceği açıkça düzenlenmelidir. Bir sınırlandırma getirmeksizin tüm suçlar bakımından elde edilen verilerin değerlendirilebileceği varsayılsa, bu, tedbirin uygulanmasının mümkün olmadığı suçların soruşturulması için tedbirin kötüye kullanılmasına kapı açar ve hukuki güvence kaybına neden olur.

SONUÇ

Gizli bir soruşturma tedbiri olan online arama, tedbire maruz kalan kişinin bilgi teknolojisi sistemine sızılmak suretiyle gerçekleştirilen bir tedbirdir.

Online aramanın amacı, üçüncü taraf bilgi teknolojisi sisteminin kullanımını gizlice izlemek, depolanan içeriği kaydetmek ve bu bilgileri soruşturma makamlarına üzerindeki şifreleme tekniklerini aşarak analiz etmek üzere internet aracılığıyla iletmektir.

Günümüz bilgi ve iletişim teknolojilerindeki gelişmelerle daha fazla mücadele edebilmek için dijital verilerin elde edilmesi ve değerlendirilmesi bakımından online arama gibi yeni tedbirlere başvurulması vazgeçilmezdir.

Nitekim Alman hukuk sisteminde online arama hem önleyici hem adli amaçlı düzenlenmiş şekliyle yer almaktadır.

Federal Almanya Anayasası 27 Şubat 2008 tarihli kararında, önleme amaçlı online arama tedbirinin yasallığı bakımından koşullarını net bir şekilde ortaya koymuştur. Tedbirin son derece müdahaleci yapısı nedeniyle, konut dokunulmazlığı, haberleşmenin gizliliği ve kişiliğin korunması haklarının koruması kapsamına giremeyeceğinden, federal anayasa mahkemesi, genel kişilik hakkının yansıması olan bilgi teknolojisi temel hakkı (“IT-Grundrecht”) olarak da bilinen bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğünün garanti altına alınması hakkını (“Recht auf Gewaehrleistung der Vertraulichkeit und Integritaet informationstechnischer Systeme”) geliştirmiştir. Kararda, bilgi teknolojisi temel hakkının, bilimsel ve teknolojik ilerleme ile değişen yaşam koşullarından kaynaklanabilecek tehditlere karşı boşluk doldurucu bir işleve sahip olduğu; bu hakkın sınırsız bir şekilde güvence altına alınmadığını gerek önleyici gerekse adli amaçla müdahalelerin meşru olabileceğini; tehlikenin önlenmesinin sınırlarının yüksek tutulması ve katı koşullara bağlanması gerektiği açıklanmıştır. Bu kapsamda online arama ancak üstün öneme sahip hukuki değerlerin korunması ve somut bir tehlikeye ilişkin olgusal göstergelerin bulunduğu takdirde gerçekleştirilebilir. Federal Anayasa Mahkemesinin dönüm noktası

niteliğindeki 2008 tarihli kararı ile yasa koyucuya bilgi teknolojisi sistemlerine müdahaleler için anayasal çerçevenin sağlanmış olduğunu ve "kişiliğin korunması hakkını" buna göre tanımlamış olduğunu görmekteyiz.

Bu doğrultuda 2008 yılında Federal Kriminal Polis Dairesi'nin uluslararası terörizm tehlikelerine karşı savunma yapmasını öngören yasa kabul edilmiş, Federal Anayasa Mahkemesi'nin belirlediği şartlara uygun olarak, bilgi teknolojisi sistemlerine gizli müdahale de dahil olmak üzere, ilk kez önleyici yetkiler verilmiştir. 2017 yılında ise online arama tedbiri Alman Ceza Muhakemesi Kanunu'nda ilk kez adli amaçla düzenleme altına alınmıştır.

Ancak online arama, başta özel hayatın gizliliği, haberleşme gizliliği ve kişisel verilerin gizliliği olmak üzere çok sayıda temel hak ve özgürlüğü kısıtladığı, şüphelinin ve soruşturma konusu suçla ilgisi olmayan üçüncü kişilerin ve temel hak ve özgürlüklerine yoğun bir müdahale teşkil ettiği, hakkında tedbir uygulanan kişinin tüm kullanım davranışlarını izlediği ve hayatının gizli alanındaki tüm verilere erişerek kapsamlı kişilik profilleri oluşturabildiği için yoğun bir şekilde eleştirilmektedir.

Tedbirin teknik kapsamı bakımından "bilgi teknolojisi sistemi" kavramının tercih edilmesi, bilinçli bir şekilde belirli bir cihaz türüne, belirli bir işletim sistemine, programlamaya veya benzerine bağlı kalmaktan kaçınıldığını göstermektedir. Bu doğrultuda bulut bilişim sistemleri de dahil olmak üzere her türlü elektronik veri işleme sistemi online arama tedbirinin kapsamı dahilindedir. Bilgi teknolojisi sistemine erişim sağlamak için kullanılan teknik araç ise "casus yazılım" olarak adlandırılan bir arama yazılımıdır. Online arama tedbiri ile hedeflenen amaca ulaşılabilmesi bakımından sisteme sızma (infiltrasyon) yönteminin başarılı bir şekilde gerçekleşmesi gerekir. Burada söz konusu olabilecek yöntemler yazılım modifikasyonu yoluyla infiltrasyon, yazılım ve donanım üreticileri vasıtasıyla infiltrasyon veya fiziksel müdahale yoluyla manuel kurulumdur.

Mevzuatımızda yürürlükte olan önleme ve adli amaçlı düzenlemelerin incelemesi, online aramanın Türk hukuk sisteminde düzenlenmediğini göstermektedir.

Türkiye'nin Siber Suç Sözleşmesi'ni imzalamış olması, Konsey üyesi ülkelerin çoğunun online arama tedbirine mevzuatlarında açıkça yer vermesi ve günümüzde bilgi teknoloji sistemleri ile bağlantılı olarak işlenen suçlar ve bunlarla mücadelede etkin bir rol alabileceği nedeniyle bu tedbirin Türk hukukunda da düzenlenmesi gerektiği kanaatindeyiz.

