DİJİTAL ÇAĞDA TÜRK CEZA MUHAKEMESİ: SİBER SUÇLAR ÖZELİNDE KORUMA TEDBİRLERİNİN GENEL TEORİSİ

TURKISH CRIMINAL PROCEDURE IN THE DIGITAL AGE: GENERAL THEORY OF PROTECTIVE MEASURES WITH SPECIAL REGARD TO CYBER CRIMES

Araştırma Makalesi

Şenel SARSIKOĞLU[*]

Kürşad Kağan ERGÜN[**]

ÖZ

Bu çalışma, dijitalleşmenin ceza muhakemesi hukukunda yol açtığı yapısal değişimleri siber suçlar özelinde ele alarak koruma tedbirlerinin mevcut kanuni çerçeve içerisinde ne derece işlevsel olduğunu incelemektedir. Günümüzde dijital/elektronik delillerin artan rolü, klasik muhakeme araçlarının yetersiz kaldığını ve özellikle Ceza Muhakemesi Kanunu (CMK) ve Polis Vazife ve Salahiyet Kanunu (PVSK) gibi mevcut yasal düzenlemelerde yer alan koruma tedbirlerinin dijital/siber ortamlara uygun şekilde güncellenmesi gerektiğini ortaya koymaktadır. Çalışmada dijital koruma tedbirleri üzerinde durularak uygulamada karşılaşılan teknik, normatif ve anayasal sorunlara değinilmektedir. Mevcut düzenlemelerin fiziksel delil esaslı olduğu, oysa dijital çağın farklı delil türleri, veri güvenliği sorunları, teknik izleme biçimleri ve bireysel hak ihlalleri gibi yeni meseleleri doğurduğu tespit edilmektedir. Yeri geldikçe Almanya, Fransa ve Amerika Birleşik Devletleri (ABD) hukuk sistemlerinden örnekler verilerek analiz yapılmakta ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları doğrultusunda ölçülülük ve denetim ilkelerine dayalı normatif bir güncellemenin gerekliliği vurgulanmaktadır. Sonuç olarak dijital delillerin güvenliği ve bireysel hakların korunması arasındaki denge gözetilerek koruma tedbirlerinin yeniden yapılandırılması önerilmektedir. Bu kapsamda koruma tedbirlerinin yeniden sınıflandırılması ve CMK'ya

DOI: 10.32957/hacettepehdf.1706831

Makalenin Geliş Tarihi: 27.05.2025 **Makalenin Kabul Tarihi:** 20.08.2025

[*] Dr., Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi

E-Posta: senellaw@hotmail.com

ORCID: 0000-0002-2204-8422

[**] Adalet Bakanlığı

E-Posta: kkaganergn@gmail.com

ORCID: 0000-0002-4943-7049

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

"Dijital Koruma Tedbirleri" başlıklı yeni bir bölüm eklenmesi gerektiğine dikkat çekilmektedir. Böylece hem bireysel hakların korunması hem de ceza adalet sisteminin etkinliğinin artırılması açısından bütüncül bir çerçeve sunulmaktadır.

Anahtar kelimeler: Ceza Muhakemesi Hukuku, Koruma Tedbirleri, Siber Suç, Dijital/Elektronik Delil, Ölçülülük İlkesi

ABSTRACT

The study examines the structural changes caused by digitalization in criminal procedure law, with a special focus on cybercrimes, and examines the extent to which protective measures are functional within the current legal framework. The increasing role of digital/electronic evidence today reveals that classical reasoning tools are inadequate and that the protective measures included in existing legal regulations especially the Code of Criminal Procedure (CPC) and the Police Duty and Authority Law (PDAL) need to be updated in accordance with digital/cyber environments. The study focuses on digital protection measures and addresses technical, normative and constitutional problems encountered in practice. It is determined that the current regulations are based on physical evidence, whereas the digital age has given rise to new issues such as different types of evidence, data security problems, technical surveillance methods and violations of individual rights. When appropriate, examples from the legal systems of Germany, France and the United States of America (USA) are given for analysis, and the necessity of a normative update based on the principles of proportionality and control in line with the jurisprudence of the European Court of Human Rights (ECHR) is emphasized. As a result, it is suggested that the protection measures should be restructured by considering the balance between the security of digital evidence and the protection of individual rights. In this context, it is emphasized that the protection measures should be reclassified and a new section titled "Digital Protection Measures" should be added to the CPC. Thus, a holistic framework is presented in terms of both protecting individual rights and increasing the effectiveness of the criminal justice system.

Keywords: Criminal Procedure Law, Protection Measures, Cybercrime, Digital/Electronic Evidence, Principle of Proportionality

EXTENDED ABSTRACT

In the digital era, criminal procedure law has been undergoing significant structural transformations driven by the increasing prevalence of cybercrimes and digital technologies. This study aims to examine the functionality and adequacy of protective measures regulated under the Turkish Code of Criminal Procedure (CPC) in addressing the complex challenges posed by cyber offenses. The research identifies a pressing

need to revise and adapt procedural safeguards to accommodate the unique nature of digital evidence and the evolving landscape of cybercriminal activities.

Cybercrimes differ fundamentally from conventional offenses in terms of spatial anonymity, technical complexity, cross-border impact, and evidentiary dynamics. As the methods of committing crimes increasingly shift into cyberspace, traditional legal mechanisms become insufficient for detecting, investigating, and prosecuting these offenses effectively. The study focuses particularly on Articles 134 and 135 of the CPC, which regulate search and seizure in digital systems and the interception of telecommunications. These provisions, originally designed for physical evidence, lack the technical precision and legal clarity necessary for managing digital evidence, creating normative gaps and practical uncertainties in the enforcement process.

The research adopts a comparative legal approach by analyzing legal frameworks and case law from Germany, France, and the United States. In particular, it highlights the German Federal Constitutional Court's recognition of the right to the confidentiality and integrity of IT systems, the U.S. Supreme Court's Carpenter v. United States decision concerning geolocation privacy, and the detailed procedural safeguards in the French Code of Criminal Procedure. Additionally, the jurisprudence of the European Court of Human Rights (ECtHR), especially decisions such as Klass v. Germany, Zakharov v. Russia, and Szabó and Vissy v. Hungary, underscore the importance of legality, foreseeability, judicial oversight, and proportionality when applying intrusive measures in the digital domain.

