İNTERNET VEYA DİĞER AĞLAR ÜZERİNDEN YAPILAN İLETİŞİMİN UZAKTAN ERİŞİM, CASUS YAZILIM VEYA ÇEREZ KULLANILARAK DENETLENİP DENETLENEMEYECEĞİ SORUNU

THE PROBLEM ON INTERCEPTING OF THE INTERNET OR ANOTHER NETWORKS COMMUNICATION WHETHER USING SPY OR COOKIE OR REMOTE ACCESS

Araştırma Makalesi

Fatih BİRTEK*

ÖZ

Bir koruma tedbiri olarak iletişimin denetlenmesi, pek çok ülkede olduğu gibi Türk hukukunda da açık bir şekilde düzenlenmiştir. Yürürlüğe girdiği 2005 yılından bu yana tedbire ilişkin Ceza Muhakemesi Kanunu'nun (CMK'nin) m 135-138 hükümlerinde pek çok değişik yapıldığı halde, tedbirin internet veya diğer ağlar marifetiyle yürütülen iletişimin denetlenebilmesine dair detaylı bir düzenleme yapılmamıştır. Karşılaştırmalı hukukta iletişimin denetlenmesi tedbirine ilişkin uygulama, internet veya diğer ağlar üzerinden gerçekleştirilen iletişimini de kapsayacak şekilde ve uzaktan erişim yoluyla denetimi kapsayacak şekilde genişlemektedir.

CMK'nin 135. maddesinde düzenlenen iletişimin denetlenmesi tedbiri, internet veya diğer ağlar üzerinden yapılan iletişimin denetlenebilmesini kapsamına alsa da bu ağlar üzerinden yapılacak iletişimin, uzaktan erişim veya casus yazılımlar ya da çerez kullanılarak denetlenmesine dair yeterli açıklığı içermemektedir. Günümüz iletişiminin, klasik iletişim araçlarından internet veya diğer ağlar üzerinde çalışan iletişim araçlarına doğru belirgin bir şekilde yoğunlaşması nedeniyle, iletişimin denetlenmesi tedbirinin bu ağlar marifetiyle yapılan iletişimin uzaktan erişim veya casus yazılımlar ya da çerez kullanılarak denetlenmesini/ izlenmesini kapsayacak şekilde düzenlenmesi ve tedbirin uygulama alanının genişletilmesi bir zorunluluk halini almıştır.

DOI: 10.32957/hacettepehdf.1841319

Makalenin Geliş Tarihi: 12.12.2025 **Makalenin Kabul Tarihi:** 04.02.2026

* Prof. Dr., Sivas Cumhuriyet Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi

E Posta: fatihbirtek@hotmail.com

ORCID: 0000-0001-7019-0653

Bu makale Hacettepe Hukuk Fakültesi Dergisi Araştırma ve Yayın Etiği kurallarına uygun olarak hazırlanmıştır.

Anahtar Kelimeler: İletişimin Denetlenmesi, Denetim, Koruma Tedbiri, Uzaktan Erişim, Casus Yazılım, Çerez

ABSTRACT

Interception of communication as a protective measure is clearly regulated in Turkish Criminal Procedure Law, as in many other countries. Since its entry into force in 2005, too many amendments have been made to Articles 135-138 of the Criminal Procedure Act (CPA) but have not been a detailed regulation has been introduced regarding the ability to monitor communications conducted via the internet or other networks. Within the comparative law, implementing of interception of communication preventive measure has expanded to include systems for conducted via the internet or other network and also remote acces surveillance.

While the process of intercepting communications regulated in Article 135 of the CMK encompasses the ability to monitor communications conducted via the internet or other networks, it does not include implementing of remote access, spyware, or cookie-harvesting in terms of communications conducted via these networks. Due to the significant concentration of communication from classical kinds of communication tools towards means of communication operating on the Internet or other networks, the implementing of surveillance of communication is now being carried out through these networks. Therefore a new wide amendment shoud be made on implementing of interception of communication preventive measuries which is by means of remote access or spyware, or using cookies.

Keywords: Interception of Communication, Monitoring, Preventive Measures, Remote Access, Spyware, Cookie

EXTENDED SUMMARY

At the present time, electronic communication tools are more preferable to traditional communication tools because they are both economical and more accessible. Especially with the widespread use of the internet, electronic communication is largely internet-based. However, legal regulations governing the protection of communication tools have not kept up with the dizzying advances in telecomunication technology.

Electronic communication conducted via the internet or other networks presents certain technical challenges in terms of monitoring and control (difficulty of detection/ interception and tracking or the availability of encrypted communication methods or the ability to quickly change the communication tool, etc.). These challenges are exploited by perpetrators, and communication related to crimes is largely conducted via communication platforms provided via the internet or other networks.

In comparative law, the interception/ monitoring of communication is expanded to include electronic communication tools and then to include internet-based communication tools. Public authorities are

exploring new ways to legally intervene in the ever-evolving and evolving telecommunication tools. Undoubtedly, the search for such methods, which emerged in the United States, the United Kingdom, and Germany, has sparked serious and long-standing debates in the countries concerned, on the grounds that they violate the right to privacy and respect for the right to privacy.

In the practice of the European Court of Human Rights (ECtHR), regardless of the means of communication, the privacy of the parties involved in individual communication is prefable. Therefore, it is necessary and imperative for legal certainty that any interference with freedom of communication, even for the purpose of criminal investigation/prosecution, be foreseen by law in advance, that the provisions of the law be known and foreseeable, and that the interference be necessary and proportionate in a democratic society. Furthermore, legal safeguards must be in place to prevent of abuse of this preventive measure.

Since the subject of the preventive measure of interception/ monitoring of communication regulated in Article 135 of the Criminal Procedure Act (CPA) which is include communication "conducted via telecommunications,". It is prima facie considered that communication conducted via the internet or other networks is also within the scope of this preventive measure. However, the CPA and the relevant Regulation do not explain how communications conducted via the internet or other networks can be monitored/ intercepted, nor do they explain the safeguards associated with this monitoring/ intercepting procedure. Furthermore, the Law and Regulation restrictively regulate the monitoring/ intercepting procedure for communications based on communication tools other than those conducted via the internet or other networks.

A review of Articles 135-138 of the CPA reveals many questions, including how and by which authority communications conducted via the internet or other networks can be monitored/ intercepted, whether spyware or cookies or via remote Access can be used in monitoring, whether the communication information of the other party or the device can be intercepted, etc.

To monitor voice or video transmissions through internet-based applications, it is necessary to intercept "data in flow/ movement of data". Such an interception necessitates accessing at least one of the devices connected to the internet or the internal network of the service provider. While it is possible that certain obligations regarding the implementation of measures can be imposed on the service provider by law, particularly when the service provider for the internet or other network is located in Turkey, it is possible that; If they are abroad, such an obligation cannot be imposed on them – without prejudice to the provisions of the Council of Europe Convention on Cybercrime or another conventions.

It should also be noted that communication conducted via internet- based applications can be conducted between two individuals or in groups. In the case of video communication, the image and other elements of private life, in addition to audio can be monitored. In addition to monitoring/ intercepting the communication itself (especially when performed using spyware), the communication device and the information/data on it can be damaged.

For judicial interception of communications conducted via the internet or other networks, the use of spyware or remote access is possible, and information obtained through cookies (especially the username, code, and password related to the communication device, etc.) may also be needed. Therefore, the legal regulations must ensure that such interventions are known and foreseeable to the person subject to the measure and, if necessary, to the person on the other side of the communication.

It is possible to interception of communication via the internet by capturing information about the communication medium through direct remote access or spyware or cookies. Interception of communication via the internet or other networks (intranet, etc.) in this interventions be derived from individual users (natural or legal entities) or from public authorities (national law enforcement or investigative/prosecutory authorities except for exceptions accepted by international conventions) for crime prevention or criminal investigation/ prosecution purposes.

As in the Pegasus software example, it is also possible for state and non-state actors to use spyware to intervene in individuals' communications via the internet or other networks for unlawful purposes. Undoubtedly, firstly, procedural and substantive measures should be taken in the law to prevent such interventions, and secondly, public authorities should implement such interventions. Similarly, it is a separate requirement and obligation for the content or hosting provider providing the communication infrastructure to take measures to prevent unlawful interventions.

In our opinion, just as with the monitoring of communications conducted via the internet or other networks, clear and detailed regulations are needed regarding the implementation of the measures, the manner in which interception, recording, and, if necessary, destruction will be carried out, whether the code or password information of the communication device can be accessed, and whether the other party to the communication (who is not the part of the preventive measure) can remote access information related to the communication device, etc.

Since interception of communication conducted via the internet or other networks may require the seizure or remote access of the computer or mobile phone used for communication, the search, copying, or seizure of these devices or the information system through which the communication is conducted, or simultaneous monitoring/ intercepting with technical means, a comprehensive legal framework is needed to enable the combined application of these measures (as recommended in our study).

GİRİŞ

Günümüzde iletişim, sadece sabit veya mobil telefonlar kullanılarak yapılan bir faaliyet olmaktan çıkmış, özellikle internet yoluyla da yapılır hale gelmiştir. İletişim araçlarının teknolojiyle bağlantısının artması ve daha erişilebilir ve maliyetinin daha az olması (ve suç işleme fikri olan kişiler bakımından da tespitinin ve denetiminin zor

olduğunun düşünülmesi) nedeniyle, internet veya diğer ağlar (intranet[1] vs) marifetiyle yapılan iletişim yoğunlaşmıştır.

Sabit veya mobil telefonlar marifetiyle gerçekleştirilen iletişimin yasal olarak denetimi mümkün ve daha kolay olmakla birlikte, internet kullanılarak gerçekleştirilen iletişimin tespiti ve denetlenmesi ciddi güçlükler barındırmaktadır[2]. Hiç şüphesiz bu güçlükler, kriminal alanda suç işleyen veya suç işleme potansiyeli bulunan kişiler tarafından bir "avantaj" olarak kabul edilmektedir.

Türk hukukunda iletişimin denetlenmesi istihbari (suç önleme) ve adli (suç soruşturma ve kovuşturma) amaçlı olmak üzere iki farklı şekilde düzenlenmiştir. İstihbari amaçlı iletişimin denetlenmesi bir önleyici tedbir olarak Polis Vazife ve Selahiyet Kanunu (PVSK)[3] Ek Madde 7, Jandarma Teşkilat, Görev ve Yetkileri Kanunu (JTGYK)[4] Ek Madde 5 ve Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (MİT Kanunu)[5] m 6'da düzenlenmiştir. Adli amaçlı iletişimin denetlenmesi ise bir koruma tedbiri olarak 5271 sayılı Ceza Muhakemesi Kanunu (CMK)[6] m 135'te düzenlenmiştir[7].

---

1 İntranet, sadece belli bir kuruluş/ organizasyon içindeki bilgisayarları veya yerel ağları ve geniş alan ağlarını birbirine bağlayan TCP/ IP tabanlı (internet tabanı üzerinden işletilen) ağdır. İntranet tabanlı uygulamalarla, tek bir organizasyon veya işletmeye ayrılmış bilgisayarlar arasında oluşturulan ağ üzerinden kurum içi iletişimin yürütülebilmesi mümkündür. Tanımlama için bkz. Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları* (1. Baskı, Legal Yayıncılık, 2013), 26-27.

2 İnternet veya diğer ağlar kullanılarak yapılan ses aktarımının (VoIP- Voice over IP) denetimindeki güçlükler nedeniyle birçok ülkede bu tür iletişimin denetlenmesi yoluyla delil elde etmenin önünde engel bulunduğu ve ülkelerin yasal düzenlemelerini bu engelleri aşacak şekilde "genişlettiği" ifade edilmektedir. Bahri Öztürk, Durmuş Tezcan ve Mustafa Ruhan Erdem (Editörler), *Dijital Ceza Muhakemesi Hukuku* (3. Baskı, Seçkin Yayınevi 2024), 597.

3 Polis Vazife ve Selahiyet Kanunu, Kanun Numarası: 2559, Kabul Tarihi: 04.07.1934, RG 14.07.1934/ 2751.

4 Jandarma Teşkilat, Görev ve Yetkileri Kanunu, Kanun Numarası: 2803, Kabul Tarihi: 10.03.1983, RG 12.03.1983/ 17985.

5 Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, Kanun Numarası: 2937, Kabul Tarihi: 01.11.1983, RG 03.11.1983/18110.

6 Ceza Muhakemesi Kanunu, Kanun Numarası: 5271, Kabul Tarihi: 04.12.2004, RG 17.12.2004/25673.

7 İstihbarat/ suç önleme amacıyla iletişimin denetlenmesi için bkz. Fatih Birtek, 'İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği' (2011) (16) Ceza Hukuku Dergisi 100, 100 vd; Feyzan Olgunsoy, *Terörle Mücadelede İstihbarat Faaliyetlerinin Özgürlükler Rejimine Etkisi (Türkiye, Birleşik Krallık, Amerika Birleşik Devletleri),* (1. Baskı, On İki Levha Yayıncılık 2020) 409 vd; Cavidan Yemez, 'Önleyici Kolluk Faaliyeti Kapsamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi', içinde Fatih

Söz konusu yasal düzenlemeler kapsamında bir değerlendirme yapıldığında denetimin konusunun "telekomünikasyon yoluyla yapılan" iletişim olduğu ve bu iletişim türü içerisine "*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*"[8]nın dahil olduğu anlaşılmaktadır. Bu haliyle iletişimin denetlenmesi tedbirinin, internet tabanlı iletişim de dahil olmak üzere "telekomünikasyon yoluyla yapılan" bütün iletişim biçimlerini "konu bakımından" kapsadığı hususunda herhangi bir tartışma bulunmamaktadır.

Telekomünikasyon kavramı içerisinde yer alan "internet" yoluyla gerçekleştirilen iletişimin denetlenmesinin, yukarıda yer verilen mevzuat hükümleri kapsamında mümkün olduğu açık olmakla birlikte bu denetimin nasıl yapılacağı hususunda açık bir düzenleme bulunmamaktadır.

Sabit veya mobil telefonlar yoluyla yapılan iletişim bakımından kamu otoritelerinin düzenleme ve denetleme yetkileri etkin ve uygulanabilir olduğundan, bu yollarla gerçekleştirilen iletişimin denetlenmesinde teknik açıdan ciddi bir güçlükle karşılaşılmamaktadır. Ancak internet yoluyla akıllı telefonlar veya bilgisayarlar kullanılarak (WhatsApp, facetime vs online/çevrimiçi, kriptolu[9] veya kriptosuz

Birtek (edt), *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)*, (1. Baskı, Adalet Yayınevi 2024), 529.

[8] 10.11.2005 tarih ve 25989 sayılı Resmi Gazete'de yayınlanan 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 Yönetmelik m 3/1-r. (Yönetmelik). Benzer bir tanımlama Adalet Bakanlığı tarafından çıkarılan Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik m 4/1-j'de de yer almaktaydı. Ancak bu Yönetmelik Danıştay 10. Dairesi'nin 09.03.2017 tarih ve E. 2012/1001, K. 2017/1361 sayılı kararı ile CMK'da Adalet Bakanlığı'na bu konuda düzenleme yapma yetkisi verilmediğinden bahisle iptal edilmiştir.