Yargıtay kararlarının incelenmesi sonrasında, online aramanın önemi gizli erişime izin vererek şifreleme sorununun üstesinden gelebilmesi ve cep telefonu gibi bilgi teknolojisi sitemlerine fiziksel olarak el konulmasını gerektirmemesi noktasında ortaya çıkmaktadır.

Özellikle organize suç ve uluslararası terörizm ile mücadelede geleneksel arama, elkoyma ve telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinin şifrelenmiş bilişim sistemlerine erişim sağlayamadıkları hallerde, online aramanın etkili bir koruma tedbiri olabileceği kanaatindeyiz. Dolayısıyla, bilişim sistemlerinden kaynaklanan suçlarla mücadelede, özellikle de organize suçlarla ilgili olarak, teknoloji tabanlı ve teknoloji destekli tedbirlerin kullanılması gerektiğini düşünmekteyiz.

Ancak online arama tedbiri temel hak ve özgürlüklere ciddi bir müdahale teşkil ettiğinden, yasallaştırılmasına ilişkin koşulların katı bir şekilde düzenlenmesi zaruridir. Bu, devletin bir "gözetim devleti" haline gelmesini önlemek ve hukukun üstünlüğünden sapmayarak özgürlük ve güvenlik arasındaki dengeyi sağlamak için gereklidir. Ceza yargılamasının temel amacının, maddi gerçeği ortaya çıkarırken, kişisel hak ve özgürlüklere saygı ile toplumsal düzenin korunması arasında bir denge kurmak olduğu unutulmamalıdır.

Online arama tedbirinin Türk hukukunda yasal zemine kavuşturulması noktasında dikkate alınması gereken bazı önemli hususlar bulunmaktadır. Bu kapsamda önerilerimizi müdahalenin yoğunluğu, tedbirin teknik özellikleri, bağlantılı olduğu temel haklar ve ilkeler, hizmet ettiği amaç ve uygulanma şartları bakımından ele aldık.

Online aramanın şifreli veriler konusunda geleneksel tedbirlerin yetersizliği sorununu aşmasının yanı sıra, gizlice ve uzunca bir süre uygulanabilir olması tedbire, suçla mücadelede etkin bir rol kazandırmaktadır. Keza dijital çağın sunduğu RAM kapasitesindeki iyileşme ve bulut bilişim sistemleri gibi harici depolama alanlarında depolanan verilere de erişim ancak online arama ile sağlanabilir.

Tedbirin teknik özellikleri bakımından, devletin kendisi, bilişim teknolojileri sistemlerinin tüm versiyonlarına uygun yazılım geliştirmelidir. Zira casus yazılımı kendisi geliştirmezse, bunu üçüncü kişilerden temin etmesi gerekecektir. Casus yazılımı üçüncü kişilerden, hele ki karanlık ağda faaliyet gösteren kimselerden temin etmesi halinde, bu durum bilişim güvenliği konusunda devletin yükümlülükleri ile ciddi çelişki doğuracaktır. Bu tür ortamlardan temin edilecek yazılımların güvenlik açıklarından istifade ederek tersine casusluk riski barındırmasının yanı sıra söz konusu

kara borsa faaliyetlerinin güçlenmesine dolaylı yoldan yapacağı katkı da göz önünde bulundurulmalıdır.

Online arama araçlarının teknik özellikleri ve veri koruma konusundaki gereksinimler nedeniyle, tedbirin oldukça karmaşık olduğu ve her bir uygulamanın somut soruşturma bakımından özel olarak tasarlanması gerekmektedir. Bu durum, çok sayıda uzmanlaşmış personele ihtiyaç doğurmaktadır. Bu gerekçelerle, online arama geleneksel teknik araçlarla izleme tedbirlerine bir alternatif değildir. Bu geleneksel yöntemlerden sonuç alınmaması veya sonuç alınma ihtimalinin açıkça düşük veya imkânsız olması gibi çok istisnai durumlarda online arama tedbirine başvurulması düşünülmelidir.

Tedbirin Almanya'daki uygulanmasına baktığımızda, adli amaçlı online arama bakımından istatistikler tedbire uygulamada kısıtlı bir şekilde başvurulduğunu göstermektedir. Bu istatistiklerden görüldüğü üzere, adli tedbir olarak düzenlenmiş olan online arama 2019, 2020 ve 2021 yıllarında fiilen yalnızca toplam 29 kez gerçekleştirilmiştir. Bunun başlıca sebepleri olarak; katı normatif koşulların bulunması, teknik açıdan karmaşık bir müdahale tedbiri olması, hedef sistemin teknik ortamının iyi bir şekilde hazırlanmasını ve araştırılmasını gerektirmesi, casus yazılımın izlenecek olan bilgi teknolojisi sistemine yüklenmesi, yüksek kaynak harcamaları ve uzman personel ihtiyacı gösterilebilir.

Online arama tedbiri, içerisinde bulunduğumuz dijital çağ bakımından her ne kadar gerekli ise de temel hak ve özgürlükler açısından, özellikle de hukuk devleti ilkesi, insan haysiyetinin korunması ilkesi, ölçülülük ilkesi, özel ve aile hayatına saygı hakkı, adil yargılanma hakkı ve kişisel verilerin korunmasını isteme hakkı bakımından çeşitli riskleri de beraberinde getirmektedir. Online aramanın mevzuatımızda düzenlemesi halinde, tüm bu temel hak ve özgürlüklerin dikkate alınması zaruridir. Bu çerçevede özellikle ölçülük ilkesi bakımından, online arama tedbirine örneğin yalnızca örgütlü suçlarla mücadele çerçevesinde başvurulması öngörülebilir. Bununla birlikte mevzuatımızda halihazırda yürürlükte olan gizli soruşturma yöntemlerinde olduğu gibi online arama tedbiri de sıkı uygulanma koşullarına bağlanmalı, hatta temel hak ve özgürlüklere daha ağır bir şekilde müdahale etmesi sebebiyle çok daha sıkı koşullara bağlanmalıdır.