One of the key arguments of the study is the inadequacy of the current CCP structure in addressing the specific demands of cybercrime investigations. For example, the concept of "copying" in Article 134 fails to reflect the technical standards required for forensic duplication, such as hashing and imaging. Similarly, Article 135 does not sufficiently distinguish between content data and metadata, despite the latter's critical implications for privacy. These deficiencies hinder both the effectiveness of investigations and the protection of fundamental rights, potentially jeopardizing the fairness of criminal proceedings.

In response to these challenges, the study proposes the introduction of a new classification of protective measures tailored to digital contexts: (1) visible interventions, (2) remote interventions, and (3) in-system surveillance. Each category reflects different levels of intrusiveness and requires corresponding procedural safeguards. Visible interventions involve physical searches of digital devices, remote interventions pertain to accessing systems without the user's knowledge, and in-system surveillance refers to continuous monitoring through embedded software or technical tools. This classification aims to enhance legal predictability and guide practitioners in applying proportionate and rights-compatible measures.

Furthermore, the study recommends the inclusion of a dedicated section in the CPC titled "Digital Protective Measures" that would regulate the acquisition, preservation, and use of digital evidence with clear references to forensic protocols, data integrity standards, and judicial authorization. The objective is

to harmonize Turkish criminal procedure law with international human rights norms while ensuring the technical reliability and admissibility of digital evidence in courts.

From a methodological standpoint, the study employs qualitative legal research techniques, including doctrinal analysis, comparative evaluation, and document review. It draws on statutory texts, court decisions, academic literature, and international treaties, including the Council of Europe's Convention on Cybercrime, which Türkiye has ratified. The research identifies both normative and institutional shortcomings in the current system and proposes legislative amendments, capacity-building measures, and judicial training programs to address them.

In conclusion, the study argues that the legitimacy and effectiveness of criminal justice in the digital age depend on the timely modernization of protective measures. This modernization should not only account for technological realities but also safeguard constitutional principles such as legality, proportionality, and due process. The proposed reforms are not merely technical adjustments; they represent a fundamental recalibration of the balance between state power and individual rights in a digital society. By integrating a comprehensive, rights-based, and technically informed approach to digital protective measures, Turkish criminal procedure law can better fulfill its role in protecting both public order and personal freedoms in the face of rapidly evolving cyber threats.

GİRİŞ

Günümüzde internet teknolojilerinde yaşanan gelişmeler neticesinde toplumsal alana ilişkin her alanda önemli değişiklikler yaşanmaktadır. Bu kapsamda gündelik hayata dair iş ve işlemler kademeli olarak dijital/siber alan olarak da adlandırılabilecek internet ortamına taşınmaktadır[1]. Söz konusu dönüşüm beraberinde önemli kolaylıklar sağlamakla birlikte hukuki bir takım meseleleri, çözüm arayışlarını ve entegrasyon

[1] Mehmet Çatlı, "Yapay Zekanın Anayasası: 'Akıllı Anayasa' Üzerine" (2023) 1 (70) *Adalet Dergisi* 381. Yazar, dijitalleşme sürecinin yalnızca birey ve toplumu değil, devletin işleyişi ve hukuki yapısını da derinden etkilediğini; bu bağlamda klasik "devlet" kavramının dijital çağın gereklerine uyum arayışına girdiğini; dijital dönüşümün ise anayasal düzenlemelerden kamu hizmetine kadar birçok alanda öncelikli bir hedef haline geldiğini belirtmektedir. Bu doğrultuda, *"demokratik ceza adaletinin her çağda varolabilmesi için ceza (muhakemesi) hukukunda çok şeyin değişmesine ihtiyaç vardır."* Gerçekten de bu ideale giden yolda dijitalleşme ve yapay zeka (AI) gibi hayatımıza giren bu yeni unsurlar, suç(luluk)la mücadelede yeni bakış açılarına, arayışlara ve çözüm önerilerine yepyeni bir kapı aralamış gibi gözükmektedir. Tırnak içerisinde alıntıladığımız Prof. Dr. Faruk Erem'e ait cümleyi nakleden: Ercan Yaşar, *Maddi ve Şekli Suç Hukuku Boyutlarıyla Klasik Ceza Muhakemesine Alternatif Usuller* (1. Baskı, Seçkin Yayıncılık 2022) 5. Hal böyleyken klasik suçların önemli bir kısmının aydınlatılmasında dijital materyallerden yararlanılması da kaçınılmaz bir hal almaktadır. Murat Volkan Dülger, *Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri (Search, Copy and Seizure Measures on Information Systems)* (24 Şubat 2021) 5 http://dx.doi.org/10.2139/ssrn.3792260

ihtiyaçlarını da beraberinde getirmektedir. Mukayeseli hukuk sistemleri incelendiğinde yargı süreçlerinde dijitalleşmenin öncelikli gündem maddelerinden biri haline geldiği ve bu dönüşümü destekleyen altyapı çalışmalarının hızla devam ettiği gözlemlenmektedir[2]. Anılan süreçte klasik hukuki kavram ve kurumların yeni meselelerin çözümünü içerir biçimde yeniden tanımlanması ve ihtiyaçlara binaen yeni kavramların üretilmesi gerekliliği ortadadır.

Bir bütün olarak ceza (muhakemesi) hukuku toplumsal düzenin korunması, suçun önlenmesi, suçluların topluma geri kazandırılması ve mağdurların zararının tazmin edilmesi gibi konularda belirleyici olmaktadır. Önceki paragrafta zikredilen dijitalleşme öncesi dönemde ceza hukuku kapsamında suç olarak tanımlanan fiiller, esas itibarıyla failin doğrudan fiziki eylemleriyle vücut bulmakta; bu fiillere karşı alınan önleyici tedbirler ve soruşturma işlemleri ise yetkili birimlerin yine fiziki müdahaleleriyle icra edilebilmekteydi[3]. Diğer bir ifadeyle hırsızlık suçunun faili, suçun konusunu oluşturan eşyayı fiziki hareketlerle zilyedinin rızası dışında almakta, mala zarar verme suçunun faili suçun konusunu oluşturan eşyaya fiziki müdahaleyle zarar verebilmekte, hakaret veya tehdit suçunun faili de suçu oluşturan eylemi ya da beyanı fiziki hareketlerle ika etmekteydi. Benzer şekilde önleyici ve soruşturmacı birimler de suçun önlenmesi,