[9] 5809 sayılı Elektronik Haberleşme Kanunu'nun 39. maddesine göre *"telsiz haberleşme sistemleri üzerinden*", kriptolu haberleşme yapma yetkisi Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı'na aittir. Bu kurumlar dışında elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme usul ve esasları belirleme yetkisi Bilgi Teknolojileri ve İletişim Kurumu'na aittir. 39. maddenin ikinci cümlesi, bütün "*elektronik haberleşme*" araçlarını kapsayacak biçimde kaleme alınmıştır. Sözü edilen düzenlemeye aykırılık aynı Kanun'un m 63/6 hükmüne göre suç sayılan bir eylemdir. Bu sebeple, Kanun'un m 3/1-h bendinde tanımlanan bütün elektronik haberleşme sistemleriyle kodlu ve kriptolu haberleşme ancak BTİK tarafından belirlenen usul ve esaslar dahilinde

uygulamalar marifetiyle) gerçekleştirilen iletişim bakımından, kamu otoritelerinin düzenleme ve denetleme yetkileri -bu iletişim türünün mahiyeti ve işleyiş biçimi nedeniyle- çok zayıf olduğundan, bu yolla gerçekleştirilen iletişimin adli veya idari amaçlı olarak denetlenmesinde ciddi teknik (ve bu çalışmada ele alınacağı üzere yasal) güçlüklerle karşılaşılmaktadır.

Özellikle suç aktivitelerini planlı bir şekilde yürüten kapalı suç gruplarının (suç örgütleri vs) suçun soruşturulmasını veya kovuşturulmasını önleyebilmek/ zorlaştırabilmek için internet veya diğer ağlar marifetiyle sunulan (kriptolu veya kriptosuz) iletişim araçlarına yönelmeleri nedeniyle, bu tür suç grupları veya failler bakımından iletişimin denetlenmesine ilişkin mevcut yasal düzenlemelerin veya denetim yöntemlerinin yeterli olup olmadığı ve gelişen teknolojinin gerisinde kalıp kalmadığı, gizli metotların uygulanma biçimleri sürekli olarak tartışılmaktadır[10].

Telefon ve bilgisayara sızan casus yazılımlar (veya internet çerezleri) kullanılmaksızın, uzaktan erişim yapılmaksızın veya çerez kullanılarak elde edilen bilgilerden faydalanılmaksızın, internet tabanlı uygulamalar marifetiyle gerçekleştirilen iletişimin "anlık" olarak denetlenmesi neredeyse imkansızdır. Uzaktan erişim, casus yazılım[11] veya çerez kullanılmak suretiyle iletişime müdahale ise pek çok ciddi sorunu

yapılabilecektir. Bununla birlikte, düşüncemize göre madde internet tabanlı haberleşme sistemlerini kapsamamaktadır. Zira Kanun'un m 3/2 düzenlemesinde, kapsamı belirlenirken "*4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümleri saklıdır*." hükmüne yer verildiğinden, internet yoluyla yapılan haberleşme bakımından 5809 sayılı Kanun'un 39. maddesindeki yasağın uygulanma kabiliyeti bulunmamaktadır. Bkz. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun Numarası: 5651, Kabul Tarihi: 04.05.2007, RG 23.05.2007/26530 ve Elektronik Haberleşme Kanunu, Kanun Numarası: 5809, Kabul Tarihi: 05.11.2008, RG 10.11.2008/ 27050 (Mükerrer).

[10] Avrupa Konseyi'nin Ceza Hukuku Uzmanlı ve Organize Suçların Kriminolojik Görünümleri Komitesi'nin konu hakkındaki raporu için bkz. Fatih Birtek, 'Avrupa Konseyi İletişimin Denetlenmesi ve Gizli İzleme Raporu (En İyi Uygulama Mütalaası 3)' (2011), (94) Türkiye Barolar Birliği Dergisi 393, 393 vd

[11] Casus yazılımlar kullanılmak suretiyle iletişime müdahale sadece ulusal açıdan değil aynı zamanda uluslararası açıdan da tartışmaları beraberinde getirmektedir. Örneğin; İsrail menşeli bir siber güvenlik şirketi olan NSO Group'un ürettiği "Pegasus" isimli casus yazılım yoluyla, pek çok ülkede "elektronik izleme" yapıldığı bilinmektedir. Söz konusu yazılım bir tür "*stratejik bir siber silah*" olarak da tanımlanmaktadır. Haberler için bkz. https://www.aa.com.tr/tr/dunya/israil-yapimi-pegasus-casus-yazilimi-dunyanin-dort-bir-yaninda-kullanildi/2481656; 26 Ağustos 2024; https://www.aa.com.tr/tr/analiz/dunyayi-tehdit-eden-casus-yazilim-pegasus/2314321; 26 Ağustos

beraberinde getirmektedir. Çalışmamızda Türk hukuku bakımından CMK m 135 kapsamında uzaktan erişim, "*casus yazılım*" veya çerez kullanılmak suretiyle adli amaçlı iletişimin denetlenmesinin (dinlemesinin ve kayda alınmasının)[12] mümkün olup olmadığı ve mümkün ise bu denetimin ne şekilde gerçekleştirileceği konusu ele alınacaktır.

I. İLETİŞİMİN DENETLENMESİ KORUMA TEDBİRİNİN KAPSAMI

CMK m 135/1'e göre katalog suçlarla sınırlı olmak üzere şüpheli veya sanığın kullandığı iletişim aracı hakkında "*telekomünikasyon yoluyla yapılan iletişimin denetlenmesi*" koruma tedbiri uygulanabilmektedir. Kanun'da telekomünikasyon kavramına ve kapsamına ilişkin bir ifadeye yer verilmemekle birlikte kavram, 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 Yönetmelik'te (Yönetmelik)[13] tanımlanmıştır.

Yönetmelik'te yer alan tanımlamaya göre telekomünikasyon yoluyla gerçekleştirilen iletişim kavramı içerisine elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri marifetiyle yapılan iletişim de dahildir[14]. Yönetmelik'te "*diğer iletişim sistemleri*" (m3/i) ve "*diğer her türlü iletişim*"

2024. Pegasus hakkında bkz. Pegasus Yazılımı: Telefondaki Casus, https://www.youtube.com/watch?v=EPGfgvrr2q4; 2 Kasım 2025.

[12] Bu yolla gerçekleştirilen "*iletişimin tespiti*", internet trafik verilerinin tespiti/ tutulması anlamına gelmektedir. İnternet trafik verilerinin tutulması hakkında ayrıntılı tartışma için bkz. Fatih Birtek ve Beyza Nur Topal, 'Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti', (2023) (2), GSÜHFD 1137, 1139-1142. Ceza muhakemesinde "*internet trafik verilerine erişim*" (internet trafik verilerinin tespiti) ve bu verilerin ispat kuvveti ayrı bir çalışmanın konusu olduğu için, çalışmanın amacı ve kapsamı da gözetilerek daha detaylı açıklamada bulunulmamıştır. Avrupa Konseyi Siber Suç Sözleşmesi kapsamında "*depolanmış*" ve "*akış halindeki/ gerçek zamanlı*" internet trafik verilerinin tutulması ve bu verilere erişim hususunda bkz. Yavuz Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri (AKSS)* (1. Bası, Legal Yayıncılık 2018) 164, 257.

[13] 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 Yönetmelik, RG 10.11.2005/ 25989. Çalışmamızda kullanılan "Yönetmelik" deyimiyle, bu Yönetmelik kastedilmektedir.

[14] Klasik posta haberleşmesine müdahale CMK m 129 kapsamında "*postada elkoyma*" koruma tedbiri olarak ayrıca düzenlenmiştir. Telekomünikasyon" dışındaki haberleşme araçlarının CMK m.135 dışında olduğu hususunda bkz. Yener Ünver ve Hakan Hakeri, *Sorularla Ceza Muhakemesi Hukuku* (1. Baskı, TBB Yayınları 2006) 171.

(m3/h) denilmek suretiyle, gelecekte ortaya çıkabilecek telekomünikasyon iletişim türleri de kapsama alınmıştır[15]. Bu sebeple CMK m 135 ve Yönetmelik hükümleri kapsamında adli amaçlı iletişimin denetlenmesi koruma tedbiri kapsamındaki iletişim araçlarının "*sınırlı bir şekilde sayılmadığı*" ve internet tabanlı bütün uygulamaların ve programların da bu kapsamda olduğu sonucu ortaya çıkmaktadır. Kanun koyucunun, mevcut ve gelecekte ortaya çıkabilecek bütün iletişim araçlarını kapsama alabilmek amacıyla iletişim araçlarını sınırlamadığı kabul edilmektedir[16].

Nitekim öğretide de internet yoluyla yapılan her türlü iletişimin de CMK m 135 kapsamında olduğu kabul edilmektedir[17]. İnternet ortamında yapılan e- posta

---

[15] Yönetmelikte (m 3/h'de) "*İletişimin dinlenmesi ve kayda alınması: Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri*" karşılayacak şekilde tanımlanmıştır. Bu tanımlamadan, internet yoluyla yapılan her türlü (sözlü veya yazılı) yapılan iletişimin de Yönetmelik kapsamında olduğu sonucu ortaya çıkmakla birlikte, bu yolla gerçekleştirilen iletişimin nasıl denetleneceğine dair herhangi bir usule yer verilmemiştir. Öğretide de Yönetmelik'te geçen "*her türlü iletişim*" ibaresinden hareketle, bilişim sistemlerinin birbirleriyle olan iletişiminin (veri trafiğinin) "uygun teknik araçlarla dinlenmesi ve kayda alınmasının" CMK m 135 kapsamında mümkün olduğu ifade edilmektedir. Görüş için bkz. Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (1. Baskı, Seçkin Yayıncılık 2014) 386. Bununla birlikte, söz konusu görüş kapsamında, "*uygun teknik araçların*" ne olduğu ve bu tür bir denetimin nasıl yapılacağı hususunda herhangi bir tespite yer verilmemiştir.

[16] M. Murat Yardımcı, *Amerika Birleşik Devletleri, Avrupa İnsan Hakları Mahkemesi İçtihatları ve Türk Hukukunda İletişimin Denetlenmesi*, (Yayımlanmamış Doktora Tezi, YÖK Tez Merkezi 2008) 173, 183.

[17] Cumhur Şahin, 'Telekomünikasyon Yoluyla İletişimin Denetlenmesi -Yargıtay Kararları Çerçevesinde Bir Değerlendirme-', (2007) XI, 1-2, Gazi Üniversitesi Hukuk Fakültesi Dergisi 1095, 1099; Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku* (24. Baskı, Adalet Yayınevi 2025), 447; Ersan Şen, *Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir* (4. Baskı, Seçkin Yayıncılık 2010) 82-83; Seydi Kaymaz, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (5. Baskı, Seçkin Yayıncılık 2025) 162; Mustafa Taşkın, *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi* (1. Baskı, Seçkin Yayıncılık 2008) 75-76; Bahri Öztürk, Behiye Eker Kazancı ve Sesim Soyer Güleç, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri* (2. Baskı, Seçkin Yayıncılık 2017) 250; Değirmenci, *Sayısal Delil*, 385; Necati, Meran, *Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Takip* (1. Baskı, Adalet Yayınevi 2009) 43-44; Mustafa Özen, *Ceza Muhakemesi Dersleri* (6. Baskı, Adalet Yayınevi 2021) 569; Juan Carlos Da Silva, Albrecht Stange ve Fatih Birtek, *İletişimin Denetlenmesi Tedbiri*, (1. Baskı, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği- Avrupa Konseyi Ortak Projesi Yayını, MATBAM Ajans 2014) 121-127, 199-200; Kasım Karagöz ve Fatih Birtek 'İnsan Hakları Avrupa Sözleşmesi'nin 8. Maddesi Kapsamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi' (2008) III (2), Erciyes Üniversitesi Hukuk Fakültesi Dergisi 71, 73 vd; Ahmet Gökcen, M. Emin Alşahin ve Kerim Çakır, *Ceza Muhakemesi Hukuku* (8. Baskı, Adalet Yayınevi 2024) 424; Hakan Karakehya, *Ceza Muhakemesi Hukuku* (6. Bası, Adalet Yayınevi 2024) 363; Murat Volkan Dülger ve Şaban Cankat Taşkın, *Ceza Muhakemesi Hukuku* (1. Baskı, Seçkin Yayıncılık 2023) 487. SMS ve e-posta marifetiyle yapılan iletişimin CMK m 135 kapsamında olmadığı hususunda bkz. Uğur Alacakaptan ve Kaan Karcılıoğlu, 'Çağdaş Demokratik Toplumda Özel Hayatın Korunması Bağlamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi' (2012) IX, (2) YÜHFD (Prof. Dr. Duygun Yarsuvat'a Armağan) 35, 46. SMS iletişiminin madde kapsamında olduğu ancak yasa koyucunun bu iletişim

gönderilerinin ve çevrimiçi görüşmelerin bir başka servis sağlayıcı üzerinden denetlenebilmesi mümkündür[18]. Esasında internet tabanlı uygulamalar marifetiyle yapılan yazışmalar (e- posta, mesaj vs) ile sesli ve/veya görüntülü iletişim, bir tür "*akış halindeki veri*"[19] (live stream)[20] olup bunların denetimi de akış halindeki veri trafiğinin -hizmet sunucunun iç ağına veya iletişimin taraflarından birisinin bilgisayar veya telefonuna- girilerek yakalanmasından/ tutulmasından ibarettir.

Öğretideki baskın düşünceye göre telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbiri, geçmişte gerçekleşip tamamlanan iletişim bakımından değil, halen gerçekleşen (aktüel) ve gelecekte gerçekleşecek iletişim bakımından uygulanabilecektir[21]. Geçmişte gerçekleşip tamamlanmış iletişimin denetlenmesi CMK

---

biçimine ilişkin açık bir düzenleme öngörmesi gerektiği hususunda bkz. Şen, Telefon Dinleme (n 17) 82. Düşüncemize göre internet tabanlı ve diğer ağlar marifetiyle gerçekleştirilen bütün iletişim (e posta, mesaj, sesli ve/veya görüntülü görüşme vs) CMK m 135 kapsamındadır.