Tedbirin hizmet ettiği amaç bakımından önemle ifade edilmelidir ki, online aramanın, kişilerin temel hak ve özgürlüklerine ağır müdahale oluşturan bir tedbir olması sebebiyle uygulama alanının mümkün olduğunca sınırlı bir kapsamda

belirlenmesi gerekmektedir. Bu sebeple tedbirin -en azından başlangıçta- yalnızca adli amaçlı olarak kullanılmasına cevaz verilmesi gerektiği düşüncesindeyiz. Önleyici amaçlarla online arama tedbirine başvurulması hususuna ise ihtiyatla yaklaştığımızı ifade etmek isteriz. Nitekim Türk hukukunda mevcut önleyici tedbirler (örn. PvSK Ek m. 7) bağlamında yasal düzenlemedeki belirsizliklerden ve hatalı uygulamalardan kaynaklanan sorunlara bir yenisinin eklenmemesi için online arama tedbirinin önleyici amaçlarla uygulanmasına dair bir yasal düzenleme getirilmek istenirse, bu tedbirin uygulanma koşulları, usul ve esasları hiçbir tereddüde yer vermeyecek şekilde açık yasal zemine kavuşturulmalıdır. Aksi takdirde, demokratik bir hukuk devletinde bireylere sağlanması gereken asgari standartlar tehlikeye düşebilir.

Online arama tedbirinin kanuni bir zemine kavuşturulması halinde, tedbirin tüm uygulanma şartları titizlikle ele alınmalıdır.

Online arama yalnızca, bir suç işlendiğine dair kuvvetli bir şüphenin bulunduğu ve delil elde etmenin başka bir yolunun olmadığı, diğer gizli soruşturma tedbirlerinin sonuç vermediği yahut sonuç alınmasının mümkün olmadığının açık olduğu istisnai hallerde uygulama alanı bulması gerekir.

Bununla birlikte hükümde tedbirin uygulama alanına giren suçlar bir katalog halinde yasada düzenlenmeli, bu kataloğun diğer gizli soruşturma tedbirlerinde yer alan suç kataloglarına nazaran daha dar kapsamlı olması da düşünülmelidir.

Bunun ötesinde teknik güvenlik önlemleri alma yükümlülüğü, rapor tutma yükümlülüğü, verileri silme ile bilgilendirme yükümlülüğü gibi yükümlülüklerin açıkça yasa da düzenleme altına alınmaları, hukuki güvencenin sağlanması bakımından önem arz etmektedir.

Açıkça düzenlenmesi gereken bir diğer husus ise, mutlak koruma altında olan özel hayatın çekirdek alanına müdahaleyi önlemeye yönelik önlemlerdir.

Tedbire karar verme yetkisi bakımından yine sıkı koşullar getirilmelidir. Bu surette tedbire ancak ağır ceza mahkemesinin oybirliği ile karar verilebileceği gibi yüksek bir eşik belirlenmesi yerinde olur. Tedbirle müdahale edilen temel hak ve özgürlükler ile Alman Hukukunda da yetkinin üç hakimli devlet güvenlik dairesine verildiği göz önünde bulundurulduğunda en uygun çözüm bu gibi görünmektedir. Gecikmesinde sakınca bulunan bir halin söz konusu olmasında, yine Alman Hukuku dikkate alınarak, ağır ceza mahkemesi başkanı tarafından karar verme yetkisi düzenlenebilir. Bu durumda dahi derhal kararın heyetin onaya sunulması yönünde düzenleme yapılmalıdır.

Tedbirin uygulanma süresi bakımından temel hak ve özgürlüklere teşkil ettiği ağır müdahale göz önünde bulundurulduğunda, tedbirin Alman hukuk sisteminde öngörüldüğü gibi bir ay ile sınırlandırılması düşünülebilir.

Sonuç olarak, online arama tedbiri, diğer gizli soruşturma tedbirlerine kıyasla temel hak ve özgürlüklere ciddi bir müdahale teşkil ettiğinden, uygulanmasına ilişkin tüm koşullar eksiksiz ve net bir şekilde düzenlenmeli, şekli ve maddi koşullar hiçbir soru işaretine yer bırakmayacak biçimde açıklık ve belirlilik kriterlerine göre hüküm altına alınmalıdır.

KAYNAKÇA

Akyürek, Güçlü: Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu, TBB Dergisi, 2012.

Altıparmak, Kerem, Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu, İçinde: Türkiye Barolar Birliği Dergisi, Y.19, 2006.

Ataman, Ahmet, Ceza Yargılaması Hukukunda İletişimin Denetlenmesi Tedbiri, Adalet Yayınevi, Ankara, 2016.

Autorenteam iRights.Lab für bpb.de, Das Sphärenmodell zur Bemessung von Persönlichkeitsrechtsverletzungen, Abschnitt „Die Privatsphäre“, Lizenz CC BY-NC-ND 3.0 DE, Erişim: www.bpb.de, Erişim tarihi: 01.06.2024.

Aydın, İbrahim, AİHM Kararları Işığında Terörle Mücadelede İdari Kolluğun Genel İzleme ve Takip Yetkisi ve Özel Hayatın Korunması, F.Ü. Sosyal Bilimler Dergisi, 2024-34/1.

Baer in: Wabnitz/Janovski, Handbuch Wirtschafts-und Steuerstrafrecht, 4. Auflage, Beck Verlage, München 2014.