---

[2] Bahri Öztürk, Durmuş Tezcan ve Mustafa Ruhan Erdem (eds), *Dijital Ceza Muhakemesi Hukuku* (3. Baskı, Seçkin Yayıncılık 2024) 233; Candide Şentürk, "Ceza Muhakemesi Hukuku Özelinde Yargıda Dijitalleşme" (2021) 25 (2) *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 755. Bu kapsamda e-duruşma sistemleri, dijital/elektronik dava dosyaları, uzaktan tanıklık, yapay zeka destekli yargı karar destek sistemleri gibi teknolojiler ceza muhakemesinin işleyişine entegre edilmektedir. Bu noktada ifade edelim ki kanaatimizce dijitalleşme kavramı, yalnızca teknolojik altyapının geliştirilmesine yönelik bir modernleşme hamlesinin de ötesinde yargı sisteminin şeffaflık, hesap verebilirlik ve insan haklarına dayalı işleyiş ilkeleriyle uyumlu hale getirilmesinde temel bir araç niteliğindedir. Dijitalleşme olgusu da ceza muhakemesi bağlamında temel hak ve özgürlüklerin tanınıp güvence altına alınması yönündeki normatif hassasiyetin daha keskin biçimde tezahür ettiği bir kırılma noktası olarak ortaya çıkmaktadır.

[3] Yeni teknik gelişmelerin yeni bilgi edinme ve değerlendirme biçimlerini ortaya çıkardığı, özellikle veri analizi yöntemiyle bilgi edinme ve değerlendirme imkanlarının ceza muhakemesinde kullanılmaya başlanıldığı belirtilmektedir. Friedrich-Christian Schroeder and Torsten Verrel, *Ceza Muhakemesi Hukuku* (tr Salih Oktar, 1. Baskı, Yetkin Yayınları 2019) 96. Nitekim olay yeri birçok suç bakımından fiziki bir alan olmaktan çıkıp sayılardan oluşan siber bir alana dönüştüğünden artık dijital/elektronik delillerin sadece siber suçlarla ilgili olmadığı da ifade edilmektedir. Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku El Kitabı,* (7. Baskı, Beta Yayıncılık 2021) 228. Bununla beraber, yargıda yapay zeka kullanımının da başlamasıyla artan düzeyde etik kaygılar baş göstermiş ve birçok uluslararası ve uluslarüstü kuruluş, devletlerin resmi organları, sivil toplum örgütleri veya uzman gruplar tarafından neticeleri itibariyle birbirine yakın etik ilkeler ileri sürülmüştür. Ayrıntılı açıklamalar için bkz. Oğuzhan Sapan, *Ceza Muhakemesinde Yapay Zeka Kullanımı* (1. Baskı, Adalet Yayınevi 2024) 60.

faillerin tespiti ve delillerin temini süreçlerini doğrudan fiziki müdahaleler yoluyla gerçekleştirmekteydi. Suçun önlenmesine, tespitine, soruşturulması ve kovuşturulmasına ilişkin olarak düzenlenen ceza (muhakemesi) kanunları da anılan fiziksel ortamın gereklilikleri göz önünde bulundurularak düzenlenmişti. Dönüşüm sonrası gelinen aşamada ise suç oluşturan eylemler ve suç araçları da dijital/siber alana taşınmış ve bu alana özgü suç tipleri türemiştir. Siber suçların sınır ötesi nitelikleri göz önüne alındığında bu fiillerin işlenme biçimi, gerçekleştiği yer ve zaman ile ortaya çıkardığı zarar ya da tehlike; çoğu durumda birden fazla ülkenin yetki alanını ilgilendiren kapsamlı bir soruşturma ve kovuşturma sürecini beraberinde getirmektedir. Bu bağlamda CMK ve PVSK gibi ilgili kanuni düzenlemelerin suçun önlenmesi, soruşturulması ve kovuşturulması açısından teorik ve pratik yeterlilikleri sorgulanmakta ve mevcut düzenlemeler dijital/siber alanın dinamik yapısının da bir gereği olarak her an bünyelerinde güncellenme potansiyeli taşımaktadır.

Bu çalışma, Ceza Muhakemesi Kanunu'ndaki koruma tedbirlerinin dijital çağın gereklerine uygun biçimde yeniden yapılandırılması gerektiği düşüncesiyle hazırlanmıştır. Çalışmada ceza muhakemesinin amacı çerçevesinde dönüşen suç tipleri, suç işleme araçları ve yöntemleri dijital/siber alan özelinde ve koruma tedbirleri kapsamında analiz edilmiştir. Yapılan analizle mevcut CMK'da düzenlenen koruma tedbirlerinin yetersiz kaldığı noktalar tespit edilmiş, ihtiyaç duyulan güncellemeler belirtilmiş ve çözüm önerileri geliştirilmiştir.

Çalışmada öncelikle dijital/siber alana ilişkin temel kavramlarla siber suç ve koruma tedbirlerinin tanımı yapılmış, ardından CMK ve PVSK kapsamındaki mevcut düzenlemeler ile bu düzenlemelerin uygulamadaki sorunları değerlendirilmiştir. Özellikle mobil cihazlar ve kişisel veri yoğunluğu sebebiyle yaşanan ölçülülük ve denetlenebilirlik sorunlarına odaklanılmış, PVSK ek madde 6'nın Anayasa Mahkemesi (AYM) tarafından iptali bu bağlamda incelenmiştir.

Çalışmanın içerisinde yeri geldikçe Almanya, Fransa ve ABD gibi ülkelerin konuya yaklaşımları ile AİHM içtihatlarına yer verilerek hem teorik hem normatif açıdan karşılaştırmalı örneklerden yararlanılmıştır. Son olarak ise mevcut sorunlara yönelik çözüm önerileri geliştirilmiş ve müdahale türlerinin sınıflandırılması, CMK'ya yeni bir

"dijital koruma tedbirleri" bölümü eklenmesi ile yargısal denetimin güçlendirilmesi önerilmiştir.

Çalışma, mevcut bir probleme ilişkin teorik ve normatif çözüm önerileri sunar özelliği nedeniyle nitel araştırma durumunda olup bu nedenle çalışmada nitel araştırma yöntemlerinden faydalanılmıştır. Mevcut hukuki düzenlemeler, teorik eserler ve mahkeme kararlarının incelenmiş olması karşısında doküman inceleme ve metin analizi teknikleri kullanılmıştır. Çalışmanın yeni bir düzenleme öneriyor olması karşısında güncellenmeye ilişkin önerilere örnek teşkil edebilecek teorik ve pratik kaynakların bulunmaması veya sayıca azlığı ise sınırlılık olarak tespit edilmiştir.