[18] Şen, Telefon Dinleme (n 17) 83. Ünver ve Hakeri'ye göre sms veya e- mail iletişimi "geleceğe" yönelik olarak denetlenecekse CMK m 135 kapsamında, "geçmişteki" kayıtlara erişilmek isteniyorsa CMK m 134 kapsamındadır. Açıklama için bkz. Ünver ve Hakeri, Ceza Muhakemesi Hukuku (n 17) 448. Aynı yönde bkz. Değirmenci, Sayısal Delil (n 15) 333; Dülger ve Taşkın, (n 17) 487. Dülger ve Taşkın'a göre somut olayın özelliğine göre her iki tedbire (CMK m 134 ve 135) birbirini izleyecek veya kombine şekilde karar verilmesi suretiyle delil elde etme işlemi hukuka uygun ve sonuç elde etmeye elverişli olarak uygulanabilecektir. Ibid 487. Meran'a göre ise cep telefonları marifetiyle yapılan mesajlaşmaların ve bilgisayar tabanlı görüşmelerin, denetlenip denetlenemeyeceği hususunda açık bir yasal düzenleme bulunmamaktadır. Açıklama için bkz. Meran (n 17) 55.

[19] Kavram hakkında bkz. Değirmenci, Sayısal Delil (n 15) 385; Erdoğan, AKSS (n 17) 257.

[20] Dülger ve Taşkın (n 17) 487.

[21] Yargıtay da aynı görüştedir. Yargıtay'a göre "*Bilgisayarlarda, bilgisayar programları, bilgisayar kütükleri veya diğer araçlarda yapılacak aramanın konusu "elektronik veri"dir. Bu araçlarda arama işleminde amaç suçla bağlantılı her türlü elektronik veriye ulaşmaktır. Bu kapsamda bilgisayardaki mevcut klasördeki dokümanların tümü taranabilir. Bilgisayarda, 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. maddesine göre değil CMK'nın 134. maddesine göre yapılabilir. Zira CMK'nın 135. maddesinde düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbiri, teknik araçlarla iletişimin tespitini, dinlenmesini ve kayda alınmasını kapsamaktadır. CMK'nın 135. maddesine göre yapılan iletişimin dinlenmesi ve kaydı, geçmişe dönük olarak değil geleceğe dönük olarak yapılabilir. Diğer bir ifadeyle geçmişte gerçekleşen iletişimin dinlenebilmesi, kayda alınabilmesi mümkün değildir. Ancak internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından bu iletişim kayıtları hakkında CMK'nın 134. maddesindeki koruma tedbiri kapsamında arama, kopyalama ve elkoyma tedbirleri uygulanabilir. Bireyin e-posta, yazışma ve haberleşmeleri CMK'nın 135. maddesi kapsamında değerlendirilirken, bireyin kendisine e-posta ile gelen bir yazı, resim, görüntü veya ek dosyayı kullandığı bilgisayara veya taşınır belleğe kaydettiğinde, artık bu belge haberleşme hürriyetinin dolayısıyla iletişimin denetlenmesinden çıkıp CMK'nın 134. maddesi kapsamında bilişim cihazına kayıtlı bilgi ve belgeye dönüşecektir. Kriptolu haberleşme sonucunda silinmiş mesajların gerek bilgisayarda gerekse sistem üzerinde ele geçirilmesi de telekomünikasyon yoluyla yapılan iletişim denetimi kapsamında olmayıp bu gibi hallerde CMK'nın 134. maddesinde*

m 160-161 kapsamında genel suç soruşturma yetkisi içerisinde veya m 134 bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri kapsamında değerlendirilmektedir[22].

AİHM uygulamasında da telekomünikasyon yoluyla yapılan iletişim, "araç" bakımından sınırlandırılmamış ve bu husus ülkelerin iç hukukuna bırakılmıştır[23].

Düşüncemize göre de CMK m 135'te yer alan düzenleme nazara alındığında internet tabanlı uygulamalar marifetiyle yapılan iletişimin denetlenmesinin konu itibariyle telekomünikasyon yoluyla iletişimin denetlenmesi kapsamında olduğu hususunda bir tereddüt bulunmamaktadır. Bununla birlikte, internet veya diğer ağlar (kurum içi ağlar/ intranet vs) marifetiyle gerçekleştirilen iletişimin CMK m 135'e istinaden "casus yazılım" veya "cookie (çerez)" yüklenmek suretiyle denetlenip

düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri söz konusu olabilir." Yargıtay CGK, 495/116, 17.03.2021, Aynı yönde bkz. "*15/01/2020 tarihli ifade tutanağına 'özet' halinde geçirilen whatsapp mesajlaşma kayıtlarının, CMK'nın 134. maddesi kapsamında görüşme tarihleri, saatleri belirtilerek, ayrıntılı diyaloglar şeklinde, ekran görüntülerine de yer verilerek denetime olanak verecek şekilde tutanağa bağlanması, bu şekilde düzenlemiş bir tutanak mevcut ise aslı ve denetime olanak verecek şekilde onaylı suretinin dosyaya konulması…*" Yargıtay 10 CD, 2849/5922. 24.05.2021. (*Bu çalışmada yararlanılan yargı kararlarına -aksi belirtilmedikçe Kazancı İçtihat Bilgi Bankası'ndan erişilmiştir*).

[22] İletişim "bitmiş/ sona ermiş" ise buna dair kayıtlara erişilmesi CMK m 160-161 kapsamındadır. Görüş için bkz. Ünver ve Hakeri, Ceza Muhakemesi Hukuku (n 17) 447. Belleğe kaydolan, canlı bir görüşme olsa da anlık tespit edilmeyip iletişimin yapıldığı aygıtın belleğinde saklanan her türlü dijital verilerin CMK m 134 uyarınca, bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri kapsamında olduğu hususunda bkz. Değirmenci, Sayısal Delil (n 15) 333; Dülger ve Taşkın (n 17) 487. Aksi düşünceye göre ise "*maddi gerçeğe (delile ve şüpheliye) ulaşabilmek amacıyla soruşturma ve kovuşturma makamlarına tanınan genel yetkiye (CMK m 160-161) dayanılarak koruma tedbirleri uygulanamayacağından -koruma tedbirlerine eş değer ağırlıktaki- müdahalelerde bulunulamaz*": Fatih Birtek, 'Ceza Muhakemesinde Tanık Hakkında İletişimin Tespiti Koruma Tedbirine Başvurulup Başvurulamayacağı Sorunu', (2022) 17 (49), Ceza Hukuku Dergisi 189, 205. Yargıtay'a göre ise şüpheli sıfatının belirlenebilmesi amacıyla (düşüncemize göre bir tür otomatik veri tarama işlemi yapılarak) yapılan ve belli bir şüpheli için değil de belli bir "numara/ hat" esas alınarak yapılan "iletişimin tespiti" işlemi CMK m 160, 161 kapsamında Cumhuriyet savcısının suç soruşturmasına ilişkin genel yetkisi içerisinde kabul edilmelidir. "*İçeriğine müdahale edilmeden, iletişim araçlarının diğerleri ile kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespitine yönelik işlem olması ve daha çok dış bağlantı verilerini ifade etmesi nedeniyle "iletişimin tespiti", Cumhuriyet savcısının soruşturma yetkisini düzenleyen CMK'nın 160 ve 161. maddeleri kapsamında istenebilecek delillerdendir. Cumhuriyet savcısı soruşturmanın ayıklayıcılık ve kişilerin lekelenmeme hakkı ilkelerini dikkate alarak delil toplarken Anayasa'da ve yasada düzenlenen "orantılılık" ilkesini göz önüne almak durumundadır. İletişimin tespitinin istenmesi her zaman aleyhe sonuç doğurmaz. Bazen suça katılmayan kişilerin erkenden tespiti ile haklarında başkaca ceza muhakemesi tedbirine başvurmama imkânını da sağlayabilir."* Yargıtay CGK, 495/116, 17.03.2021.

[23] Öztürk, Eker Kazancı ve Soyer Güleç (n 17) 252.

denetlenemeyeceği, denetlenebilecekse denetimin nasıl yapılacağının tartışılması gerekmektedir. Konu aşağıda ayrı başlık altında ayrıca tartışılacağından burada daha fazla açıklamaya yer verilmemiştir.

II. İLETİŞİMİN DENETLENMESİ KORUMA TEDBİRİNİN UYGULANMA USULÜ

İletişimin denetlenmesi koruma tedbirinin uygulanma usulü tedbirin kapsamında yer alan iletişim aracına göre değişebilmektedir.

Sabit veya mobil iletişim araçları bakımından, soruşturma veya kovuşturma aşamasında verilen iletişimin denetlenmesine (dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine) dair karar (veya emir), işletmecilere gönderilmeksizin (Yönetmelik m 14) Bilgi Teknolojileri ve İletişim Kurumu'nun (BTİK'nin) koordinasyonunda yerine getirilmektedir.

Elektronik Haberleşme Kanunu m 12/5 hükmüne göre elektronik haberleşme sektöründe faaliyet gösteren işletmeciler "*elektronik haberleşme sistemleri üzerinden millî güvenlikle ve 5397 ve 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlüdür*". İşletmeciler tarafından kurulan bu altyapı marifetiyle -işletmecilerin bilgisi ve müdahalesi olmaksızın ve gizlilik içerisinde- BTİK'nin koordinasyonunda iletişimin denetlenmesi tedbiri uygulanabilmektedir.

İnternet tabanlı uygulamalarda gerçekleştirilen iletişim bakımından; BTİK'nin koordinasyon sağlayabilmesi ve bu tür bir yapı kurularak işlemlerin tek merkezden koordine edilebilmesi mümkün değildir[24]. Zira internetin doğası gereği ulus ötesi oluşu,

[24] İnternet tabanlı uygulamalar marifetiyle gerçekleştirilen iletişimin denetlenmesi bakımından CMK m 135 kapsamında "dinleme ve kayda alma" tedbirlerinin uygulanması mümkün iken; sinyal bilgilerinin değerlendirilebilmesi tedbirinin uygulanabilmesi mümkün değildir. Çünkü sinyal bilgilerinin değerlendirilmesi daha çok mobil cihazlar bakımından uygulanabilir bir tedbirdir. İnternet tabanlı uygulamalar marifetiyle gerçekleştirilen iletişim bakımından sinyal bilgilerinin değerlendirilmesi yerine "*internet trafik verilerinin*" değerlendirilmesinden ve kullanıcıların internet trafik verilerinin karşılaştırılmasından söz edilebilir. İnternet trafik verileri hakkında açıklama için bkz. Birtek ve Topal (n 12) 1139 vd İnternet trafik verilerine suç önleme amacıyla müdahale konusunda bkz. Fatih Birtek, 'Suç İşlenmesini Önleme Amacıyla İnternet veri Trafiğinin (İnternet Trafik Bilgilerinin) Tespiti', içinde

yer sağlayıcının veya erişim sağlayıcının yurt dışında olduğu hallerde telekomünikasyon yoluyla yapılan iletişimin denetlenmesinde olduğu gibi "yerel/ ulusal bir idari otorite aracılığıyla" iletişimin denetlenebilmesine imkan yoktur. Yine erişim ve yer sağlayıcılar[25] açısından bakıldığında da yer sağladığı internet kullanıcılarının sayısı ve erişim sağlanan aracın sayıca çokluğu dikkate alındığında, ulusal bir idari otorite marifetiyle yer sağlayıcılara internet aracılığıyla gerçekleştirilen iletişimin denetlenebilmesi için yükümlülük öngörmek de çok güçtür[26]. Kaldı ki; internet erişim sağlayıcının hizmet sunduğu kullanıcının internet marifetiyle gerçekleştirdiği iletişime anlık olarak müdahale ederek (herhangi bir casus yazılım veya çerez kullanmaksızın) sadece izleme yaparak müdahale edebilmesi ve adli mercilere denetim imkânı sunabilmesi de teknik olarak pek çok imkansızlığı beraberinde getirmektedir. Hiç şüphesiz yer sağlayıcının yurt dışında olduğu hallerde bu imkansızlığın daha belirgin olacağı kaçınılmaz bir sonuçtur.

CMK ve Yönetmelik kapsamında, internet tabanlı uygulama ve programların telekomünikasyon yoluyla yapılan iletişimin denetlenmesi koruma tedbiri kapsamında olduğu açık olsa da internet yoluyla online/çevrimiçi gerçekleştirilen iletişimin ne şekilde denetleneceği konusunda herhangi bir düzenlemeye yer verilmemiştir.

CMK m 135 metni incelendiğinde (özellikle m 135/4), koruma tedbirinin uygulanmasına ilişkin kararda "*iletişim aracının türü…iletişim bağlantısının tespitine imkan veren kodu"* gibi bilgilerin bulunması gerektiğinden hareketle, kanun koyucunun sadece sabit veya mobil telefon ile değil aynı zamanda internet veya diğer ağlar (intranet

---

Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı Adalet Yayınevi 2024) 663 vd

[25] 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a göre (2/1-e,f,m); "*erişim sağlayıcı*", Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü ger-çek veya tüzel kişi; "*yer sağlayıcı*", hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişi; "*içerik sağlayıcı*" ise internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişidir.

[26] 5651 sayılı Kanun'da (Ek Madde 4), yurt dışındaki sosyal ağ sağlayıcılar bakımından, temsilci atamama, aynı maddenin 5. fıkrasında sayılan suçlarla sınırlı olarak internet içeriklerini oluşturan veya yayan faillere ulaşmak için gerekli olan bilgiler soruşturma aşamasında Cumhuriyet savcısı, kovuşturma aşamasında yargılamanın yürütüldüğü mahkemeye vermeme ve içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğinin yerine getirmeme hallerinde "idari para cezası" ve "*bant genişliğinin daraltılması*" gibi idari tedbirler uygulanabilmektedir. Bu istisna dışında, yurt dışında bulunan yer veya içerik sağlayıcısı bakımından herhangi bir yükümlülük bulunmamaktadır.

vs)[27] marifetiyle gerçekleşen iletişimin denetlenebilmesine ilişkin koşulları da düzenlendiği kabul edilse de bu tür araçlar bakımından denetimin ne şekilde gerçekleştirileceği açık ve ayrıntılı bir şekilde düzenlenmemiştir.

Özellikle, yer sağlayıcısı yurt dışında olan internet uygulamaları (WhatsApp, facetime vs) bakımından bu tür bir denetimin ne şekilde gerçekleştirileceğine dair bir usule yer verilmemiştir. İletişimin denetlenmesine ilişkin kararın yerine getirilmesini düzenleyen m 137/1'e bakıldığında ise tedbirin, "*telekomünikasyon hizmeti veren kurum ve kuruluşların yetkilileri*" marifetiyle uygulanabileceği düzenlenmiştir[28].

Yine Yönetmelik hükümlerine (m 12-15) bakıldığında tedbirin uygulamasına ilişkin kuralların sabit veya mobil telefonlar marifetiyle gerçekleştirilen iletişime ilişkin bir usulü düzenlediği, internet veya diğer ağlar (intranet) marifetiyle gerçekleştirilen iletişimin denetlenmesine dair herhangi bir kurala yer verilmediği görülmektedir. Bu bağlamda, CMK m 135 düzenlemesinin internet veya diğer ağlar (intranet vs) marifetiyle gerçekleştirilen iletişimin denetlenmesini kapsadığı ancak bu uygulamalar marifetiyle gerçekleştirilen iletişimin denetlenmesine dair herhangi bir usulün veya uygulama biçiminin mevzuatta açık bir şekilde düzenlenmediği anlaşılmaktadır[29].