Balcı, Murat, Delillerin Suçun İşlendği Hususunda Yeterli Şüphe Sebebi Oluşturması, Terazi Hukuk Dergisi, Yıl: 7, 2012.

Balcı, Murat/Çakır, Kerim, Investigation Authorities’ Ability to Secretly Obtain Evidence From Electronic Devices Through Remote Activation in the French Penal Procedural Code, Bilişim Hukuk Dergisi 2023/2.

Bantlin, Franziska, Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, JuS 2019.

Başlar, Yusuf, Ceza Yargılamasında Elektronik Delil, Yetkin, Ankara, 2016.

Başlar, Yusuf, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, Uyuşmazlık Mahkemesi Dergisi, 2014.

Baştürk, İhsan, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", Fasikül Hukuk Dergisi, Cilt 2, Sayı 9, 2010.

Baum, Gerhart Rudolf/Schantz, Peter, die Novelle des BKA-Gesetzes-Eine rechtspolitische und verfassungsrechtliche Kritik, ZRP 2008.

Bayraktar, Çiler Damla, Die Online-Durchsuchungsmassnachme in der deutschen Rechtsordnung mit Gesetzesaenderung vom 25.05.2018 und 24.08.2017 und die Durchführbarkeit dieser Massnahme in der türkischen Rechtsordnung, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019.

Beukelmann, Stephan: Verwertbarkeit von EncroChat-Daten NJW-Spezial 2022.

BGH, Beschl. V. 2.3.2022 – 5 StR 457/21, Kein Verwertungsverbot von Encro-Chat-Daten, NStZ 2022.

BGH, Beschl. V. 6.7.2022 – 4 StR 63/22, Verwertbarkeit von Encro-Chat Daten, NStZ-RR 2022.

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter: Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018.

BMI - Bundessministerium des Innern, Fragenkatalog des Bundesministeriums der Justiz vom 22.08.2007, Erişim: https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, Erişim tarihi: 01.06.2024.

Bode, Thoma A., Verdeckte strafprozessuale Ermittlungsmassnahmen, 2012.

Borges, Georg, Rechtsfragen des Phishing – Ein Überblick, NJW 2005.

Böhm, Klaus; Die Umsetzung der Europäischen Ermittlungsanordnung, NJW 2017.

Bratke, Bastian, die Quellen-Telekommunikationsüberwachung im Strafverfahren, 2013.

BSI, Sicher im digitalen Alltag - Informationen, Empfehlungen und Hilfe-zur-Selbsthilfe, Erişim: BSI - Tipps für mehr Sicherheit im digitalen Alltag (bund.de).

Buermeyer, Ulf /Prof. Dr. Baecker, Matthias, Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (kurz: HRRS) 2009.

Buermeyer, Ulf, Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme. HRRS, Ausgabe 4/2007.

Buermeyer, Ulf, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur Formulierungshilfe des MMJV zur Einführung von Rechtsgrundlagen für Online Durchsuchung und Quellen-TKÜ im Strafprozess, 2015.

Buermeyer, Ulf, Wann darf der Staat in den PC? Verfassungsrechtliche Grenzen der Online-Durchsuchung, 2008.

Bulduk, Seyfi, Telekomünikasyon Yoluyla Yapılan İletişimin Adli ve Önleme Amaçlı Olarak Denetlenmesi. 1.baskı, Adalet Yayınevi, Ankara, 2015.

Bundesamt für Justiz, Statistik zur Online-Durchsuchung Erişim: BfJ - Detailsuche (bundesjustizamt.de) Erişim Tarihi: 01.06.2024

Bundesinnenministerium beantwortet Fragen zur Online-Durchsuchung (netzpolitik.org), Erişim tarihi: 01.06.2024.

Centel, Nur/Zafer, Hamide, Ceza Muhakemesi Hukuku, 15. Baskı, Beta Yayınevi, Ankara 2018.

Centel, Nur: "5271 Sayılı Ceza Muhakemesi Kanunu'na Göre, Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", GSÜHFD (Prof. Dr. Köksal Bayraktar'a Armağan), C:1, 2010.

Çağlayan, Ramazan, Kolluk ve Güvenlik Hukuku, 1. Baskı, Ankara, 2022.

Çulha, Rıfat; Demirci, Turgay; Nuhoğlu, Ayşe; Yenisey, Feridun: Ceza Muhakemesinin Soruşturma Evresindeki Süjeler İçin CMK Cep Kitabı, 5.bs, TBB Yayınları, Ankara, 2016.

Dağ, Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması" Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora Tezi, 2011.

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

Dencker, Friedrich, Verwertungsverbote im Strafprozess, Köln 1997.

Derin, Benjamin / Dr. Golla, Sebastian J., Der Staat als Manipulant und Saboteur der IT-Sicherheit, NJW 2019.

Derin, Benjamin / Singelnstein: Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NStZ 2021.

Directive - 95/46 - EN - Data Protection Directive - EUR-Lex (europa.eu), Erişim tarihi: 01.06.2024.

Deutscher Bundestag, BT-Drucksache 18/127, Erişim: https://dserver.bundestag.de/btd/18/127/1812785.pdf , Erişim Tarihi: 01.06.2024

Deutscher Bundestag, BT-Drucksache 18/127, Erişim: https://dserver.bundestag.de/btd/18/112/1811272.pdf , Erişim Tarihi: 01.06.2024

Dewald, Andreas/Freiling, Felix C., Forensische Informatik, Oktober 2015.

Duran, "Ceza Muhakemesi Kanunu'nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK m.134)", Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 14, Sayı: 173, 2019.

Dülger, Murat Volkan, Bilişm Suçları ve İnternet İletişim Hukuku, 10. Baskı, Seçkin, Ankara, 2023.

Dülger, Murat Volkan/Taşkın, Şaban Cankat, Ceza Muhakemesi Hukuku, 2023, 1. Baskı, Seçkin, Ankara, 2023.