I. DİJİTAL ÇAĞDA SİBER SUÇLAR VE KORUMA TEDBİRLERİ

A. Siber Suç Kavramı, Özellikleri ve Ceza (Muhakemesi) Hukukuna Etkisi

Ulusal ve uluslararası hukuk düzenlemelerine bakıldığında siber suç kavramının tanımı yapılmak yerine, bu alanda işlenen eylemlerin çeşitliliği göz önüne alınarak ve kanunilik ilkesi çerçevesinde suç teşkil eden fiillerin tek tek tanımlandığı görülmektedir[4]. Bununla birlikte, esasen siber sistemlere ve burada yer alan verilere karşı yine bu sistemler kullanılarak ika edilen suçların bazı özel bilgi, beceri ve deneyim sahibi faillerce gerçekleştirilmesi, siber suçların üst seviye niteliğini ve teknolojinin sürekli gelişimi karşısında yeni işleniş biçimlerini ortaya koymaktadır. Bu nedenle siber suçların birçok tanımının yapıldığı görülmektedir[5]. Öğretide ve uygulamada genel kabul gören

[4] Doktrinde siber suç kavramını ifade etmek üzere "bilişim suçu", "dijital suç", "elektronik suç", "e-suç", "bilgi çağı suçu", "yüksek teknoloji suçu", "sibernetik suç", "bilişim alanında suç", "bilgisayar suçu", "internet suçu" ve "internet alanında suç" gibi çeşitli kavramlar zaman zaman birbirinin yerine kullanılmaktadır. Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları" (1994) 49 (3) *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* 158; Regner Sabillon, Jeimy Cano, Victor Cavaller and Jordi Serra, "Cybercrime and Cybercriminals: A Comprehensive Study" (2016) 4 (6) *International Journal of Computer Networks and Communications Security* 165 https://www.proquest.com/scholarly-journals/cybercrime-cybercriminals-comprehensive-study/docview/1874038161/se-2?accountid=15875 Ancak biz, çalışmamızda uluslararası terminolojide daha yaygın biçimde tercih edilen "siber suç" kavramını esas almaktayız.

[5] Tanımlama sorunlarına hakkında ayrıntılı açıklamlar için bkz. Ulrich Sieber, *İnternetteki Suçlar ve Suçun İnternette Takibi* (Editör: Yener Ünver, 1. Baskı, Seçkin Yayıncılık 2014) 23. Bu tanım ve kapsam sorunları sebebiyle siber suçlara "çizgisiz çerçeveli suç" da denilmektedir. Hüseyin Akarslan, *Bilişim Suçları* (2. Baskı, Seçkin Yayıncılık 2015) 36. Mesela, dijital verilerin ve hesap erişim bilgilerinin kötüye kullanımı klasik dolandırıcılık veya hırsızlık suçlarının unsurlarını taşımamakta olup suç tipleri ve tanımları değişirken dijital çağda koruma tedbirlerinin uygulanma kriterleri de farklılaşmaktadır. Örnekler için bkz. Muammer Ketizmen, "İnternet Bankacılığı Aracılığıyla Başkalarının Hesaplarında

yaklaşıma göre; siber suçlar bilişim sistemlerinin kendisine ya da bu sistemlerin içerdiği verilere ilişkin olarak yine bu sistemler kullanılarak işlenen hukuka aykırı fiiller bütünüdür[6]. Bize göre, siber alandaki gelişime ve teknolojik yeniliklere cevap verme kabiliyetini haiz ve dolayısıyla ilk defa ortaya çıkabilecek yepyeni davranış modellerini de kapsamına alabilecek bir tanımlama yapma perspektifiyle hareket edilmelidir[7]. Nitekim siber suçların tanımı ve takibi açısından temel bir referans niteliği taşıyan, Avrupa Konseyi tarafından 2001 yılında kabul edilen ve Türkiye'nin de taraf devlet olarak yer aldığı "Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)" siber suçları dört ana kategori altında tanımlamaktadır[8].

Bununla birlikte an itibariyle sırf işlenişinde siber sistemler kullanıldığı için fiili de siber suç kabul eden genişlikte bir tanım yapmaktan kaçınmak adına ve bir başlangıç noktası olmak üzere Türk Ceza Kanunu (TCK) çerçevesinde üçlü tasniften yararlanabileceğini düşünmekteyiz. Buna göre; ilk katalogda siber sistemlerin sadece suçun işlenmesinde bir araç olarak kullanıldığı fakat suçun unsurunu oluşturmadığı suçlar, ikinci katalogda siber sistemlerin kullanılmasını nitelikli hal olarak kabul eden suçlar ve son katalogda siber sistemlere ve buralarda yer alan verilere karşı işlenen suçlar yer almaktadır. Bu yaklaşım sayesinde siber suçları dar ve geniş olmak üzere iki farklı perspektiften ele alma imkanı bulunmaktadır. Geniş anlamda siber suç, sayılan üç kataloğu da içine alan yani hem siber sistemler kullanılarak işlenen hem de siber

Usulsüz İşlemler Yapılması Suretiyle Yarar Sağlanmasında Suçun Mağduru" (2024) 4 (2) *Kırıkkale Hukuk Mecmuası* 1004.

6 Ömer Demirci, *Bilişim Suçları ve Soruşturma Yöntemleri* (1. Baskı, Seçkin Yayıncılık 2022) 23; Didem Yeldan, *Siber Suçlar* (2. Baskı, Seçkin Yayıncılık 2023) 39; Sacit Yılmaz, *Türk Ceza Hukuku Sisteminde Siber Suçlar* (2. Baskı, Adalet Yayınevi 2023) 6; Durmuş Tezcan, Mustafa Ruhan Erdem ve R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku* (22. Baskı, Seçkin Yayıncılık 2024) 1008.

7 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (10. Baskı, Seçkin Yayıncılık 2023) 82. Yazar, gelişen teknoloji ve yeni suç işleme modellerinin suç tipleri arasındaki ayrımı güçleştirdiğini ve geniş tanım yapılmasından kaçınılması gerektiğini ifade etmektedir. Ancak, doktrinde yaşadığımız bu modern çağda dijital bir boyutu bulunmayan herhangi bir suçu hayal etmenin zor olduğu da haklı olarak belirtilmektedir. Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Elsevier 2011) 3.