---

[27] AİHM, kurum içerisindeki (dahili) telefon hattına yapılan müdahalenin özel hayatın gizliliğine saygı hakkı kapsamında kabul etmekte ve bu tür müdahaleleri de AİHS m8 kapsamında değerlendirmektedir. Fatih Birtek, 'Özel Hayata Saygı- İhlal Kararı, Halford/ Birleşik Krallık Kararı' (2009) (40) Terazi Hukuk Dergisi 165, 165 vd Bu sebeple internet dışındaki bir ağ üzerinden (örneğin kurumsal iletişim sistemleri veya kurum/ ülke içindeki ağlar) gerçekleştirilen iletişimin de telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri kapsamında ele alınması gerekmektedir.

[28] CMK m 135'te düzenlenen koruma tedbirinin uygulanmasında koordinasyonu sağlamak üzere 2005 yılında 2559 sayılı PVSK'ye 5397 sayılı Kanun ile eklenen düzenleme ile (Ek madde 7) kurulan ve 2006 yılında faaliyete başlayan Telekomünikasyon İletişim Başkanlığı (TİB), 15.08.2016 tarih ve 671 sayılı Olağanüstü Hal Kanun Hükmünde Kararnamesi'nin 22. maddesiyle kapatılmış ve görevleri BTİK'ye devredilmiştir. Mezkûr KHK, 09.11.2016 tarih ve 6757 sayılı Kanun ile aynen kabul edilerek kanunlaşmıştır. Düşüncemize göre eski uygulamada TİB (Telekomünikasyon İletişim Başkanlığı) yeni uygulamada da BTİK'nin telekomünikasyon yoluyla yapılan iletişimin denetlenmesi koruma tedbirinin uygulanması altyapısını sağlayan ve uygulamayı denetleyen bir birim olarak görevlendirilmesiyle birlikte CMK m 137/1'in fiilen uygulanamayan "metruk" bir norm haline geldiği söylenebilir. BTİK, tedbiri uygulayan değil "*uygulanmasında koordinasyonu sağlayan*" bir birim olup tedbirin fiilen uygulanması, tedbire karar veren adli merciin bulunduğu yerdeki kolluk tarafından gerçekleştirilmektedir. BTİK tarafından yapılan işlem iletişim hizmetini sunan işletmeci ile adli merciler arasında bağlantı kurma ya da teknik adıyla "*uç verme*" işlemidir.

[29] Tarafımızdan yapılan araştırmada da uygulamada internet veya diğer ağlar (intranet vs) marifetiyle gerçekleştirilen haberleşmenin CMK m 135 kapsamında denetlendiği bir örneğe (yargı kararına vs) rastlanılmamıştır.

Temel hak ve hürriyetler açısından bakıldığında; bir hakka yönelik müdahalenin "*kanunilik*", "*meşru amaç*", "*demokratik toplumda gereklilik* ve "*ölçülülük*" kriterlerini taşıması gerektiği tartışmasızdır[30].

İncelediğimiz konu bakımından -CMK'de ve Yönetmelik'te internet veya diğer ağlar (intranet vs) marifetiyle gerçekleştirilen iletişimin denetlenme usulüne dair bir düzenleme bulunmadığından- "kanunilik" ölçütünün "öncelikle" ve ayrıca ele alınması gerekmektedir. Zira AİHS m 8 metni ve AİHM uygulaması bir bütün olarak değerlendirildiğinde, bireysel iletişim/ haberleşme hürriyetine yapılacak bir müdahalenin meşruluğu, "*öncelikle söz konusu müdahalenin yasaya uygun bir şekilde gerçekleştirilmesine bağlıdır*"[31].

Koruma tedbirleri bakımından "kanunilik" ilkesi (tedbirin uygulanmasına imkân veren bir kanuni dayanağın bulunması) ortak bir özellik ve zorunluluk olup[32] Anayasa'nın 13. maddesi uyarınca temel hak ve hürriyetler ancak "kanun" ile sınırlandırılabileceğinden, suç soruşturması/ kovuşturması amacıyla dahi olsa temel hak

[30] Anayasa Mahkemesi'nin uygulamasına göre bir temel hakka ilişkin müdahale Anayasa'da ilgili maddede yer verilen "*haklı sebeplerden bir veya daha fazlasına dayanmadığı ve Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe*" Anayasa'ya aykırı kabul edilmelidir. Anayasa Mahkemesi [GK], 2013/1461, 12.11.2014, par 80. Anayasa Mahkemesi, bireysel başvurular bakımından hak ihlalinin bulunup bulunmadığının tespitinde, "*kanunilik*", "*meşru amaç*" ve "*demokratik toplumda gereklilik ve ölçülülük*" biçiminde bir "anayasaya uygunluk testi" uygulamaktadır. Çalışmamızın odaklandığı asıl konu nazara alınarak sadece "kanunilik" ölçütü bağlamında değerlendirmelerde bulunulacaktır.

[31] AYM, 2013/299, 4.2.2016, par 57. AİHM uygulamasına göre Sözleşme'nin 8. maddesindeki özel hayatın gizliliğine saygı hakkında müdahale teşkil eden bir tedbir, kanunla düzenlenmemişse Sözleşme'nin 8. maddesinin 2. fıkrasında yer alan diğer güvence ölçütlerinin mevcut olup olmadığı araştırılmaksızın müdahalenin Sözleşme'ye aykırı olduğu kabul edilmektedir. Aynı yönde bkz. Y.F. vs Türkiye, (2003), par 44. 44. Koruma tedbirlerinde kanunilik ilkesinin esas olması (koruma tedbirlerinin kanunla düzenlenmesinin zorunlu olması) nedeniyle, her ne kadar ceza muhakemesinde kıyas serbestisi temel bir ilke olsa da koruma tedbirlerine ilişkin kanuni düzenlemelerde kıyas yasağının geçerli olduğu hususunda bkz. Ünver ve Hakeri, Ceza Muhakemesi Hukuku (n 17) 74. Yargıtay'a göre de " *Ceza muhakemesinde kıyas ve her türlü yorum mümkün olmakla birlikte, temel hak ve özgürlükleri daraltan normlar ile istisnai normlarda kıyas yasağı mevcuttur. Kanun koyucunun düzenlediğinin aksine sonuçlara ulaşmaya izin verecek şekilde, kıyas veya yorum yoluyla temel hak ve özgürlüklere ilişkin normları daraltıcı, istisnai normları genişletici şekilde hareket etmek mümkün değildir*." Yargıtay CGK, 12-205/36, 22.01.2025.

[32] Öztürk, Eker Kazancı ve Soyer Güleç, (n 17) 24-25.

ve hürriyetlere yapılacak müdahalenin öncelikle kanuni bir dayanağının bulunması gerekmektedir[33].

AİHM'e göre gizli uygulanan koruma tedbirlerinde kötüye kullanım (ve keyfi uygulama) riski her zaman söz konusu olabileceğinden, gizli tedbirin uygulanmasına imkan veren kanunun; *izleme kararı verilmesine yol açabilecek suçların niteliğini, iletişimleri izlenecek kişi kategorisini, izleme sürelerinin sınırlarını, elde edilen verilerin inceleme, değerlendirme ve saklanmalarına ilişkin esasları, verilerin başkalarıyla paylaşılmasına ilişkin önlemler ve elde edilen verilerin ortadan kaldırılmasına ilişkin koşulları* açık bir şeklide düzenlemesi gerekmektedir[34]. AİHM, iç hukuktaki bir müdahalenin Sözleşme'yi ihlal edip etmediğini değerlendirirken ilk olarak iç hukukta kanuni/ hukuki bir dayanağının bulunup bulunmadığını dikkate almaktadır[35].

Anayasa Mahkemesi'ne göre "*Posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetlerinin, haberleşme özgürlüğü ve haberleşmenin gizliliği kapsamında değerlendirilmesi gerekir. Kamu makamlarının, bireyin haberleşme özgürlüğüne ve haberleşmesinin gizliliğine keyfi bir şekilde müdahale etmelerinin önlenmesi, Anayasa ve Sözleşme ile sağlanan güvenceler kapsamında yer almaktadır. Haberleşmenin içeriğinin denetlenmesi, haberleşmenin gizliliğine ve dolayısıyla haberleşme özgürlüğüne yönelik ağır bir müdahale oluşturur. Telekomünikasyon yoluyla iletişimin dinlenmesi ve kayda alınması da bu kapsamdaki müdahalelerdir.*"[36] "*Hak ve özgürlüklerin yasayla sınırlanması ölçütü anayasa hukukunda önemli bir yere sahiptir.*

---

[33] Wieser and Bicos Beteiligungen GmbH vs Avusturya, (2008) par 54.

[34] AİHM'nin The Association For European Integration And Human Rights ve Ekimdzhiev vs Bulgaristan (2007) par 76-77. Karara ilişkin değerlendirme için bkz. AYM, Yasemin Çongar ve diğerleri [GK], 2013/7054, 6.1.2015, par 60.

[35] Avrupa Birliği ülkelerinde bilgisayar korsanlığı yöntemleri kullanılarak iletişim araçlarına (delil elde etme amacıyla) müdahale yetkisine ilişkin olarak ülke bazında değerlendirme ve bu konuda genel bir yasağın bulunmadığı hususunda bkz. Avrupa Parlamentosu İç Politikalar Genel Direktörlüğü (C Departmanı), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Mart 2017, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf 7 Kasım 2025.

[36] AYM, Yasemin Çongar ve diğerleri [GK], 2013/7054, 6.1.2015, par 50. AYM'ye göre "*Gizli uygulanmaları nedeniyle kötüye kullanılma riski barındıran, haberleşmenin gizliliğine yönelen tedbirlerin, uygulama alanı ve prosedürünün çok açık kanun hükümleri ile düzenlenmesi şarttır*" (par 59).

Hak ya da özgürlüğe bir müdahale söz olduğunda öncelikle tespiti gereken husus, müdahaleye yetki veren bir kanun hükmünün, yani müdahalenin hukuki bir temelinin mevcut olup olmadığıdır."[37]

Anayasa Mahkemesi'nin uygulamasına göre "kanunilik" şartının sağlandığının kabul edilebilmesi için kanunun bizatihi "şeklen" varlığı yeterli olmayıp; nitelik itibariyle "*sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini*" göstermesi gerekmektedir Bu yolla kanun, "*uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta, bu yönüyle hukuk güvenliği güvencesi sağlamaktadır*"[38].

Gerek AİHM gerekse AYM tarafından, CMK'de düzenlenen "*telefon görüşmelerinin dinlenmesine"*[39] yönelik olarak açık ve detaylı kuralların konulduğu ve kamu makamlarının takdir yetkisinin kapsam ve sınırlarının net bir şekilde çizildiği nazara alınarak "*müdahalenin dayanağı olan kanun ve yönetmelik hükümlerinin, haberleşme hürriyeti ve haberleşmenin gizliliğine yönelen müdahalelerin sınırlarını yeterli açıklıkta ortaya koyan, erişilebilir ve öngörülebilir nitelikte düzenlemeler olduğu*" kabul edilmiştir[40].

Yargıtay'a göre de[41] "*Ceza muhakemesi önlemlerinin temel haklara müdahale niteliğinde olduğu ve temel haklara müdahalenin de ancak kanuni bir düzenleme bulunduğu takdirde hukuka uygun sayılabileceği, bu nedenle koruma tedbirlerinin mutlaka bir kanun hükmü ile düzenlenmesi gerektiği, Avrupa İnsan Hakları Mahkemesinin de bir koruma tedbiri uygulanarak, temel bir hakka müdahalenin, öncelikle ulusal hukukta bir dayanağı olmadığı sürece hukuka uygun olarak kabul edilemeyeceğini kararlarında sıklıkla vurguladığı, bu açıdan bakıldığında*

[37] AYM, Sevim Akat Eşki, 2013/2187, 19.12.2013, par 36.

[38] AYM, Hilmi Yıldız, 2013/299, 4.2.2016, par 58.

[39] Anılan yüksek mahkemelerin bu kabulünün "telefon görüşmeleri" bakımından geçerli olduğu, internet veya diğer ağlar (intranet vs) marifetiyle yapılan iletişime ilişkin bir değerlendirmeyi içermediği de ayrıca belirtilmelidir.

[40] AİHM, Gülmez/Türkiye, 16330/02, 20.5.2008, par 51; AYM, Hilmi Yıldız, 2013/299, 4.2.2.2016, par 65.

[41] Yargıtay 5 CD, 16791/516, 17.01.2014.

CMK'nın 135 ve 140. maddelerinde düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması ile teknik araçlarla izleme [bakımından] bu koşulun hukukumuzda mevcut olduğu" kabul edilmektedir.

Kanunilik kriteri bakımından bir değerlendirme yapıldığında; CMK m 135'te yer alan düzenlemenin bütün telekomünikasyon araçlarını (ve internet tabanlı uygulamaları) kapsadığı ve bu yönüyle bireylerin, iletişim özgürlüklerine ve özel yaşamlarına yönelik müdahaleyi "öngörebilecekleri" ve "bilebilecekleri" söylenebilir. Lakin, CMK m 135'te yer alan düzenlemede, iletişimin denetlenmesi tedbirinin internet tabanlı uygulamalarla gerçekleştirilen iletişim bakımından nasıl uygulanacağına dair bir hüküm bulunmadığından (ve Yönetmelik'te de bu şekilde bir düzenlemeye yer verilmediğinden), internet veya diğer ağlar (intranet) marifetiyle gerçekleştirilen iletişimin uzaktan erişim veya casus yazılımlar ya da çerez kullanılarak denetlenebileceğinin bu yolla iletişim kuran kişilerce (tedbirin muhatabı olması muhtemel kişilerce) bilinebilir veya öngörülebilir olduğu söylenemez.

Belirtmek gerekir ki; AİHM uygulamasına göre iç hukukta bir temel hakka ilişkin müdahaleye imkân sağlayan ve yeterli güvenceleri içeren bir kanuni dayanağın mevcut olması halinde, bu koruma tedbirinin kapsamında değerlendirilebilecek müdahaleler bakımından (örneğin; aramaya ilişkin yasal ve yeterli güvencelerin bulunması halinde, elektronik verilerin aranmasına ve elektronik verilere el konulmasına yönelik müdahalelerde)[42] ayrı ve özel bir yasal düzenleme yapılması gerekli/ zorunlu değildir. İç hukuk uygulamasında mahkemelerin, genel mahiyetteki güvenceleri koruma tedbirinin kapsamına dahil edilen diğer müdahaleler bakımından da geçerli kabul etmesi yeterli ve uygun bir güvence oluşturmaktadır[43].