Eisenberg, Ulrich, Beweisrecht der StPO, 10. Auflage 2017.

Ejder Yılmaz, Hukuk Sözlüğü, Yetkin Yayınları, Ankara, 2006.

Ekici, Şerafettin, Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon (Elektronik İletişim) Hukuku, Vedat Kitapçılık, İstanbul 2006.

Epping, Volker, Grundrechte, 7. Auflage 2017.

Erdem, Mustafa Ruhan, Ceza Muhakemesinde, Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri, Ankara, Seçkin Yayıncılık, 2001.

Erdem, Dilek Özge, Dijital Delillerin Elde Edilme Yöntemi Olarak Alman Ceza Muhakemesinde (Alman CMK §100b) Online (Çevrimiçi) Arama Tedbiri ve Tedbirin Türk Hukukunda Uygulanabilirliği, CHD Ağustos 2023, Sayı: 52.

Erden Tütüncü, Efser/Taşçı Aydemir, Ece. "Kişisel Verilerin Ceza Muhakemesinde Korunmasına İlişkin Kısa Bir Değerlendirme", Fasikül Aylık Hukuk Dergisi, 2022/4 (Ekim-Kasım-Aralık)(Baskıda).

Eroğlu, Fulya: "Örgütlü Suçlarda Yargılama Sistemi", Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora Tezi, 2016.

Eschelbach in: Satzger/Schluckebier/Widmaier StPO 5. Auflage, 2022.

Feyzioğlu, Metin: Ceza Muhakemesinde İspatın Ölçütü Olarak Vicdani Kanaat, Ankara 2015.

Fox, Dirk, Online-Durchsuchung, in DUD 2007.

Fredrik Roggan, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung, StV 2017.

Flade, Florian, Überwachungssoftware: Der Bundestrojaner, den keiner nutzt | tagesschau.de, Erişim tarihi: 01.06.2024.

Fragenkatalog des Bundesministeriums der Justiz (netzpolitik.org), Erişim tarihi: 01.06.2024.

Fechner, Nina, Wahrung der Intimität? Grenzen des Persönlichkeitsschutzes für Prominente, Düsseldorf, 2010, Peter Lang Verlag

Freiling/Saffering/Rückert,Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018.

Gebhard, Angelina /Michalke, Reinhart: Der Zweck heiligt die Mittel nicht, NJW 2022.

Gedik, Doğan, "Bilişim Suçlarında IP Tespiti ile Ekran Görüntüleri Çıktılarının İspat Değeri", Bilişim Hukuku Dergisi, cilt 1, sayı 1, 2019.

Geleri, Aytekin/İleri, Hakan, Organize Suçlarla Mücadelede Gizli ve Örtülü Yaklaşımlar, Seçkin, Ankara, 2003.

Gökcen, Ahmet / Balcı, Murat / Alşahin, Mehmet Emin / Çakır, Kerim, Ceza Muhakemesi Hukuku, Adalet Yayınevi, 6. Baskı, Ankara, 2022.

Gökcen, Ahmet / Balcı, Murat / Alşahin, Mehmet Emin / Çakır, Kerim, Ceza Muhakemesi Hukuku II, Adalet Yayınevi, Ankara, 2017.

Gökcen, Ahmet, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma (Özellikle Telefonların Gizlice Denetlenmesi), 1. Baskı, Dokuz Eylül Üniversitesi Hukuk Fakültesi Döner Sermaye İşletmesi Yayınları, Ankara,1994.

Gökcen, Ahmet/Çakır, Kerim, Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019.

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

Gören, Zafer, Anayasa Hukukuna Giriş, İzmir, 1997.

Görevlinin Görevin Gerektirdiği Suçlar Bakımından Cezalandırılabilirliği, Yetkin, Ankara, 2003.

Graf in: BeckOK StPO mit RiStBV und MiStra, Graf 50. Edition Stand: 2024.

Grossmann, Sven, Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, JA 2019.

Grözinger in: Müller/Schlothauer/Knauer, Rn. 291, 292 Münchener Anwaltsbuch Strafverteidigung 3. Auflage, 2022.

Gümüşay, Mert, Türk Hukukunda Adli ve Önleme Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2009.

Gün, Nagihan, "Türk Ceza Hukukunda Bilişim Suçları", Çankaya Üniversitesi, 2020.

Hafızoğulları, Zeki, Ceza Normu, Normatif Bir Yapı Olarak Ceza Hukuku Düzeni, Ankara 1996.

Hartmann in: Dölling/Duttge/Rössner, Gesamtes Strafrecht, 2022.

Hauck in: Löwe-Rosenberg StPO 27. Auflage, 2019.

Heermann, Thorsten: BGH: Encro-Chat Daten dürfen zur Aufklaerung schwerer Straftaten verwertet werden ZD-AKtuel 2022, 01213.

Heinrich, Manfred, Surfen im Internet und Cloud-Computing zwischen Telekommunikationsüberwachung und Online-Durchsuchung, ZIS Ausgabe 09/2020.

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integritaet eigengenutzter informationstechnischer Systeme, JZ 21/2008.

Hofmann, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005.

Hornung, Gerrit, Ermächtigungsgrundlage für die „Online-Durchsuchung"?, DuD 2007, 575 (580).

Joecks, Wolfgang, Strafprozessordnung, 4. Auflage 2015.

Kaboğlu, İbrahim Ö., Özgürlükler Hukuku, Ankara, 2002.

Karagülmez, A, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, 5. Baskı, Ankara, 2014.

Karakehya, Hakan, Ceza Muhakemesinin Amacı, İÜHFM C. LXV, S. 2, 2007.

Karlsruher Kommentar, KK STPO/Heinrichs/Weingast 9. Auflage, 2023.

Kassebohm in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, §43 Strafrecht im Bereich der Informationstechnologien, 2019.

Kaufmann, Noogie C., BGH lehnt Online-Durchsuchungen ab und NRW schafft statthaftes Gesetz, MMR 2/2007.