8 Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar *(mesela, 2'nci madde-yetkisiz erişim, 4'üncü madde-veri müdahalesi)*; içerik kaynaklı suçlar *(mesela, 9'uncu madde-çocuk pornografisiyle ilgili suçlar)*; bilişim yoluyla işlenen klasik suçlar *(mesela, 8'inci madde-bilgisayarla ilgili dolandırıcılık)* ve usul hukukuna ilişkin hükümlerle bağlantılı suçlar *(mesela, 10'uncu madde-telif hakkı ihlaliyle ilgili suçlar)*. 2001 tarihli *"Avrupa Konseyi Siber Suç Sözleşmesi (Convention on Cybercrime)"* https://rm.coe.int/1680081561

sistemlere karşı işlenen suçlardır. Dar anlamda siber suç ise yalnızca siber sistemlere ve buralarda yer alan verilere karşı işlenen suçlardır. Biz, siber suçlar özelinde koruma tedbirlerine ilişkin bir genel çerçeve sunulurken geniş anlamda siber suç kavramından hareket etmekteyiz. Nitekim içinde yaşadığımız dijital çağda siber sistemlerle ilişkilendirilemeyen neredeyse hiçbir hukuki değer ya da bu değerlere karşı işlenen suç kalmamış; ceza (muhakemesi) mevzuatının korumayı amaçladığı hemen her alan doğrudan ya da dolaylı biçimde siber sistemlerle temas eder hale gelmiştir[9].

Bu bakımdan siber uzay kavramı dijital bir ekosistemi, yeni nesil internet ve ağ uygulamalarını temsil eden, etkileşim kurabilen, kendi kendini organize edebilen, gelişebilen ve uyum sağlayabilen tamamen yeni bir dağıtılmış ve açık sistem dünyası vaat eden bir yeni sınır olarak kabul edilmektedir. Günümüzde bireyler, sivil toplum kuruluşları, hükümet ve devlet kurumları da dahil olmak üzere ülkelerin her düzeydeki idari, ticari, ekonomik, sosyal ve kültürel faaliyetleri ile alışverişlerinin çoğu siber uzayda gerçekleştirilmektedir. Ayrıca ülkelerin ve grupların karşı karşıya olduğu zorlukların ve çatışmaların çoğu siber uzayı içermektedir. Çünkü küresel ölçekte hiçbir sektör siber savaşın etkilerinden muaf olmayıp küresel çok uluslu şirketlerden her düzeydeki hükümet kurumlarına, büyük kuruluşlardan kritik altyapı sağlayıcılarına kadar tüm sektörler merkezleri nerede olursa olsun veya hangi ülkeden olurlarsa olsunlar siber suç(lu)ların etki alanına girmektedir[10]. Zaman içinde bu konudaki siber saldırıları yönlendiren motivasyon, ün peşinde koşmaktan kar elde etme veya politik kazanım peşinde koşmaya kaymış ve bu da çeşitli ölçeklerde siber terörizme yol açmıştır. Mesela, 2010 haziranında keşfedilen ve İran ülkesinin nükleer programına yönelik yönlendirilmiş bir saldırı olan Stuxnet, siber savaşta bir dönüm noktasını temsil etmiş ve saldırı stratejisindeki karmaşıklığı nedeniyle siber saldırıları analiz etme ve anlama konusunda yeni bir eşik

9 Centel ve Zafer (n3) 228; Dülger (n7) 83.

10 Ravi Chandra and P. W. C. Prasad, "Cyber Warfare: Challenges Posed in a Digitally Connected World: A Review" in Subhas Chandra Mukhopadhyay, S.M. Namal Arosha Senanayake and P. W. Chandana Withana (eds), *Innovative Technologies in Intelligent Systems and Industrial Applications* (Lecture Notes in Electrical Engineering, vol 1029, Springer 2023) https://doi.org/10.1007/978-3-031-29078-7_16

oluşturmuştur[11]. Ayrıca tipik bir siber suç olarak siber dolandırıcılık, kişilerin mülkiyet hakkı kadar toplumsal güvenlik bakımından da ciddi tehditler oluşturmaktadır. Geleneksel kriminolojik teoriler, özünde bireysel özelliklerin siber suç mağduriyeti üzerindeki etkilerine odaklanmakla beraber makro düzeydeki çevresel faktörlerin etkilerini göz ardı etmektedir. Mesela, Çin'de yapılan çalışmalar siber dolandırıcılığın dağılımının bölgesel ekonomi ve nüfus yapısından önemli ölçüde etkilendiğini göstermektedir[12]. Yine COVID-19 salgını da sosyo-ekonomik faaliyetleri önemli ölçüde değiştirmiş ve potansiyel olarak suç modellerinde değişikliklere neden olmuştur. Mesela, İngiltere'de polis kayıtlarına geçen dolandırıcılık ve siber bağlantılı suçlara ilişkin belirlenen örüntülerin öncelikle sosyo-ekonomik faktörler ile ardından hükümetin sınırlama önlemleri ve hareketlilik faktörleriyle ilişkili olduğu görülmektedir[13]. Gelişmekte olan ekonomilerdeki insanların çoğu da yüksek işsizlik ve düşük ücretler nedeniyle her geçen gün siber suçlara çekilmekte[14] ve fail ya da mağdur olarak siber suçlarla ilişkili hale gelmektedir.