Her ne kadar CMK m 135'te yer alan "telekomünikasyon" kavramı ve Yönetmelik'te yer alan "*diğer iletişim sistemleri*" (m3/i) ve "*diğer her türlü iletişim*"

[42] Elektronik verilerin, genel mahiyetteki arama ve elkoyma içerisinde ele alınmasının koruma tedbirlerinde geçerli olan kıyas yasağına aykırı olduğu hususunda bkz. Ünver ve Hakeri, (n 17) 335. Bu tür bir uygulamanın "*genişletici yorum*" olarak kabul edilmesi gerektiği hususunda bkz. Olgun Değirmenci, Sayısal Delil (n 15) 80, dn 35. Bununla birlikte Değirmenci'nin bizim de katıldığımız düşüncesine göre bilgisayar sistemlerinde arama, kopyalama ve elkoyma tedbirinin bir koruma tedbiri olarak kanunda açık bir şekilde düzenlenmesi gerekmektedir. Açıklama için bkz. Ibid, 82.

[43] AİHM, Wieser and Bicos Beteiligungen GmbH vs Avusturya, (2008) par 54.

(m3/h) kavramları internet veya diğer ağlar marifetiyle gerçekleştirilen iletişimin denetlenebilmesine imkan tanısa da Kanun ve Yönetmelik (kabul edildikleri zamanda yaygın olarak kullanılan iletişim aracı olmaları nedeniyle), temelde sabit veya mobil telefonlar marifetiyle yürütülen iletişimin denetlenmesini esas alarak hazırlanmıştır. Bu sebeple ne Kanun'da ne de Yönetmelik'te bu denetimin nasıl yapılacağı, iletişimin tarafı olmayan kişilere olan etkisinin *ne olacağı ve bu kişilerin haberleşme hürriyetine ilişkin güvencelerin neler olduğu, elde edilen verilerin inceleme, değerlendirme ve saklanmalarına ilişkin esasların neler olduğu,* açık bir şeklide düzenlenmemiştir.

İnternet tabanlı uygulamalar marifetiyle gerçekleştirilen iletişimin, iki kişi arasında yapılabileceği gibi çoklu (grup) olarak da yapılabileceği, görüntülü iletişim yapılması halinde ses dışında görüntünün ve sair özel hayat unsurlarının da denetime tabi tutulabileceği, iletişimin denetlenmesi dışında (özellikle casus yazılım kullanılarak denetim yapıldığında) iletişim aracına ve araçtaki bilgilere/ verilere zarar verilebileceği nazar alındığında, bu tür bir erişime ilişkin kötüye kullanımı engelleyen güvencelerin neler olduğu açık bir şekilde düzenlenmeksizin, CMK m 135 vd. hükümleriyle Yönetmelik'teki düzenlemelerin iletişim özgürlüğünün korunmasına ilişkin uygun ve yeterli güvence teşkil ettiği söylenemez. Bu yönüyle, internet tabanlı uygulamalarla gerçekleştirilen iletişimin denetlenmesi bakımından CMK m 135 vd. ve Yönetmelik hükümlerinin (AİHM'nin yukarıda yer verilen karar ve uygulamasında belirtildiği şekliyle) "*sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini*" gösteren ve "*uygulayıcının keyfi davranışlarının önüne geçen, kişinin hukuku bilmesine de yardımcı olan ve hukuk güvenliği güvencesini sağlayan"* nitelikte olduğu söylenemez.

III. CASUS YAZILIM (SPYWARE) VEYA ÇEREZ (COOKIE) KULLANILMAK SURETİYLE İNTERNET İLETİŞİMİNE MÜDAHALE

A. Casus Yazılım ve Çerez Kavramları

Kötücül yazılımlar, "*bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış*" yazılımların genel adı olup, bu tür yazılımlar çoğu kez kullanıcının haberi olmadan veya

kullanıcıyı yanıltmak suretiyle (yetkisiz bir şekilde bilişim sistemine dahil olarak) bulaşmaktadır[44].

Casus yazılım (spyware), casus (spy) ve kötü amaçlı yazılım (malicious software) kelimelerinden türetilmiş bir kavramdır. Casus yazılımlar, en genel kötücül yazılımlardan birisidir[45]. Casus yazılımlar, "kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan" yazılımlardır[46].

Bu yazılımların amacı, kurban/ hedef olarak seçilen bilişim sistemi üzerinde gizli kalarak, istenilen bilgileri toplamak olup bu tür yazılımlar kendi kopyalarını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar, bu sebeple de bu tür yazılımların tespiti virüs ve solucanlara kıyasla daha zordur[47]. Casus yazılımlarla ancak karşı casus yazılımlar (anti spyware) kullanılarak baş edilebilir[48]. Casus yazılımlar kullanılarak, ortam dinleme, telefon dinleme, mesaj bildirimi, arama bildirimi, SIM bildirimi ve yer bilgisi gibi pek çok bilgi elde edilebilir[49].

Cookie (çerez), internet sitelerinin daha kullanışlı hizmet verebilmesi için kullanıcı bilgilerini, şifrelerini, internet kullanımıyla ilgili bütün tercihleri toplayan/

---

44 Gürol Canbek ve Şeref Sağıroğlu, 'Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma', (2013) 22 (1) Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi 121, 121; Gürol Canbek, *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme* (Yayımlanmamış Yüksek Lisans Tezi YÖK Tez Merkezi 2005) 13, 31-32, 43, 50, 58, 154; Mehmet Emin Arslan 'Siber Güvenlik ve Siber Saldırı Türleri', (academia, 2 Kasım 2025), 7. https://www.academia.edu/31827545 2 Kasım 2025.

45 Canbek ve Sağıroğlu (n 44) 122.

46 Ibid 125.

47 Arslan (n 44) 7; Canbek ve Sağıroğlu (n 44) 125.

48 Canbek ve Sağıroğlu (n 44) 126. Bir bilişim sistemindeki (akıllı telefon vs) casus yazılımın tespiti ancak cihaz üzerinde ayrıntılı bir inceleme ile ortaya çıkarılabilmektedir. Casus yazılımlar, işlevini yerine getirdikten sonra kendisini sistemden silmek üzere de programlanabilmektedir. Açıklama için bkz. Banu Salman ve Kahraman Yapıcı, 'Elektronik Gözaltı Dünyası: e- Göz@altı', (2009) (436) TMMO, Elektrik Mühendisleri Odası, Elektrik Mühendisliği, 17. Dergiye erişim için bkz. https://www.emo.org.tr/ekler/ff07078ffdc6a65_ek.pdf?dergi= 2 Kasım 2025.

49 Sümeyra Kavruk Şenol, *Mobil Akıllı Cihazlarda Casus Yazılımların Uygulamalı Analiz Yöntemiyle Tespiti*, (Yayınlanmamış Doktora Tezi, YÖK Tez Merkezi 2018) 39-40.

kaydeden ve bir sonraki kullanımda bu bilgileri/ tercihleri hatırlayarak ilgili içeriklere çok daha hızlı bir şekilde erişim imkânı sunan yazılımlardır[50].

Cookie'ler (çerezler), kişisel kullanıcı bilgilerinin elde edilmesi ve işlem yapılan internet sitesiyle ve bunun dışında -kullanıcının başlangıçta verdiği onay dahilinde veya onayı olmaksızın-[51] üçüncü kişilerle paylaşılabilmektedir. Özellikle, casus yazılım çerezleri (spyware cookie), iz sürme çerezleri (tracking cookie) gibi çerezlerle[52], kişilerin internet veya diğer ağlar (intranet) marifetiyle gerçekleştirdiği iletişim denetlenebileceği gibi kişinin kullandığı iletişim aracına "cookie'ler marifetiyle elde edilen kullanıcı adı ve şifre gibi bilgiler kullanılarak" yetkisiz erişimle iletişim izlenebilmektedir.

Casus yazılımlar marifetiyle cep telefonuyla veya internet tabanlı uygulamalar marifetiyle gerçekleştirilen bütün mesaj, sesli ve/veya görüntülü iletişimin eş zamanlı veya iletişimin tamamlanmasından sonra paket halinde gönderilmesi suretiyle izlenebilmesi ve denetlenebilmesi mümkündür[53]. Yine casus yazılımlar, bilgisayar veya internet ayarlarını kendi komutları dahilinde değiştirebilir, bir bilişim sistemini başka bir bilişim sistemine yönlendirebilir[54].

---

50 Canbek ve Sağıroğlu (n 44) 132. PHP Cookie (Çerez): "*Girilen sitelerin tarayıcılar(browserlar) üzerinde bıraktığı izlere cookie, Türkçesiyle de çerez denir. Bu izler siteye tekrar ziyaret edildiğinde yeniden gönderilerek bazı şeylerin yeniden hatırlanmasını sağlar.*

Mesela giriş formlarında kullanıcının şifresini ve kullanıcı adını cookieler sayesinde tarayıcıya kaydederek bir sonraki gelişinde bilgilerini yeniden girmek zorunda kalmadan direkt giriş yapabilir.

Temel olarak kullanıcı bilgilerini hatırlanmasında kullanılan çerezleri hayal gücünüzün el verdiği kadar bir çok alanda da kullanmak mümkün." https://www.phpr.org/php-cookie-cerezler/ 2 Kasım 2025.

51 Kullanıcının sadece belirli bir uygulama ya da site için verdiği iznin her daim geçerli olmayacağı, bu izni aşarak arka planda ya da uygulama açık değilken çerezlerin, botların ya da uygulamaların sisteme erişmesi halinde rızanın geçerli olmayacağı hususunda bkz. Gülennur Erkan, *Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları* (Yayınlanmamış Yüksek Lisans Tezi, YÖK Tez Merkezi 2021), 73.

52 Canbek ve Sağıroğlu (n 44) 132.

53 Salman ve Yapıcı (n 48) 17. Casus yazılımı içeren "*…ileti açılır açılmaz bu iletinin eklentisi olarak gönderilen casus yazılım kendisini sistemin değişik yerlerine gizli bir şekilde kopyalamaktadır. Görüldüğü gibi iletiyi gönderen şahıs burada bu safhaya kadar bilişim sistemine fiili olarak hiç girmemektedir. Ancak sistem içine değişik yöntemlerle sokulan casus program sayesinde fail her an sisteme ulaşabilir hale gelmekte, sistemin içinde her yapılan işlemi istediği takdirde izleme imkanına kavuşmakta yani o sistem içine nüfuz edebilme imkanını elinde tutmaktadır."* Açıklama için bkz. Erdoğan, Bilişim Suçları (n 1) 166.

54 Arslan (n 44) 7.

İnternet marifetiyle gerçekleştirilen iletişimin gizli bir şekilde denetlenmesi konusunda pek çok casus yazılım bulunmakla birlikte, dünya çapında en bilineni Pegasus casus yazılımdır[55]. Pegasus casus yazılımına ilişkin olarak Toronto Üniversitesi tarafından 2018 ve 2022 yıllarında hazırlanan araştırma raporlara göre yazılım, dünya geneline yayılan ve 2018 yılı itibariyle -aralarında Türkiye'nin de bulunduğu-[56] 45 ülkede kalıntıları tespit edilen bir yazılımdır[57].

Pegasus yazılımı marifetiyle bir cep telefonunda veya bilişim sistemindeki, mikrofon veya ses kaydetme cihazına, e- postalara, SMS'lere, konum izlerine, bağlantı detaylarına, cihaz ayarlarına, internet geçmişine, kişi listesine, sosyal bağlantılara, telefon aramalarına, takvim kayıtlarına, depolanmış dosyalara, doğrudan mesajlara, fotoğraflara ve ekran görüntülerine erişilebilmektedir[58].

Doğrudan casus yazılımlar veya cookie'ler ele geçirilmek suretiyle internet yoluyla yapılan iletişimin denetlenmesi mümkün olup bu şekilde internet veya diğer ağlar (intranet) marifetiyle gerçekleştirilen iletişime müdahale bireysel (gerçek veya tüzel kişi) kullanıcılardan gelebileceği gibi suç önleme veya suç soruşturması/ kovuşturması

---

55 https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ 2 Kasım 2025. 2022 yılı ek raporu için bkz. https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf 2 Kasım 2025. Yazılım ve geliştirilme süreci hakkında detaylı bilgi için bkz. Pınar Demirci, 'Siber Güvenlikte Siber Gözetim: Pegasus Projesi' (2024 3 (2) İstihbarat Çalışmaları ve Araştırmaları Dergisi 185 vd

56 2018 yılı raporunda, Türkiye'den de Pegasus yazılımıyla enfekte olduğu tespit edilen operatör ve internet erişim sağlayıcısı bulunmaktadır. Açıklama için bkz. 2018 yılı raporu, 34.

57 WhatsApp uygulamasının sahibi Meta şirketi tarafından Amerika'da, NSO Group'a karşı dava açılmış ve mahkemece "*1400 WhatsApp kullanıcısına karşı kullanıldığı*" iddiasını sabit kabul ederek, NSO'yu sorumlu tutmuştur. Mahkeme/ hâkim, NSO'nun WhatsApp'a "*casus yazılımın bütün fonksiyonları hakkında*" bilgi vermesine ancak NSO'nun, uygulamayı kullandığı telefonları, müşterilerinin isimleri ve sunucu mimarisine ilişkin bilgileri açıklamak zorunda olmadığına karar vermiştir. Dava için bkz. https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group 2 Kasım 2025. Özet kararın tam metni için bkz. https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.494.0.pdf 2 Kasım 2025.

58 https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ 7. 2 Kasım 2025. Yazılımın nasıl tespit edilebileceği hususunda bkz. Amnesty International, Forensic Methodology Report: How to Catch NSO Group's Pegasus, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ 7 Kasım 2025.

amacıyla kamu otoritelerinden (kolluk veya soruşturma/ kovuşturma mercilerinden) de gelebilecektir[59].

B. CMK'nin 135. Maddesi Kapsamında Casus Yazılım veya Çerez Kullanılarak İnternet Marifetiyle Yapılan İletişimin Denetlenebilmesi Mümkün Müdür?

Yukarıda yer verildiği üzere Türk hukukunda, CMK m 135'te yer verilen "telekomünikasyon" kavramından ve Yönetmelikte yer alan "her türlü iletişim" ibaresinden hareketle, internet veya diğer ağlar (intranet vs ağlar) marifetiyle yapılan iletişimin denetlenmesinin, CMK m 135 kapsamında olduğu kabul edilmektedir. Bu kabulden hareketle öğretide, internet marifetiyle yapılan iletişimin "*uygun teknik araçlarla*"[60] ve "*teknik imkân olması halinde*"[61] denetlenebileceği kabul edilmektedir[62].

Aksi düşünceye göre ise[63] Cumhuriyet savcısı tarafından yürütülen bir soruşturmada, şüphelinin telefonuna casus program yüklenmesini talep etmesi ve CMK m 134 ve 135'i bu işleme dayanak göstermesi, Kanun'da açıkça düzenlenmeyen bir

---

59 Pegasus yazılımının devletler tarafından -siyasi amaçlarla- "*ülke dışında yaşayan aktivistleri ve muhalifleri taciz etmek, sindirmek, susturmak, zulmetmek veya başka şekillerde takip etmek*" için casus yazılım da dahil olmak üzere dijital teknolojilere giderek daha fazla yöneldiği ve yazılımın özellikle sınır ötesi "hedeflere" karşı daha yaygın kullanıldığı hususunda bkz. 2022 yılı raporu, 17. Sınır ötesindeki "hedefler" için yazılımın kullanılması "*ulusötesi dijital baskı*" olarak tanımlanmaktadır. Tanım için bkz. Noura Al-Jiwazi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft ve Ron Deibert, 'Psychological and Emotional War: Digital Transnational Repression in Canada' *The Citizen Lab* at 1 (2022), 3 vd https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf 2 Kasım 2025.