Kaygusuz, Ziyaettin, Zor ve Silah Kullanmada Standart Bir Uygulama Modeli: Ölçülülük İlkesi, Bilge Yayınevi, Ankara, 2016.

Kaymaz, Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 3. Baskı, Seçkin, Ankara, 2013.

Kemal Oğuzman, Özer Seliçi, Saibe Özdemir Oktay, Eşya Hukuku, Gözden Geçirilmiş 11. Bası, Filiz Kitabevi, İstanbul, 2006.

Kemper, Martin, Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZRP 2007.

Kızılırmak, Baran, Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2018, s. 34.

Kipker, Denis Kenji/Bruns, Hauke: Digitale Bewaehrungsprobe für ein Recht auf faires Verfahren MMR 2022.

Knierim, Thomas C / Dr. Oehmichen, Anna, in Knierim/Oehmichen/Beck/Geisler, Gesamtes Strafrecht aktuell, 1. Auflage 2018, Kapitel 20: Quellen-TKÜ und Online Durchsuchung, 2018.

Kochheim, Dieter, Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmassnahmen in der StPO seit dem 24.08.2017, KriPoZ 2/2018.

Kohlmann, Diana, Online-Durchsuchungen und andere Massnahmen mit Technikeinsatz 1. Auflage, 2012.

Köhler in: Meyer -Gossner/Schmitt STPO mit GVG und Nebengesetzen, 65. Auflage, 2022.

Köker, Nilüfer, Çeviri: Prof. Dr. Prof. h.c. Arndt Sinn, “Kaynak Telekomünikasyon Denetimi ve Online Arama Yoluyla Yeni Gizli Soruşturma Tedbirleri”, Fasikül Aylık Hukuk Dergisi, Haziran, 2019.

Kruse, Björn /Grzesiek, Mathias, Die Online-Durchsuchung als digitale Allzweckwaffe – Zur Kritik an überbordenden Ermittlungsmethoden, KritV 4/2017.

Kubiciel, Michael, Zwischen Effektivität und Legitimität: Zum Handlungsspielraum des Gesetzgebers nach der "Deal"-Entscheidung des BVerfG, HRRS 2014.

Kudlich, Hans, JR 2003, Rn. 453, 454

Kudlich, Hans, Zur Zulaessigkeit strafprozessualer Online-Durchsuchungen, HFR 19/2007.

Kunter, Nurullah, "Tehlike Tedbiri Genel Teorisi ve Para Cezaları İçin Haciz ve İhtiyati Haciz", İÜHFM, C.34, S:1-4, 1968.

Kunter, Nurullah/ Feridun Yenisey/Ayşe Nuhoğlu: Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18.Bası, Beta Yayınevi, İstanbul, 2010.

Kutscha, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007.

Kühne, Heinz Heiner, Strafprozessrecht, 9. Auflage, 2015.

Küzeci. Elif, Kişisel Verilerin Korunması, 2. baskı, Turhan Kitabevi Yayınları, 2018.

Leipold, Klaus, Die Online_Durchsuchung, NJW Spezial, 2007.

Lepsius, Oliver, Der große Lauschangriff vor dem Bundesverfassungsgericht, Jura 2005.

Martini, Mario / Fröhlingsdorf, Sarah, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020.

Mathew ve Rodrigues, 2018. Mathew, H.L., Rodrigues, L. L. R. (2018). Prioritizing the Factors Affecting Cloud ERP Adoption – An Analytic Hierarchy Process Approach. International Journal of Emerging Markets, 13(6), 1559-1577. doi:10.1108/IJoEM-10-2017-0404.

Meyer-Gossner, Lutz/Schmitt-Bertram, Strafprozessordnung: StPO – Gerichtsverfassungsgesetz, Nebengesetz und ergaenzende Bestimmungen, 65. Auflage, C.H.Beck, München 2022.

Momsen, Carsten / Bruckmann, Philipp, Soziale Netzwerke als Ort der Kriminalitaet und Ort von Ermittlungen – Wie wirken sich die Online-Durchsuchung und Quellen-TKÜ auf die Nutzung sozialer Netzwerke aus? KriPoZ 1/2019.

Naumann in: BKAG, 1. Auflage 2023.

Nockemann, Annamaria, Online-Durchsuchung im Spannungsfeld zwischen Praevention und Repression, 2018 Erişim: https://monami.hs-mittweida.de/frontdoor/deliver/index/docId/10347/file/BA-AnnamariaNockemann.pdf Erişim tarihi: 01.06.2024.

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

Önok, Murat R., "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği." Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. 19/2 (Prof. Dr. Nur Centel'e Armağan), 2013.

Özbek, Mücahid, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", 2015, Erişim: GSI_Articletter_2015_Summer_Article6.pdf (goksusafiisik.av.tr), Erişim tarihi: 01.06.2024.

Özbek, Veli Özer, Ceza Muhakemesi Hukukunda Delil Yasakları, Alman-Türk Karşılaştırmaı Ceza Hukuku, Cilt III, İstanbul, 2010.

Özbek, Veli Özer, Polis Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler ve Hukuka Aykırı Müdahalelere Karşı Korunma Çareleri (Önleme ve Koruma Tedbirleri), 2. Baskı, Seçkin, Ankara, 2023.

Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar, Ceza Muhakemesi Hukuku, 16. Baskı, Ankara, 2023.

Özbek, Veli Özer: "Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları", DEÜHFD, C:4, S:2, 2002.

Özbudun, Ergun, Özel Haberleşmenin Gizliliği, AÜHFM, 50. Yıl Armağanı, Ankara, 1977.

Özbudun, Ergun, Türk Anayasa Hukuku, İstanbul, 2001.

Özen, Mustafa, Öğreti ve Uygulama Işığında Ceza Muhakemesi Hukuku, 1.baskı, Adalet Yayınevi, Ankara, 2017.