Ayrıca dijitalleşmenin etkisiyle suçun işleniş biçimleri mekan ve zaman sınırlarını aşarak sanal ortamlara taşınmış; böylece yalnızca fiziki müdahalelere dayalı geleneksel yöntemler yetersiz hale gelmiştir. Modern toplumda suçlulukla mücadele edilebilmesi artık konvansiyonel koruma tedbirlerinin teknoloji ile uyumlu hale getirilmiş çeşitlerinin varlığını gerektirmekte[15] olup delil toplama, fail tespiti ve suçun önlenmesi gibi temel faaliyetler artık dijital iz sürme, elektronik veri analizi ve siber güvenlik teknikleri gibi yöntemleri zorunlu kılmaktadır. Bu dönüşüm, ceza muhakemesi hukukunun müdahale

---

[11] Haitao Du and Shanchieh Jay Yang, "Temporal and Spatial Analyses for Large-Scale Cyber Attacks" in V. S. Subrahmanian (ed), *Handbook of Computational Approaches to Counterterrorism* (Springer, 2013) 559 https://doi.org/10.1007/978-1-4614-5311-6_25

[12] Shuai Chen and others, "The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China" (2021) 10 (12) *ISPRS International Journal of Geo-Information* 802 https://doi.org/10.3390/ijgi10120802

[13] Jun Zhuo and others, "The Spatiotemporal Patterns and Driving Factors of Cybercrime in the UK during the COVID-19 Pandemic" (2024) 11 *Humanities and Social Sciences Communications* 1525 https://doi.org/10.1057/s41599-024-04051-9

[14] Nir Kshetri, "Diffusion and Effects of Cyber-Crime in Developing Economies" (2010) 31 (7) *Third World Quarterly* 1057 https://doi.org/10.1080/01436597.2010.518752

[15] Candide Şentürk Akaner, *Bir Koruma Tedbiri Olarak Online Arama ve Türk Hukukunda Uygulanabilirliği* (1. Baskı, Seçkin Yayıncılık 2022) 5.

araçlarında da köklü bir değişimi beraberinde getirmiştir. Bununla birlikte mevcut hukuki altyapı, literatürde "normatif gecikme (norm lag)"[16] veya "normatif boşluk (norm gap)" olarak adlandırılabilecek[17] bir olguya işaret etmekte ve teknolojik gelişmelerin hızına uyum sağlamakta zaman zaman yetersiz kalmaktadır. Ceza (muhakemesi) hukuku mevzuatı, dijital ortamların kendine özgü dinamiklerini ve yeni suç örüntülerini kapsamakta güçlük çekmekte; bu durum da koruma tedbirlerinin etkinliğini, bireysel hakların korunmasını ve adil yargılanma ilkeleriyle uyumlu şekilde sürdürülmesini tehdit etmektedir[18]. Zira çevrimiçi (online) hukuk çevrimdışı (offline) hukuktan müstakil bir alan olmayıp ceza muhakemesine yönelik eylem ve işlemleriyle insan haklarını ihlal etme potansiyeli olan devlet mekanizması, bu süreçte insan haklarını korumak ve adil yargılanmayı sağlamaktan sorumlu yine tek aktör olarak karşımıza çıkmaktadır. Bu doğrultuda dijital çağın gereklerine uygun biçimde hem özelde koruma tedbirlerinin hem de genelde ceza muhakemesi mekanizmalarının yeniden yapılandırılması gerekliliği açık biçimde ortaya çıkmaktadır.

---

[16] Bu durum, William F. Ogburn'un 1922 yılında "Social Change with Respect to Culture and Original Nature" adlı eserinde ortaya koyduğu "kültürel gecikme" (cultural lag) kavramıyla açıklanmaktadır. Ogburn'a göre; maddi kültürdeki (teknoloji gibi) hızlı değişimler, manevi kültürün (normlar, yasalar, değerler) uyum sağlama sürecinden daha hızlı gerçekleşmekte ve bu da toplumsal uyumsuzluklara yol açmaktadır. Abbott P. Herman, "An Answer to Criticisms of the Lag Concept" (1937) 43 (3) *American Journal of Sociology* 440 https://www.jstor.org/stable/2768630

[17] Benoît Godin, "Innovation Without the Word: William F. Ogburn's Contribution to the Study of Technological Innovation" (2010) 48 (3) *Minerva* 277 https://www.jstor.org/stable/41821527

[18] *"Sanıklara isnat edilen eylemlerin esas olarak bilgisayar programlarıyla oluşturulmuş belgelere (CD, DVD, flash bellek, harici disk gibi) dayanması, ... bu verilerin müdahale edilebilir nitelikte olduğunun belirtilmiş olması, ... Başvurucunun, dijital delillerin içindeki belgelerin kendisi tarafından oluşturulmadığı ve temin edilmemiş olduğu iddiası karşısında ... başvurucuların, kendilerine yöneltilen suçlamaların dayanağı olan delillere karşı savunma yapma imkânı ve kovuşturmanın genişletilmesini isteme hakkı kısıtlanmış, ceza yargılamasının, maddi gerçeğin ortaya çıkartılması amacına yönelik olarak 'silahların eşitliği' ilkesi ihlal edilmiştir. ... Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkının ihlal edildiğine karar verilmesi gerekir."* Anayasa Mahkemesi, *Yankı Bağcıoğlu ve Diğerleri* (2014/253, R.G. 12/5/2015-29353) https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/253 Ayrıca silahların eşitliği ilkesi hakkında bkz. Akif Yıldırım ve Ayhan Kılıç, "Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Silahların Eşitliği İlkesi" (2021) 9 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 350.

B. Koruma Tedbiri Kavramı, Amaçları ve Denge Modeli

Koruma tedbirleri, soruşturma veya kovuşturma evrelerinde maddi gerçeğin (hakikatin) ortaya çıkarılmasını ya da verilecek hükmün infaz edilebilmesini temin maksadıyla henüz hüküm verilmemişken temel bir hakkın sınırlanması yoluyla uygulanan geçici, gecikemez ve çoğunlukla hakim kararına dayanan tedbirleri ifade etmektedir[19]. Bu yönüyle de önleyici tedbirlerden ayrılmaktadır[20]. Dolayısıyla bu tedbirler, henüz muhakemenin sonlanmadığı bir evrede anayasal düzeyde güvence altına alınan temel hak ve hürriyetlere geçici olarak müdahaleyi mümkün kılmaktadır[21]. Bununla birlikte mevzu bahis müdahalenin meşru olabilmesi için görünüşte haklılık, zorunluluk, ölçülülük ve geçicilik gibi birtakım prensiplere sıkı sıkıya riayet edilmesi gerekmektedir. Hangi tedbirin uygulanacağına ilişkin kararlar, yalnızca kanunla belirlenmiş makamlar tarafından ve açık kanuni dayanaklara istinaden verilmektedir. Tedbirin sınırlandırdığı hak ile korumayı amaçladığı yarar arasında adil bir denge gözetmesi zorunluluk arz etmektedir[22]. Bu çerçevede koruma tedbirleri birer amaç değil, araç niteliği taşımakta olup yalnızca ve yalnızca muhakeme sürecini mümkün kılacak ölçüde uygulanmaları hukuken meşru kabul edilebilmektedir[23].