60 Değirmenci (n 15) 386. Melemez'e göre de CMK m 135 kapsamında mobil telefonu hakkında iletişimin denetlenmesi tedbiri uygulanan kişinin, internet tabanlı uygulamalar vasıtasıyla iletişime geçtiği tespit edildiğinde, ilk karada belirtilen iletişim aracının "*türü*" değişmiş olacağından, bu konuda ayrı bir kararın alınması gerekir. Burak Melemez, 'Mesajlaşma Uygulamaları ile Bulut ve Sosyal Medya Ortamlarında Sayısal Delillerin Elde Edilmesi' (2023) (167) Türkiye Barolar Birliği Dergisi 83, 94.

61 Dülger ve Taşkın (n 17) 487.

62 İnternet veya diğer ağlar marifetiyle yapılan iletişim bakımından dinleme kavramı yerine "iletişimin dinlenmesi, takip edilmesi ve kayda alınması" kavramının kullanılması daha isabetlidir. Zira bu yollarla gerçekleştirilen iletişimin denetlenmesinde -iletişim araçlarının mahiyeti gereği- "dinleme" istisnaidir.

63 Ersan Şen, 'Casus Programla Dinleme' (sen.av.tr, 7 Kasım 2015), https://sen.av.tr/tr/makale/casus-programla-dinleme 2 Kasım 2025. .

koruma tedbiri mahiyetinde olacağından, kıyas yapılması anlamına gelir ve bu şekilde delil elde etmek hukuka aykırı kabul edilmelidir[64].

Düşüncemize göre her ne kadar CMK m 135'te "*telekomünikasyon yoluyla yapılan iletişimin denetlenmesi*" koruma tedbirinin kapsamına internet veya diğer ağlar marifetiyle yapılan iletişim dahil olsa da CMK'de ve Yönetmelik'te, bu tür bir denetimin nasıl yapılacağı hususunda açık bir düzenleme yer almamaktadır.

İnternet marifetiyle gerçekleştirilen bir iletişime müdahalenin internete bağlanan araca (telefona veya bilgisayara) anlık uzaktan erişim yoluyla mı yoksa araca bir uygulama yükleyerek veya çerez (cookie) kullanılmak suretiyle mi gerçekleştirilebileceği, müdahaleyi kimin hangi şekilde yapacağı, denetleme öncesinde veya denetleme sırasında tedbirin doğrudan muhatabı olmayan ve iletişimin diğer tarafının iletişim aracına (cep telefonuna veya bilgisayarına) doğrudan müdahale edilip edilemeyeceği hususları belirsizdir. Yine bu yolla elde edilen iletişim içeriklerinin nasıl kaydedileceği, saklanacağı ve gerekmesi halinde nasıl yok edileceği hususunda herhangi bir düzenlemeye yer verilmemiştir. CMK ve Yönetmelik, sabit veya mobil telefonlar marifetiyle gerçekleştirilen iletişim bakımından bu hususlarda ayrıntılı düzenlemelere yer verdiği halde, internet veya diğer ağlar marifetiyle yapılan iletişim bakımından herhangi bir düzenleme yapmamıştır.

Kanaatimizce internet veya diğer ağlar marifetiyle yapılan iletişim bakımından da tıpkı sabit veya mobil telefonlarla gerçekleştirilen iletişimin denetlenmesinde olduğu gibi tedbirin uygulanma biçimi, dinleme, kayda alma ve gerektiğinde yok etme işlemlerinin ne şekilde yapılacağı, iletişim aracının kod veya şifre bilgilerine erişilip erişilemeyeceği ve iletişimin diğer tarafı olan (tedbirin muhatabı olmayan) kişinin iletişim aracına ilişkin bilgilere erişilip erişilemeyeceği[65] vs hususlarda açık ve ayrıntılı düzenlemeye ihtiyaç bulunmaktadır.

---

[64] Şen'e göre CMK m 135, 134'e nazaran "özel hüküm" niteliğinde olup CMK m 135'te izin verilen usul dışında bir delil toplama yöntemi uygulanamaz ve bu yolla elde edilen delillerin hukuka uygun olduğu kabul edilemez. Aksinin kabulü, CMK m 135'i anlamsız hale getirir. Ibid.

[65] Öğretide CMK m 134 hükmünün, başkasına ait ve yabancı bir ülkede bulunan bulut bilişim sistemine ilişkin kullanıcı adı ve şifresini etkisiz hali getirerek bulut bilişim sistemine girme hak ve yetkisi vermediği ifade edilmektedir. Görüş için bkz. Olgun Değirmenci, 'Bulut Bilişim ve Beraberinde Getireceği Hukuksal Sorunlar Üzerine Görüşler' (2017) 12 (136) Terazi Hukuk Dergisi 106, 110. Aynı

Belirtmek gerekir ki; özel kanunlarda yer verilen istisnalar hariç olmak üzere[66] bu yollarla iletişimin denetlenmesi işlemi ancak bir ceza soruşturması veya kovuşturmasıyla bağlantılı olarak ancak Türk merciler tarafından yapılabileceğinden, yabancı bir merci tarafından veya yabancı merciye yetki verilmek suretiyle bu şekilde bir denetimin yapılabilmesi mümkün değildir.

Yine internet veya diğer ağlar marifetiyle yapılan iletişimin denetlenebilmesi bakımından iletişim için kullanılan bilgisayar veya mobil telefona el konulması, bu cihazlarda veya iletişimin yürütüldüğü bilişim sisteminde arama, kopyalama veya elkoyma yapılması ya da eş zamanlı olarak teknik araçlarla izleme yapılması gerekebileceğinden, bu tedbirlerin birlikte uygulanabileceğine dair bir düzenleme yapılması da isabetli olacaktır[67].

CMK'ye "*İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması"* başlıklı Madde 135/A eklenmek suretiyle, şu şekilde bir düzenlemeyle eksikliğin giderilebileceğini düşünmekteyiz:

"*İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin denetlenmesi*

(1) İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması yukarıdaki maddeye göre yürütülür. Bu yollarla gerçekleştirilen iletişimin

---

yönde bkz. Erdoğan, AKSS (n 12) 170. Ancak hesap bilgilerinin CMK m 134 kapsamında alınan bilgisayar kütüklerinde arama kararına istinaden, yani hukuki bir prosedür izlenerek imajı alınan sabit bir bellek üzerinde çeşitli yazılım ve programların kullanılması suretiyle öğrenilmesi ve bulutta depolanan verilerin bu yöntemle elde edilmesinin (CMK m 134/2 hükmü dikkate alındığında) hukuka aykırı olmadığı da öne sürülmektedir. Görüş için bkz. Melemez (n 60) 117.

[66] Örneğin; 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu m 25/3 ve Avrupa Konseyi Siber Suç Sözleşmesi (AKSS), m 16-17, 22-23. Sözleşme metni için bkz. https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm

[67] Ölçülülük ilkesinin koruma tedbirlerine bir yansıması olarak koruma tedbirleri arasında öncelik-sonralık/ birincillik- ikincillik sınıflandırması yapılabileceğinden, her iki grupta yer alan koruma tedbirinin bir arada uygulanabileceğine dair açık bir düzenleme muhtemel uyuşmazlıkları ortadan kaldırabilecektir. Koruma tedbirleri arasındaki öncelik-sonralık ilişkisi Yargıtay kararlarına da yansımıştır: "…*öncelikle 5271 sayılı CMK gereğince genel soruşturma usulleri ve CMK'nın 135. maddesi kapsamında iletişimin tespitine ilişkin tedbir kararı alınarak delil elde edilmeye çalışılması gerekirken sanıkla buluşma öncesinde gizli soruşturmacıların sanığı telefon ile arayarak irtibat kurdukları, gizli soruşturmacıların yalnızca pasif bir şekilde suç teşkil eden eylemi incelemekle sınırlı kalmayıp bir sonuca ulaşmak için yani kanıt toplamak amacıyla sanığın suç teşkil eden bir eylem hazırlığında olmadığı aşamada suça teşvik edecek nitelikte uyuşturucu madde isteyerek sanığın iradesi üzerinde etkili oldukları ve bu nedenle elde edilen delillerin hukuka aykırı delil niteliğinde olduğu*…" Yargıtay 10. CD, 25.03.2025, E. 2023/16840, K. 2025/3578.

denetlenmesine ilişkin kararlarda, yukarıdaki maddenin 6. fıkrasındaki bilgilere ek olarak, tedbirin konusunu oluşturan ve şüpheli veya sanığa ait olan veya şüpheli/ sanık tarafından kullanılan bilgisayar veya sair elektronik cihazların adları, denetimin hangi kurum tarafından yerine getirileceği, denetim sırasında hangi internet verilerine erişilebileceği, uzaktan erişim yönteminin veya verilere erişim için bu amaçla oluşturulmuş araçların/ yazılımların kullanılıp kullanılamayacağı, hangi verilerin kaydedileceği ve tedbirin icra edilebilmesi için iletişimin diğer tarafının kullandığı iletişim aracına müdahale edilip edilmeyeceği, müdahale edilmesi gerekiyorsa hangi verilere müdahale edileceği gösterilir.

(2) İnternet veya diğer ağlar yoluyla yapılan iletişimin denetlenebilmesi için iletişimin diğer tarafı olan kişinin iletişim aracına, denetim için gerekli olan bağlantı kodu veya sair bilgilerine uzaktan erişilebilir. Ancak bu kişi hakkında ayrıca bir karar alınmaksızın iletişimi denetlenemez.

(3) Bir suç nedeniyle yürütülen soruşturma ve kovuşturma sırasında, şüpheli veya sanığın yakalanması, delil elde edilmesi veya internet ya da diğer ağlarla yapılan iletişimin dinlenebilmesi veya kayda alınabilmesi için şüpheli veya sanığa ait olan ya da şüpheli veya sanık tarafından kullanıldığı tespit edilen iletişim aracının internet veya diğer ağdaki trafik bilgileri tespit edilebilir. Şüpheli veya sanığa ait trafik verilerinin tespit edilmesi için zorunlu olması halinde şüpheli veya sanık dışındaki kişilerin elektronik cihaz bilgilerine, cihazda kullanılan kart numarasına, koduna ve internet trafik verilerine de uzaktan erişilebilir. Ancak bu kişi hakkında ayrıca bir karar alınmaksızın iletişimi dinlenemez ve kayda alınamaz. Bu tedbire soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararıyla başvurulabilir. 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. Kararda, suçun türü, internet veya diğer ağın adı, hakkında tedbir uygulanacak kişinin kimliği, tespite konu iletişim aracının türü, iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi belirtilir.

(4) İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması ve trafik verilerinin tespiti tedbirleri, diğer koruma tedbirleriyle birlikte uygulanabilir.

Çalışmamızın başında vurgulanan ve koruma tedbirlerine ilişkin kanuni düzenlemelerin "bilinebilirliğinin" ve "öngörülebilirliğinin" karşılanabilmesi için önerdiğimiz şekilde genel mahiyette bir düzenleme yapıldıktan sonra, uygulamanın detaylarının CMK m 140/A uyarınca çıkarılacak yönetmelikte[68] düzenlenmesi gerekmektedir.

Bu bağlamda belirtmek gerekir ki; internet veya diğer ağlar marifetiyle yapılan iletişimin denetlenmesinde kullanılacak yazılımların neler olduğunun ve çalışma biçimlerinin veya yazılımlara ilişkin detayların Kanun'da ve Yönetmelik'te düzenlenmesi gerekli olmadığı gibi bu tür bir düzenleme de tedbirlerle ulaşılmak istenen amaçla çelişir. Aksinin kabulü halinde, şüphelinin/ sanığın, internet veya diğer ağlar marifetiyle yapılan iletişimin denetlenmesine karşı dijital olarak karşı koyma tedbiri alması için imkân sağlanmış olur.

IV. KARŞILAŞTIRMALI HUKUKTAKİ DURUM

A. Amerika Birleşik Devletleri

Amerikan Yüksek Mahkemesi'nin uygulamasına göre bireylerin makul bir gizlilik beklentisinin olduğu tüm konuşmalar Amerikan Anayasası'nın makul olmayan arama ve el koymaya karşı koruma sağlayan Dördüncü Değişiklik kapsamındadır[69]. Bu sebeple iletişim özgürlüğüne, suç önlenmesi veya suç soruşturması amacıyla ancak makul sebebin bulunduğu hallerde müdahale edilebilmektedir.

---

[68] Adalet Bakanlığı tarafından çıkarılan Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'in Danıştay tarafından 2017 yılında iptal edilmesinden bugüne kadar CMK m 140/A'da çıkarılacağı öngörülen yönetmeliğin halen çıkarılmadığını vurgulamak gerekmektedir.

[69] Amerikan Yüksek Mahkemesi'nin Berger v. New York, 388 US 41 (1967) ve Katz v. United States, 389 US 347 (1967) kararları. Karar metinleri için bkz. https://supreme.justia.com/cases/federal/us/388/41/ https://supreme.justia.com/cases/federal/us/389/347/ 7 Kasım 2025.

Amerikan hukukunda iletişimin denetlenmesine ilişkin temel kanun "Title III" olarak adlandırılan The Omnibus Crime Control and Safe Streets Act (Wiretap Act, 1968) olup bu Kanun, kabul edildikten sonra pek çok kez değişikliğe uğramıştır[70].

İletişimin denetlenmesi Kanun'da ağır federal suçlar olarak sayılan katalogda yer alan suçlarla (temelde en az 1 yıl hapis cezasını gerektiren suçlarla) sınırlı olarak ve ancak makul sebebin (probable cause) bulunduğu hallerde ve diğer (klasik) koruma tedbirlerine/ soruşturma yöntemlerine başvurulduktan sonra (ikincil mahiyette) uygulanabilen bir tedbirdir[71].

Title III'e göre[72] acil durumlar hariç[73] hâkim kararı/ onayı ile her türlü klasik (posta vs) veya elektronik iletişim aracının denetlenebilmesi mümkündür. Azami süre otuz gündür. Bu sürenin her defasından otuzar gün uzatılabilmesi mümkündür (§ 2518-4).

Title III'te iletişim aracı bakımından herhangi bir sınırlandırma yapılmaksızın (gezici takip dahil)[74] her türlü iletişim tedbir kapsamına alınmakla birlikte internet veya diğer ağlar marifetiyle gerçekleştirilen iletişimin denetlenebilmesi için casus yazılım veya çerez kullanılabileceği veya iletişim için kullanılan elektronik cihaza uzaktan erişilebileceği hususunda açık bir hükme yer verilmemiştir.