Öztekin Tosun, Türk Suç Muhakemesi Hukuku Dersleri, C.1, 4.basım, Acar Matbaacılık, İstanbul, 1984.

Öztürk, Bahri, Ceza Muhakemesi Hukukunda Koğuşturma Mecburiyeti (Hazırlık Soruşturması), Ankara, 1991.

Öztürk, Bahri, CMUK Reformu ve Delil Yasakları, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Haziran, 1994.

Öztürk, Bahri, Özel Hayatın Gizliliği ve Arama, Manisa Barosu Dergisi, Yıl 11, c.4, 1992.

Öztürk, Bahri/ Altınok Çalışkan, Elif/ Seyhan, Serkan, Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı, 2. Baskı, Ankara, 2022.

Öztürk, Bahri/Eker Kazancı, Behiye/Soyer Güleç, Sesim; Ceza Muhakemesi Hukukunda Koruma Tedbirleri, 5. Bası, Ankara, 2022.

Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/ Saygılar, Yasemin F./Alan, Esra/ Erden Tütüncü, Efser/Özaydın, Özdem/ Can Tok, Mehmet, Ana hatlarıyla Ceza Muhakemesi Hukuku (Ders Kitabı), 10. Baskı, Ankara, 2023.

Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/ Saygılar, Yasemin F./Alan, Esra/ Özaydın, Özdem/ Erden Tütüncü, Efser/ Can Tok, Mehmet, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 17. Baskı, Ankara, 2023.

Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/ Saygılar, Yasemin F./ Altınok Çalışkan, Elif/ Alan, Esra/ Özaydın, Özdem/ Erden Tütüncü, Efser/Güzel, İdris/Köker, Nilüfer/ Can Tok, Mehmet, 3. Baskı, Ankara, 2024.

Öztürk, Bahri: Yeni CMK'da Delil Yasakları, Uğur Alacakaptan'a Armağan, Cilt 1, İstanbul, 2008.

Öztürk, Grundlagen der Beweisverbote im türkischen und deutschen Strafverfahrensrecht, Zeitschrift für die gesamte Strafrechtswissenschaft, Berlin, New York, 1992.

Palm, Franz /Roy, Rudolf, Der BGH und der Zugriff auf Mailboxen, NJW 1997.

Park, Durchsuchung und Beschlagnahmer 5. Auflage, 2022.

Pfitzmann, Andreas, Möglichkeiten und Grenzen der Nutzungsüberwachung von IuK-Systemen, S. 5, Erişim: Microsoft Word - Möglichkeiten und Grenzen der Nutzungsüberwachung von IuK-Systemen V1.0.doc (tu-dresden.de), Erişim tarihi: 01.06.2024.

Pohl, Hartmut, Zur Technik der heimlichen Online-Durchsuchung, DuD 31/2007.

Pohlmann, Norbert / Riedel, Rene, Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen: Die Quellen-TKÜ bringt mit dem Bundestrojaner große Risiken für eine dringend notwendige vertrauenswürdige IT-Sicherheit und nachhaltige Digitalisierung, DuD 2018.

Pötters, Stephan, Beschaeftigtendaten in der Cloud, NZA 2013.

Pretz, Mona, Online-Durchsuchung und Quellen-TKÜ, Digitale Ermittlungsmethoden der Strafverfolgungsbehörden, Freilaw 2/2016.

Redaktion FD-StrafR: LG BERLİN legt den EncroChat-Fall dem EUGH vor, FD-StrafR 2022, 452559.

Rehak, Rainer: Angezapft - Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 2011.

Roggan, Fredrik, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektroniische Überwachungsmaßnahme mit Risiken für Beschuldigte und die Allgemeinheit. In: Strafverteidiger (StV) 2017, Nr. 12.

Roggan, Fredrik, Das neue BKA-Gesetz-zur weiteren Zentraliserung der deutschen Sicherheitsarchitektur, NJW 2009.

Roggan, Fredrik, Die Überwachung von IT-Systemen und das Wohnungsrundrecht, Vorgaenge Nr. 227, Polizei und Technik, 11/2019.

Roßnagel, Alexander/Skistims, Hendrik: Rechtlicher Schutz vor Staatstrojanern-Verfassungsrechtliche Analyse einer Regierungsmalware ZD 1/2012.

Roxin, Claus / SchünemannBernd, Strafverfahrensrecht, 29. Aufl. 2017.

Rückert in: Münchener Kommentar zur StPO 2. Auflage, 2023.

Saadet Yüksel, Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, Beta, İstanbul, 2012.

Schiemann, Anja, Effektivere und praxistauglichere Ausgestaltung des Strafverfahren? Was von der grossen StPO-Refomr übriggeblieben ist, KriPoZ 6, 2017.

Schlegel, Stephan, Warum die Festplatte keine Wohnung ist – Art. 13 GG und die Online-Durchsuchung, GA 2007.

Schramm, Marc / Jansen, Kathrin, Die Online-Durchsuchung im Lichte der Rechtsprechung, Erişim: https://www.uni-muenster.de/Jura.tkr/oer/wp-content/uploads/2010/06/Jur.Info_Nr1-2008-Online-Durchsuchung_im_Lichte_der_Rspr.pdf, Erişim tarihi: 01.06.2024.

SEV 108 - Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (coe.int), Erişim tarihi: 01.06.2024.

Sieber, Ulrich/Brodowski, Dominik in: Handbuch Multimedia-Recht Werkstand: 58. EL, Maerz 2022.

Sieber, Ulrich /Brodowski, Dominik, Teil 19.3 Strafprozessrecht, VI. Online Durchsuchung Rn. 161.

Sieber, Ulrich, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1BvR 370/07 zum Thema der Online-Durchsuchungen – Version 1.0 vom 09.10.2007 zur Anhörung in der mündl. Verhandlung vom 10.10.2007.