Güvenlik ve özgürlük kavramları, ceza muhakemesi hukukunun temelinde yer alan iki esas değer olarak karşımıza çıkmaktadır. Fakat bu iki değer çoğu zaman birbirine

---

[19] Bahri Öztürk, Behiye Eker Kazancı ve Sesim Soyer Güleç, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri* (5. Baskı, Seçkin Yayıncılık 2022) 29; Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Ceza Muhakemesi Hukuku* (17. Baskı, Seçkin Yayıncılık 2024) 232; Ahmet Gökcen, M. Emin Alşahin ve Kerim Çakır, *Ceza Muhakemesi Hukuku* (8. Baskı, Adalet Yayınevi 2024) 287.

[20] Feridun Yenisey ve Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku,* (12. Baskı, Seçkin Yayıncılık 2024) 293. Yazarlar, tehlike tedbirlerinin iki türde olduğunu; ilk olarak, uzak tehlikeyi önlemeye çalışan tedbirlere "önleme tedbirleri" ikinci olarak, tehlike yakın ve önlemek için geçse ve tehlikeli neticeden kendimizi koruyabiliyorsak bu tedbirlere de "koruma tedbirleri" dendiğini ifade etmektedir.

[21] Öztürk, Tezcan ve Erdem (n2) 452; Murat Volkan Dülger ve Şaban Cankat Taşkın, *Ceza Muhakemesi Hukuku* (2. Baskı, Seçkin Yayıncılık 2024) 336. Son yazarlar, koruma tedbirlerinin aynı zamanda birer delil elde etme yöntemi niteliğinde olduğunu haklı olarak belirtmektedir.

[22] Veli Özer Özbek, *Polis Hukuku, İnternet Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler ve Hukuka Aykırı Müdahalelere Karşı Korunma Çareleri,* (2. Baskı, Seçkin Yayıncılık 2023) 7. Yazar, demokratik hukuk devleti ilkesinin ancak özgürlük ve güvenlik dengesinin sağlandığı bir ülkede hayata geçirilebileceğini ve bu manada özgürlük ve güvenlik arasında "çatışmanın" "işbirliğine" dönüşmesi yönündeki haklı bir idealden bahsetmektedir.

[23] Cumhur Şahin ve Neslihan Göktürk, *Ceza Muhakemesi Hukuku,* (15. Baskı, Seçkin Yayıncılık 2024) 287.

karşıt yönde vuku bulan gerilimlere sahne olmakta ve bilhassa koruma tedbirlerinin uygulanmasında biri lehine yapılan tercihler diğerinin zedelenmesi riskini barındırmaktadır[24]. Dijital veri işleme, teknolojik gelişmeler, küreselleşme ve ortaya çıkan yeni tehditler, güvenlik ile özgürlük arasındaki dengeyi daha da hassas hale getirmekte olup günümüzde bu bağlamda sıkça sorulan sorulardan biri, artık "özgürlük yerine güvenlik mi?" şeklinde olmaktadır[25]. Siber uzayın sınır aşan, anonimliğe imkan veren ve teknik olarak denetimi güç karakteri de nazarı dikkate alındığında ceza muhakemesi süreçlerinde bu dengeyi kurmak çok daha çetrefilli bir hal almaktadır[26]. Ez cümle koruma tedbirlerinin uygulanmasında dikkate alınması gereken "denge teorisi" yalnızca kağıt üzerinde şahsi haklar ile kamu düzeni arasında soyut bir denge (güvenlik-özgürlük dengesi) kurmakla yetinmemeli, bununla beraber müdahalenin demokratik bir hukuk devletinde[27] keyfiliğe yol açmaksızın, kanunilik, ölçülülük[28] ve yargısal denetim prensipleriyle somutlaşan işlevsel bir modele dönüşmesine imkan sağlamalıdır.

II. MEVCUT YASAL DÜZENLEMELER

CMK'da yer alan temel koruma tedbirleri, ceza muhakemesinin amacına ulaşabilmesi için kişilerin belirli hak ve özgürlüklerine geçici olarak müdahale imkanı sağlamaktadır. Bu tedbirler, genellikle CMK'nın 1'nci kitabının 4'üncü kısmında yer almakta olup her bir koruma tedbiri belli koşullar altında ve ölçülülük

---

[24] Sohyun Park, *Der Schutz personenbezogener Daten im Strafverfahren: Eine rechtsvergleichende Untersuchung zum deutschen und US-amerikanischen Recht* (1st edn, Nomos 2021) 35. Yazar, kişisel verilerin geniş çapta toplanması ve analiz edilmesinin her ne kadar gelecekte işlenebilecek suçların önlenmesi ya da mevcut suçların etkin şekilde soruşturulması amacıyla yapılsa da bu tür devlet uygulamalarının bireylerin mahremiyetine ciddi biçimde müdahale edilmesi riskini de beraberinde getirmekte olduğunu ifade etmektedir.

[25] Park (n24) 35.

[26] Nezir Akyeşilmen, "Siber Uzay ve İnsan Hakları: Dijital Çağda İnsan Haklarını Korumak" *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik* (1. Baskı, Orion Kitabevi 2018) 291.

[27] İbrahim Şahbaz, "Koruma Tedbiri Olarak İletişimin Denetlenmesi" in Süheyl Donay ve Aysun Altunkaş (eds), *Ceza Yargılama Hukukunda Son Gelişmeler Sempozyumu* (1. Baskı, Seçkin Yayıncılık 2016) 27. Yazar, koruma tedbirlerinin demokratik hukuk devleti kuralları çerçevesinde değerlendirilmesi gerektiğini belirtmektedir. Böylece yargı organının hukuk devleti veya hukukun üstünlüğü ile evrensel insan hakları standartlarını esas alarak görev yapması mümkün olacaktır.

[28] Ölçülü olmak, esasında aşırıya kaçmamak demektir. Bu sebeple anılan ilke dahilinde "aşırılık yasağı" geliştirilmiştir. Uygulanan tedbirlerin temel hak ve özgürlükler bakımından aşırıya kaçmaması elzem niteliktedir. Özbek (n22) 41.