Numara ve Rota Tespit Kanunu'na (The Pen/ Trap Statute)[75] göre de gerçek zamanlı olmak kaydıyla adresleme bilgileri ve iletişim içeriği dışındaki bilgileri takip ve

---

[70] Kanun metni ve değişiklikler için bkz. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284 7 Kasım 2025.

[71] Sonradan yapılan eklemelerle suç sayısının 100'ü aştığı ifade edilmektedir. Bkz. Yardımcı (n 16) 31.

[72] Title III için bkz. https://www.law.cornell.edu/uscode/text/18/2518 7 Kasım 2025.

[73] Acil durumlar, bir kişinin ölüm veya bedeni yaralanma tehlikesinin ortaya çıkması, ulusal güvenliği tehdit eden bir komplonun olması veya organize suçlar kapsamında bir komplo faaliyetinin (örgütsel bir eylemin) gerçekleşmiş olmasıdır. Bu hallerde, Kanun'daki diğer hükümlere bakılmaksızın, Başsavcı, Başsavcı yardımcısı veya her eyaletin kanununda belirlenen soruşturma veya kolluk görevlisi iletişimin denetlenmesi tedbirine karar verebilir. Ancak bu kararın 48 saat içinde hâkim onayına sunulması gerekir (§ 2518-7/b).

[74] Takip edilen ancak takipten kurtulmak için değişik yöntemlere başvuran kişi hakkında, "*kullandığı ve gelecekte kullanacağı*" iletişim araçları için iletişimin denetlenmesine karar verilebilmektedir (§ 2518-8/b-ii).

[75] Kanun metni için bkz. https://www.law.cornell.edu/uscode/text/18/3121 7 Kasım 2025.

tespit etme imkânı bulunmaktadır[76]. Bu Kanun kapsamında, telefon numarasının tespit edilmesi, iletişimin tespiti (gelen giden arama tespiti), rota belirleme ve takip, tuşlama, yönlendirme, adresleme ve sinyal bilgilerinin kaydedilmesi ve takip edilebilmesi mümkündür.

Tedbir kapsamındaki işlemler telefon esas alınarak tanımlanmış olsa da Mahkemeler, bu Kanun'daki işlemlerin bilgisayar marifetiyle yapılan iletişimi de (bütün iletişim teknolojilerini de) kapsadığını kabul etmektedir[77]. Nitekim Kanun'da daha sonra yapılan değişiklikte (§ 3121/c) tedbirin, "elektronik iletişimleri" kapsadığı açıkça ifade edilmiştir. Anılan düzenlemede, yetki verilen görevlilerin "makul ölçüde kendisine sunulan teknolojiyi" kullanabilecekleri belirtilmekle birlikte, kullanılacak teknolojilerin neler olduğu açık ve sınırlayıcı bir şekilde sayılmamıştır[78]. Hiç şüphesiz bu düzenleme, anılan verilerin casus yazılım veya çerez kullanılmak suretiyle ele geçirilmesi yetkisini vermektedir. Ancak bu yetkinin nasıl kullanılacağı hususunda Kanun'da açık bir düzenlemeye yer verilmemiştir.

B. Birleşik Krallık

İngiltere'de iletişimin denetlenmesi tedbiri en son 2016 yılı Aralık ayında yürürlüğe konulan Soruşturma Yetkileri Kanunu (Investigatory Powers Act)[79] ile kapsamlı bir şeklide düzenlenmiş ve bu Kanun da 2024 yılında değişikliğe uğramıştır[80].

---

76 Yardımcı (n 16) 71.

77 Açıklama ve mahkeme kararları için bkz. Yardımcı (n 16) 72.

78 Amerika Federal Ceza Muhakemesi Kurallarına (Federal Rules of Criminal Procedure) göre (m 41/b-6'da 2017 yılında yapılan değişiklikle); federal bir kolluk görevlisi veya kamu adına çalışan bir avukatın talebi üzerine, hâkim kararıyla, bir suçla ilgili olarak, elektronik verilerin depolandığı ve teknolojik yöntemlerle gizlendiği ortamları uzaktan arama, verilere uzaktan erişme, verilere elkoyma, verileri kopyalama tedbirleri uygulanabilir. Kural için bkz. https://www.law.cornell.edu/rules/frcrmp/rule_41 7 Kasım 2025.

79 Kanun metni için bkz. https://www.legislation.gov.uk/ukpga/2024/9/contents 7 Kasım 2025.

80 Bu düzenlemeden önce iletişimin denetlenmesi tedbiri Regulation of Investigatory Powers Act 2000 (RIPA) hükümleri kapsamında uygulanmaktaydı. Soruşturma Yetkileri Kanunu'nun tam anlamıyla (bütün tedbirler itibariyle) yürürlüğe girdiği 2018 yılında RIPA'daki iletişimin denetlenmesine ilişkin hükümler yürürlükten kaldırılmıştır. RIPA için bkz. https://www.legislation.gov.uk/ukpga/2000/23/contents 7 Kasım 2025. Süreç hakkında bkz. AİHM, Big Brother Watch and Others vs Birleşik Krallık (2021) B. No. 58170/13, 62322/14, 24960/15, par183 vd ve par 269. Karar için bkz. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]} 7 Kasım 2025.

Soruşturma Yetkileri Kanunu'na göre (2024 yılı değişiklikleriyle birlikte) suç şüphesi altında bulunan kişiye ilişkin yığılmış/ toplu kişisel verilerde arama yapılabilmesi, üçüncü kişilerin toplu/ yığılmış kişisel verilerinde arama yapılması, iletişime ilişkin verilerde[81] (iletişimin tespiti) ve ikinci verilerde (iletişim aracına ilişkin verilerde) arama yapılması, internet kayıtlarında (internet trafik bilgilerinde) arama yapılması mümkündür.

Kanun'un 261. Bölümüne (Section 261)[82] göre bir telekomünikasyon hizmeti veya operatörü veya telekomünikasyon sistemiyle ilişkili bir kavram olarak "iletişim", kişiler arasındaki konuşma, müzik, ses, görsel görüntü veya herhangi bir veriyi veya veriye ilişkin her şeyi, bu hizmetleri sunan kurum tarafından tutulan her türlü veriyi, konum verilerini, iletişim verilerini, sistem verilerini, abone verilerini, iletişim içeriklerini (anlamlı veya makul bir şekilde değerlendirilebilecek herhangi bir şeyi ortaya koyan bütün verileri) kapsamaktadır.

"*Hedefli dinleme*" emri olarak tanımlanan ve belli bir kişinin dinlenmesine ilişkin olan emir, arama emrinde belirtilmeyen iletişimin dinlenmesini (kişinin kullandığı bütün diğer iletişim araçlarının dinlenmesini) ve iletişime ilişkin ikincil verilere erişimi, operatörde bulunan sistem verilerine erişimi, ilgili kişi hakkında denetim kararı verilmesine neden olan herhangi bir eylemi gerçekleştiren kişinin iletişiminin dinlenmesini de içermektedir[83].

İletişimin denetlenmesi (dinleme, tespit, verilere erişim ve ikincil verilere erişim) tedbirlerine, belli bir veya birkaç kişi, kişi topluluğu, kurum, kurum/ tesis kümesi, test veya eğitim faaliyetleri ile ilgili olarak karar verilebilir (Section 17).

Kanun'a göre iletişimin denetlenmesine karar verme yetkisi, istihbarat servis başkanına, ulusal suç ajansı direktörüne, metropol polis komiserine, Kuzey İrlanda Polis Teşkilatı Polis Şefine, İskoçya Polis Teşkilatı Şefine, Kraliyet Gelir ve Gümrük Komiserlerine, Savunma İstihbarat Servis Şefine ve uluslararası karşılıklı adli

[81] İletişimin içeriği dışındaki veriler "ikincil veri" (secondary data) olarak tanımlanmaktadır. Tanımlama için bkz. Soruşturma Yetkileri Kanunu (2016), Section 16.

[82] https://www.legislation.gov.uk/ukpga/2016/25/section/261 7 Kasım 2025.

[83] Part 2, Chapter 1, Section 15. Kavramların tanımları için bkz. Section 263.

yardımlaşma anlaşması kapsamında Birleşik Krallık dışındaki bir ülke veya bölgenin yetkili makamı olan kişiye aittir (Section 18)[84].

İletişimin denetlenmesi tedbiri, adli amaçlı olarak "ağır suçların" ortaya çıkarılması/ ispatı amacıyla başvurulabilecek bir tedbirdir (Section 2, Article 4/b). Kanun'a göre "ağır suç" kavramı ise *"şiddet içeren, önemli bir maddi kazanç sağlayan veya birden fazla kişi tarafından ortak bir amaç doğrultusunda gerçekleştirilen 18 yaşını tamamlamış (İskoçya ve Kuzey İrlanda da 21) ve daha önce sabıkası bulunmayan bir kişinin en az 3 yıl veya daha fazla hapis cezasına mahkum olması beklenen*" bir suçtur (Section 263).

İletişimin denetlenmesi tedbiri, acil bir durumda (yetkili bir kişinin onayı olmadan veya dinleme kararının çıkarılması bakımından acil bir ihtiyaç olduğu/ gecikmesinde sakınca bulunduğu gerekçesiyle) verilmişse karar verildiği tarihten sonraki ilk iş gününün sonunda (eğer yenilenmezse) sona erer. Diğer durumlarda, kararın verildiği günden veya yenileme süresinin sona erdiği günün ertesi gününden başlayarak 6 aylık bir süre için verilmektedir (Section 32).

Soruşturma Kanunu'nda casus yazılım veya çerezler marifetiyle iletişimin denetlenmesine dair açık bir düzenleme bulunmasa da -yukarıda da ifade edildiği üzere- Bölüm (Section) 261'deki tanımlamanın genişliği nazara alındığında, telekomünikasyon tanımına internet veya diğer ağlar marifetiyle yapılan iletişimin de girdiği ve yine tedbir kapsamında müdahale edilebilecek verilerin mahiyeti (Section 15) dikkate alındığında ise hem soruşturmanın hedef kişisi hem de bu kişilerle ilişkili kişi veya kişiler (ve hatta kurumlar) hakkında bu tür verilerin toplanması bakımından casus yazılım dahil pek çok dijital aracın kullanılabileceği ancak casus yazılım veya çerez kullanılarak iletişimin ne

[84] Toplu dinleme başvurusu ise sadece Güvenlik Servis Direktörü, Gizli İstihbarat Servis Direktörü ve Devlet Haberleşme Karargâh Direktörü tarafından yapılabilmektedir. Bkz. Interception of Communications: Draft Revised Code of Practice, October 2022, m 4.8. Erişim için bkz. https://www.gov.uk/government/publications/draft-revised-interception-of-communications-code-of-practice-2022/interception-of-communications-draft-revised-code-of-practice-october-2022-accessible 7 Kasım 2025. AİHM, "toplu iletişimin denetlenmesi" uygulamasının AİHS m.8'i ihlal ettiğine karar vermiştir. Big Brother Watch and Others vs Birleşik Krallık, par 425.

şekilde denetlenebileceğine dair açık bir yasal düzenlemenin bulunmadığı sonucu ortaya çıkmaktadır[85].

C. Almanya

Alman Ceza Muhakemesi Kanunu'nda[86] (StPO'da) aktüel/ halen mevcut olan iletişimin denetlenmesi ve kayda alınması (m 100a), sona ermiş/ tamamlanmış iletişime ilişkin içeriklerin ve iletişim bilgilerinin (olayın araştırılması veya şüphelinin yakalanabilmesi için) tespit edilmesi (m 100g) ve iletişimin sonlandığı cep telefonunun cihaz numarasının, cihazda kullanılan kartın numarası ile bu telefonun bulunduğu yerin araştırılması (m 100i) ayrı koruma tedbirleri olarak düzenlenmiştir[87].

Toplanmış iletişim verilerine erişim (m 100j) ve iletişimin tamamlanması sonrasında hizmet sunucuları dışındaki yerler nezdinde bulunan ve iletişim tespiti kapsamına giren datalara erişim, genel hükümlere göre yürütülmektedir (m 100g/3).

Alman hukukunda düzenlenen iletişimin denetlenmesi tedbirinin, sadece kablolu telefonlarla sınırlı olmadığı, telekomünikasyon kavramının geniş bir biçimde tanımlandığı ve bu kavramın içine internet telefonu, kısa mesaj gönderileri, e-mailler ve cep telefonu ile yapılan iletişimin de dahil olduğu kabul edilmektedir[88]. Yine, telekomünikasyon yoluyla yapılan iletişimin denetlenebilmesi için, m 100i'de yer verilen, iletişimin sonlandığı cep telefonunun (IMSI Catcher cihazı kullanılarak) cihaz

---

85 AİHM, iletişim hizmet sağlayıcılarından elde edilen iletişim verilerinin toplanmasına ilişkin yetkinin yalnızca ağır suçlarla sınırlı olmaması, veriler toplanmadan önce bir mahkeme veya bağımsız bir idari organ tarafından ön incelemeye tabi olmaması nedeniyle Sözleşme'nin 8. maddesini ihlal ettiğine karar vermiştir. Big Brother Watch and Others vs Birleşik Krallık, par 518-522. Aynı kararda Mahkeme, yabancı istihbarat servislerden istihbarat materyali alınmasına ilişkin yetkinin -Birleşik Krallık hukukunda yeterli güvencelerin bulunması nedeniyle- Sözleşme'nin 8. Maddesini ihlal etmediğine karar vermiştir (par 513-514).

86 Alman Ceza Kanunu'ndaki (StPO'daki) düzenlemeler için bkz. Feridun Yenisey ve Salih Oktar, *Alman Ceza Muhakemesi Kanunu* (2. Baskı, Beta Yayınları 2015) 89 vd

87 Alman Ceza Usul Kanunu (StPO) m 100 b/1'de düzenlenen online aramanın, çeşitli casus yazılımlardan faydalanarak şüphelinin kullandığı bilişim sistemine gizlice erişilip veri toplanması amacıyla başvurulan bir koruma tedbiri olduğu hususunda bkz. Melemez (n 60) 11, dn 124.

88 Friedrich- Christian Schroeder ve Torsten Verrel, *Ceza Muhakemesi Hukuku* (Çev Salih Oktar) (1. Baskı Yetkin 2019) 101. Halen hukuken kabul edilmeyen "iletişim verilerinin önceden depolanması" ve hali hazırda süren bir iletişimin bulunmadığı hallerde müdahaleyle online arama yapılması, yanlışlıkla kapatılmamış telefonun bulunduğu yerde ortam dinlemesiyle yapılan konuşmaların dinlenmesi ve dinlenen bir telefon görüşmesi sırasında telefona yansıyan ("arka plan konuşmalarının") StPO m 100a'ya göre delil olarak değerlendirilebileceği kabul edilmektedir. Açıklama için bkz. Ibid 101.

numarasının, cihazda kullanılan kartın numarasının tespiti işlemi de bir tür hazırlık olarak başvurulabilecek bir tedbirdir[89].