Singelnstein, Tobias, Strafprozessuale Verwendungsregelungen zwischen Zwecksbindungsgrundsatz und Verwertungsverboten, ZStW 2008.

Singelnstein, Tobias/Derin, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017.

Sinn, Arndt, "Kaynak Telekomünikasyon Denetimi ve Online Arama Yoluyla Yeni Gizli Soruşturma Tedbirleri", Fasikül Aylık Hukuk Dergisi, İnsan Hakları Özel Sayısı, s. 111, Şubat 2019.

Sinn, Arndt, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334), 2017.

Soine, Michael, Die strafprozessuale Online-Durchsuchung, NStZ 2018.

Soine, Michael, Eingriffe in informationstechnische Systeme nach dem Polizairecht des Bundes und Laender, NVwZ 2012.

Sönmez,Göktuğ/Çelik, Emine, Anonimlik ve İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri, Yıl: 22, Cilt:22, Sayı: 1, Haziran 2020,

Sparenberg, Philipp /Heintz, Veris-Pascal, Online-Durchsuchung und Vorratsdatenspeicheurng – Das neue BKA-esetz – mit Vollgas in den Überwachungsstaat? Freilaw 2/2009 (Freiburg Law Students Journal), HeinOnline.

Strate, Gerhard, HRRS Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht, Januar 2022 Heft 1/2022, 23. Jahrgang.

Şahin, Cumhur, Sanığın Kolluk Tarafından Sorgulanması, Doktora Tezi, Ankara, 1994.

Şahin, Cumhur/Göktürk, Neslihan, Ceza Muhakemesi Hukuku I, 12. Bası, Ankara, 2021.

Şahin, Cumhur/Göktürk, Neslihan, Ceza Muhakemesi Hukuku II, 12. Bası, Ankara, 2022.

Şen, Ersan, "E-Posta Takibi", Terazi Hukuk Dergisi, C:9, S:97, 2014.

Şen, Ersan, Türk Hukuku'nda Telefon Dinleme-Gizli Soruşturmacı-X Muhbir, 6.baskı, Seçkin Yayıncılık, Ankara, 2013.

Şentürk Akaner, Candide, Bir Koruma Tedbiri Olarak Online Arama ve Türk Hukukunda Uygulanabilirliği, 1. Baskı, Seçkin, Ankara, 2022.

Taner, Ceza Muhakemeleri Usulü, 3. Bası, İstanbul 1995.

Tanör, Bülent/Yüzbaşıoğlu, Nemci, 1982 Anayasasına Göre Türk Anayasa Hukuku, İstanbul, 2002.

Tanrıkulu, Cengiz, "Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma" Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2014.

Taşkın, Mustafa, Adli ve İstihbari Amaçlı İletişimin Denetlenmesi, 4.baskı, Seçkin Yayınları, Ankara, 2013.

Taştan, "Telekomünikasyon Yoluyla Gerçekleştirilen İletişimin, Önleme (İstihbari) Amaçlı Olarak Denetlenmesinin Amaç, Kapsam ve Sınırları", Terazi Hukuk Dergisi, S. 29, 2009.

Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sancakdar, Oğuz/ Önok, Rıfat Murat; İnsan Hakları El kitabı, 9. Baskı, 2021.

Tezcan, Durmuş, Organize Suçlulukla Mücadelede Özel Ceza Muhakemesi Tedbirleri, Ankara Barosu Hukuk Kurultayı 2000, Ankara, 2000.

Topcu/Alzoubi/Elbasi/Camalan, Social Medai Zero-Day Attack Detection Using TensorFlow, Electronics 2023, S. 2, Erişim: https://doi.org/10.3390/electronics12173554, Eriim tarihi: 13.03.2024.

Toroslu, Nevzat, Ceza Hukuku Genel Kısım, Savaş Yayınları, 14. Baskı, Ankara, 2018.

Tutar, Hasan / Yılmaz, M. Kemal, Genel İletişim, Kavramlar ve Modeller, Seçkin, Ankara 2005.

Uğraş, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", Türkiye Barolar Birliği Dergisi, 2021 Sayı 154.

Ünver, Yener/Hakeri, Hakan, Ceza Muhakemesi Hukuku, 19. Baskı, Adalet Yayınevi, 2022.

Volk, Klaus, Grundkurs StPO, C.H. Beck Verlag, München 2005.

Warntjen, Maximilian, Heimliche Zwangsmassnahmen und der Kernbereich privater Lebensgestaltung, 2007.

Yenisey, Feridun, Kolluk Hukuku, Beta Basım, 2.bs., İstanbul, 2015.

Yenisey, Feridun, Uygulanan ve Olması Gereken Ceza Muhakemesi Hukukunda Hazırlık Soruşturması ve Polis, Beta Basın Yayım Dağıtım, İstanbul, 1996.

Yenisey, Feridun/Nuhoğlu, Ayşe, Ceza Muhakemesi Hukuku, 11. Baskı, Ankara, 2023.

Yenisey, Feridun: Kolluk Hukuku, Beta Basım, 2.bs., İstanbul, 2015.

Yetim, Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği), Seçkin Yayıncılık, Ankara, 2016.

Yılmaz, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, Adalet Yayınevi, Ankara, 2016.

Yüce, Turhan Tufan, Ceza Muhakemesinde Hukuk Devleti Esasları, Ankara Barosu Dergisi, Sayı:5, 1968.

Yüce, Turhan Tufan, Sanığın Savunması ve Korunması Açısından Ceza Soruşturmasının Ümanist İlkeleri, TBBD, S.1, 1998.

Yüksel, Saadet, Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişim, 1.basım, Beta Yayınevi, İstanbul, 2012.

Zerbes, Ingeborg/El-Ghazi, Mohamed, Zugriff auf Computer: Von der gegenstaendlichen zur virtuellen Durchsuchung, NStZ 2015.