Alman hukuku bakımından, iletişimin denetlenmesinde casus yazılım veya çerez kullanılıp kullanılamayacağına dair açık bir yasal düzenleme bulunmasa da iletişimin denetlenmesi tedbirinin mahiyeti gözetildiğinde, casus yazılım veya çerez kullanılmak suretiyle iletişimin denetlenebilmesine imkân tanıdığı ancak tedbirin bu yollarla uygulanması halinde yasal ve yeterli güvencelere Kanun'da yer verilmediği görülmektedir.

SONUÇ

İletişim araçlarının her geçen gün daha gelişmiş hale gelmesiyle birlikte gerek bilişim ve bilişim araçlarıyla işlenen suçların ve gerekse diğer suçlara ilişkin maddi gerçeğin ortaya çıkarılması ve suç faillerinin tespit edilmesi güçleşmektedir. Hiç şüphesiz iletişim alanındaki her gelişme, suç failleri tarafından da yakından takip edilmektedir.

Bilişim suçları ve bilişim araçlarıyla işlenen diğer suçlar bakımından, şüpheliler arasındaki haberleşme, tespit edilmelerindeki teknik zorluklar nedeniyle büyük ölçüde internet veya diğer ağlar marifetiyle sunulan haberleşme araçlarına kaymıştır. Bu sebeple, bu tür suçlar bakımından CMK m 135'te düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbirinin halihazırdaki uygulanma biçiminin ceza muhakemesinin güncel ihtiyaçlarını karşılamakta yetersiz ve teknolojinin de gerisinde kaldığı söylenebilir. Karşılaştırmalı hukukta olduğu gibi iletişimin denetlenmesi tedbirinin kapsamının internet veya diğer ağlar marifetiyle gerçekleştirilen iletişim yöntemlerini de kapsayacak şekilde genişletilmesine ihtiyaç bulunmaktadır.

İnternet veya diğer ağlar marifetiyle gerçekleştirilen iletişimin denetlenmesi, temelde CMK m 135'te yer verilen "telekomünikasyon" kavramından ve Yönetmelikte yer alan "her türlü iletişim" ibaresinden hareketle, CMK m 135 kapsamında olduğu kabul edilse ve internet marifetiyle yapılan iletişimin "*uygun teknik araçlarla*" ve "*teknik imkân*

[89] Ibid 101.

olması halinde" denetlenebileceği düşünebilirse de bu tür bir denetimin nasıl, "hangi araçlarla" ve hangi merci tarafından yapılacağı, hangi internet iletişim verilerine erişilebileceği, üçüncü kişilerin internet iletişim verilerine müdahale edilip edilemeyeceği, bu maksatlı yazılım veya çerez kullanılıp kullanılamayacağı vs hususları Kanun'da ve Yönetmelik'te açıkça düzenlenmemiştir. Zira özellikle Yönetmelik, iletişimin denetlenmesinin sadece BTİK koordinasyonuyla yapılabileceğini düzenlemekte ve sadece sabit veya mobil telefon hatlarıyla yapılan iletişimin denetlenmesine ilişkin detaylı hükümlere yer vermektedir[90].

Hali hazırda internet veya diğer ağlar marifetiyle gerçekleştirilen iletişimin denetlenebilmesi bakımından CMK m 135'te ve Yönetmelik'te yer alan düzenlemelerin, "koruma tedbirlerinin kanuniliği" ilkesinin sağlaması gereken "bilinebilirlik" ve "öngörülebilirlik" kriterlerini sağlamaktan uzak ve hukuk güvenliği açısından yeterli güvenceye sahip olmadığı anlaşılmaktadır.

Karşılaştırmalı hukuktaki örnekler de dikkate alınarak; CMK'ye "*İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması"* başlıklı Madde 135/A eklenmek suretiyle, şu şekilde bir düzenlemeyle eksikliğin giderilebileceğini düşünmekteyiz:

"*İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin denetlenmesi*

(1) İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması yukarıdaki maddeye göre yürütülür. Bu yollarla gerçekleştirilen iletişimin denetlenmesine ilişkin kararlarda, yukarıdaki maddenin 6. fıkrasındaki bilgilere ek olarak, tedbirin konusunu oluşturan ve şüpheli veya sanığa ait olan veya şüpheli/ sanık tarafından kullanılan bilgisayar veya sair elektronik cihazların adları, denetimin hangi kurum tarafından yerine getirileceği, denetim sırasında hangi internet verilerine erişilebileceği, uzaktan erişim yönteminin veya verilere erişim için bu amaçla oluşturulmuş araçların/ yazılımların kullanılıp kullanılamayacağı, hangi verilerin kaydedileceği ve tedbirin icra edilebilmesi için iletişimin diğer tarafının kullandığı

[90] CMK m 140/A'da çıkarılacağı öngörülen yönetmeliğin 2017 yılından bu yana halen çıkarıl(a)madığına da bir kez daha vurgulamamız gerekmektedir.

iletişim aracına müdahale edilip edilmeyeceği, müdahale edilmesi gerekiyorsa hangi verilere müdahale edileceği gösterilir.

(2) İnternet veya diğer ağlar yoluyla yapılan iletişimin denetlenebilmesi için iletişimin diğer tarafı olan kişinin iletişim aracına, denetim için gerekli olan bağlantı kodu veya sair bilgilerine uzaktan erişilebilir. Ancak bu kişi hakkında ayrıca bir karar alınmaksızın iletişimi denetlenemez.

(3) Bir suç nedeniyle yürütülen soruşturma ve kovuşturma sırasında, şüpheli veya sanığın yakalanması, delil elde edilmesi veya internet ya da diğer ağlarla yapılan iletişimin dinlenebilmesi veya kayda alınabilmesi için şüpheli veya sanığa ait olan ya da şüpheli veya sanık tarafından kullanıldığı tespit edilen iletişim aracının internet veya diğer ağdaki trafik bilgileri tespit edilebilir. Şüpheli veya sanığa ait trafik verilerinin tespit edilmesi için zorunlu olması halinde şüpheli veya sanık dışındaki kişilerin elektronik cihaz bilgilerine, cihazda kullanılan kart numarasına, koduna ve internet trafik verilerine de uzaktan erişilebilir. Ancak bu kişi hakkında ayrıca bir karar alınmaksızın iletişimi dinlenemez ve kayda alınamaz. Bu tedbire soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararıyla başvurulabilir. 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. Kararda, suçun türü, internet veya diğer ağın adı, hakkında tedbir uygulanacak kişinin kimliği, tespite konu iletişim aracının türü, iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi belirtilir.

(4) İnternet veya diğer ağlar yoluyla gerçekleştirilen iletişimin dinlenmesi ve kayda alınması ve trafik verilerinin tespiti tedbirleri, diğer koruma tedbirleriyle birlikte uygulanabilir.

Önerimiz doğrultusunda veya benzer mahiyette bir yasal düzenleme yapıldıktan sonra Yönetmelik'te, internet veya diğer ağlar marifetiyle yapılan iletişimin denetlenmesinde görevli ve yetkili "ulusal" organların belirtilmesi ve tedbirin uygulanmasına ilişkin temel kuralların düzenlenmesi yeterlidir. Belirtmek gerekir ki; tedbirin icrası sırasında kullanılacak yazılımların neler olduğunun ve çalışma biçimlerinin

veya yazılımlara ilişkin detayların Kanun'da ve Yönetmelik'te düzenlenmesi gerekli olmadığı gibi bu tür bir düzenleme de tedbirlerle ulaşılmak istenen amaçla çelişir. Zira amacı ve mahiyeti gözetildiğinde gizli icra edildiğinde beklenen faydayı sağlayabilecek bir tedbirin, bütün teknik detaylarıyla birlikte mevzuatta düzenlenmesi, bu tedbirden sonuç alınmasını zorlaştırır ve suç faillerine bir tür dijital karşı koyma imkânı sunar.

KAYNAKÇA

Alacakaptan U ve Karcılıoğlu K, 'Çağdaş Demokratik Toplumda Özel Hayatın Korunması Bağlamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi', (2012) IX, (2) YÜHFD (Prof. Dr. Duygun Yarsuvat'a Armağan), 35-56.

Al-Jiwazi, N, Anstis S, Barnett S, Chan S, Leonard N, Senft A ve Diebert R, 'Psychological and Emotional War: Digital Transnational Repression in Canada' (2022) The Citizen Lab.

Amnesty International, Forensic Methodology Report: How to Catch NSO Group's Pegasus (2021).

Arslan ME, 'Siber Güvenlik ve Siber Saldırı Türleri', (academia, 2 Kasım 2025).

Avrupa Parlamentosu İç Politikalar Genel Direktörlüğü (C Departmanı), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Mart 2017

Birtek F ve Topal BN, 'Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti', (2023) (2), GSÜHFD 1137-1178.

Birtek F, 'Avrupa Konseyi İletişimin Denetlenmesi ve Gizli İzleme Raporu (En İyi Uygulama Mütalaası 3)' (2011) (94), Türkiye Barolar Birliği Dergisi 393-428.

Birtek F, 'Ceza Muhakemesinde Tanık Hakkında İletişimin Tespiti Koruma Tedbirine Başvurulup Başvurulamayacağı Sorunu', (2022) 17 (49), Ceza Hukuku Dergisi 189-216.

Birtek F, 'Özel Hayata Saygı- İhlal Kararı, Halford/ Birleşik Krallık Kararı' (2009) (40) Terazi Hukuk Dergisi 165-168.

Birtek F, 'Suç İşlenmesini Önleme Amacıyla İnternet veri Trafiğinin (İnternet Trafik Bilgilerinin) Tespiti', içinde Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı Adalet Yayınevi 2024)

Birtek Fatih 'İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği' (2011) (16) Ceza Hukuku Dergisi 100-148.

Canbek G ve Sağıroğlu Ş, 'Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma', (2013) 22 (1) Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi 121-136.

Canbek G, *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme* (Yayımlanmamış Yüksek Lisans Tezi YÖK Tez Merkezi 2005)

Da Silva JC, Stange A ve Birtek F, *İletişimin Denetlenmesi Tedbiri*, (1. Baskı, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği- Avrupa Konseyi Ortak Projesi Yayını, MATBAM Ajans 2014).

Değirmenci O, 'Bulut Bilişim ve Beraberinde Getireceği Hukuksal Sorunlar Üzerine Görüşler' (2017) 12 (136) Terazi Hukuk Dergisi 106-110.

Değirmenci O, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (1. Baskı, Seçkin Yayıncılık 2014).

Demirci P, 'Siber Güvenlikte Siber Gözetim: Pegasus Projesi' (2024 3 (2) İstihbarat Çalışmaları ve Araştırmaları Dergisi 175-211.

Dülger MV ve Taşkın ŞC, *Ceza Muhakemesi Hukuku* (1. Baskı, Seçkin Yayıncılık 2023)

Erdoğan Y, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri (AKSS)* (1. Bası, Legal Yayıncılık 2018).

Erdoğan Y, *Türk Ceza Kanunu'nda Bilişim Suçları* (1. Baskı, Legal Yayıncılık, 2013).

Erkan G, *Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları* (Yayınlanmamış Yüksek Lisans Tezi, YÖK Tez Merkezi 2021)

Gökcen A, Alşahin ME ve Çakır K, *Ceza Muhakemesi Hukuku* (8. Baskı, Adalet Yayınevi 2024)

Karagöz K ve Birtek F, 'İnsan Hakları Avrupa Sözleşmesi'nin 8. Maddesi Kapsamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi', (2008) III (2) Erciyes Üniversitesi Hukuk Fakültesi Dergisi 71-117.

Karakehya H, *Ceza Muhakemesi Hukuku* (6. Bası, Adalet Yayınevi 2024)

Kavruk Şenol S, *Akıllı Cihazlarda Casus Yazılımların Uygulamalı Analiz Yöntemiyle Tespiti*, (Yayınlanmamış Doktora Tezi, YÖK Tez Merkezi 2018)

Kaymaz S, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (5. Baskı, Seçkin Yayıncılık 2025).

Melemez B, 'Mesajlaşma Uygulamaları ile Bulut ve Sosyal Medya Ortamlarında Sayısal Delillerin Elde Edilmesi' (2023) (167) Türkiye Barolar Birliği Dergisi 83-132.

Meran N, *Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Takip* (1. Baskı, Adalet Yayınevi 2009).

Olgunsoy F, *Terörle Mücadelede İstihbarat Faaliyetlerinin Özgürlükler Rejimine Etkisi (Türkiye, Birleşik Krallık, Amerika Birleşik Devletleri)*, (1. Baskı, On İki Levha Yayıncılık 2020).

Özen M, *Ceza Muhakemesi Dersleri* (6. Baskı, Adalet Yayınevi 2021).

Öztürk B, Eker Kazancı B ve Güleç SS, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri* (2. Baskı, Seçkin Yayıncılık 2017).

Öztürk B, Tezcan D ve Erdem M.R, (Editörler), *Dijital Ceza Muhakemesi Hukuku* (3. Baskı, Seçkin Yayınevi 2024).

Salman B ve Yapıcı K, 'Elektronik Gözaltı Dünyası: e- Göz@altı', (2009) (436) TMMO, Elektrik Mühendisleri Odası, Elektrik Mühendisliği, 12-19.

Schroeder Friedrich- Christian ve Verrel Torsten *Ceza Muhakemesi Hukuku* (Çev Salih Oktar) (1. Baskı Yetkin 2019)

Şahin C, 'Telekomünikasyon Yoluyla İletişimin Denetlenmesi -Yargıtay Kararları Çerçevesinde Bir Değerlendirme-', (2007) XI, 1-2, Gazi Üniversitesi Hukuk Fakültesi Dergisi 1095-1112.

Şen E, 'Casus Programla Dinleme' (sen.av.tr, 7 Kasım 2015),

Şen E, *Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir* (4. Baskı, Seçkin Yayıncılık 2010).

Taşkın M, *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi* (1. Baskı, Seçkin Yayıncılık 2008).

Ünver Y ve Hakeri H, *Ceza Muhakemesi Hukuku* (24. Baskı, Adalet Yayınevi 2025).

Ünver Y ve Hakeri H, *Sorularla Ceza Muhakemesi Hukuku* (1. Baskı, TBB Yayınları 2006).

Yardımcı MM, *Amerika Birleşik Devletleri, Avrupa İnsan Hakları Mahkemesi İçtihatları ve Türk Hukukunda İletişimin Denetlenmesi*, (Yayımlanmamış Doktora Tezi, YÖK Tez Merkezi 2008).

Yemez C, 'Önleyici Kolluk Faaliyeti Kapsamında Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi', içinde Fatih Birtek (edt), *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)*, (1. Baskı, Adalet Yayınevi 2024).

Yenisey F ve Oktar S, *Alman Ceza Muhakemesi Kanunu* (2. Baskı, Beta Yayınları 2015).