(elverişlilik/Eignung, gereklilik/Erforderlichkeit ve oranlılık/Proportionalität)[29] ilkesine uygun biçimde uygulanmak zorundadır. Bu bağlamda yakalama ve gözaltı (m. 90-99) kişinin kısa süreli olarak özgürlüğünden yoksun kalmasına yol açarken; tutuklama (m. 100-108) daha ağır şartlar altında uygulanmakta ve kuvvetli suç şüphesinin yanında kaçma ve delil yoketme gibi nedenlerin varlığını gerektirmektedir. Ayrıca arama (m. 116-122) ve elkoyma (m. 123-132) ise delil elde edilmesi maksadıyla kişi haklarına müdahale oluşturan diğer önemli tedbirler olarak karşımıza çıkmaktadır. Her şeyden önce bilişim sistemlerinden delil elde edilmesine yönelik işlemler CMK 134'üncü maddesinde özel olarak düzenlenmektedir. Bu hüküm, dijital/elektronik delillerin nitelik farklılığı sebebiyle istisnai bir konuma sahip bulunmaktadır. Yine telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (m. 135) ve gizli soruşturmacı görevlendirilmesi (m. 139) gibi tedbirler, bilhassa dijital iletişim kanallarını kullanan örgütsel yapılarla mücadelede önemli roller üstlenmektedir. Özellikle "gizli" nitelikteki müdahalelere ilişkin bu yeni hükümler, koruma tedbirlerini hukuk devleti ilkesi bakımından incelenmesi zor bir noktaya taşımaktadır[30]. Ancak biz, bu durumun yeni meselelere çözüm önerileri oluştururken ve bilhassa koruma tedbirlerinin mevcut paradigması yeniden oluşturulurken tanımlama, sınıflandırma ve ortak özelliklerinin belirlenmesinde kritik birer malzeme teşkil ettiğini düşünmekteyiz.

İfade edelim ki bu tedbirlerin kahir ekseriyeti, geleneksel suç tipleri için geliştirilmiş olmakla birlikte siber suçların kendine has özellikleri bu tedbirlerin uygulanabilirliği ve etkinliğini sınırlayabilmektedir. Zira siber suçların sınır aşan yönleri, faillerin siber alanda anonim hale gelebilmeleri, veri bütünlüğüne yönelik hızlı tahrip riskleri ve yüksek düzeyde teknik bilgi ihtiyacı gibi kısıtlar, yukarıda sayılan klasik ceza muhakemesi tedbirlerinin yeniden yapılandırılmasını gerektirmektedir. Buna misal olarak, CMK 116'ncı maddesinde öngörülen fiziki alana ilişkin arama hükümlerinin siber

[29] Koruma tedbirlerinin keyfi ya da ihtiyaten değil, sadece soruşturma amaçları bakımından gerekli olduğu ölçüde uygulanabileceği Avrupa hukuk sistemlerinde açıkça kabul edilmektedir. Christian Bertel and Andreas Venier, *Einführung in die neue Strafprozessordnung* (2nd edn, Springer 2006) 73; Uwe Hellmann, *Strafprozessrecht* (2nd edn, Springer 2006) 74. Son yazar, temel hakları kısıtlayan tedbirlerin alınması veya emredilmesi için aranan kabul edilebilirlik şartı olarak ölçülülük ilkesinden bahsetmektedir. Buna göre; somut bir olayda belli bir koruma tedbirinin koşullarının varlığına rağmen ölçülülük ilkesine uyulmamışsa o koruma tedbirinin de kabul edilemez olduğu sonucuna varılacaktır.

[30] Schroeder and Verrel (n3) 96.

ortamlardaki veri aramalarına uygulanması noktasında ciddi belirsizlikler bulunmakta; dijital verinin neresinin "arama"ya konu teşkil ettiği ve "özel hayat" ile "delil" arasındaki çizginin nasıl tespit edileceği hususlarında doktrinde tartışmalar bulunmaktadır[31]. Aynı şekilde, CMK 134'üncü maddesi kapsamında yapılan dijital elkoymalarda, verilerin kopyalanmasıyla orijinallerinin sistemde kalmasının olası delil bozulmalarına yol açabileceği, bu sebeple devletin adil yargılama görevi ve delillerin güvenliğinin sağlanması açısından teknik ve kanuni standartların belirlenmesi gerektiği ifade edilmelidir[32]. Kısacası CMK'daki yer alan temel koruma tedbirleri bakımından mevcut hukuki çerçeve siber suçların doğasına tam olarak cevap verememekte ve yapısal olarak halen fiziksel delil esaslı klasik suçlarla mücadeleye göre şekillenmektedir. Ancak siber suçların çetrefilli yapısı ve teknolojik boyutu karşısında bu tedbirlerin gerek normatif gerek uygulama yönüyle yeniden değerlendirilmesi gerekmektedir. Kanuni altyapının güçlendirilmesi, uygulamacılar bakımından teknik kapasitenin artırılması ve muhakkak dijital/elektronik delillere has usuli güvencelerin geliştirilmesi hem ceza muhakemesinin etkinliğini artıracak hem de temel hak ve özgürlüklerin korunmasına imkan sağlayacaktır[33].

Siber suçlarla etkin mücadele edilebilmesi için CMK'da yer alan koruma tedbirlerinin siber suçlara uygulanabilir olması ve etkin bir şekilde uygulanması ayrıca nazarı dikkate alınması gereken diğer bir husustur. Bu noktada CMK 134'üncü maddesinde düzenlenen koruma tedbiri, siber suçların engellenmesine yönelik çok boyutlu bir yaklaşımı ifade etmektedir. Bu maddeye göre; bilişim sistemlerinde arama gerçekleştirilmesi, verilerin kopyalanması ve çözümlenerek metne dönüştürülmesi mümkündür. Fakat bu koruma tedbirinin uygulanmasında bir takım sorunlar ortaya çıkmaktadır. Mesela, dijital/elektronik delil elde edilmesi ve değerlendirilmesi süreçleri için kanunda "kopyalama" deyimi kullanılmakla birlikte, uygulamada "hash değeri alma" ve "imaj alma" gibi terim ve tekniklerin kullanılması ilk göze çarpan eksiklik olarak

---

31 Şentürk Akaner (n15) 63.

32 Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı" (2015) 6 (22) *Türkiye Adalet Akademisi Dergisi* 427.

33 Schroeder and Verrel (n3) 99. Yazarlar, koruma tedbirlerinin temel haklara müdahale işlevlerine göre tasnif edilebileceğini haklı olarak ifade etmektedir.

belirmektedir[34]. Bu noktada dijital/elektronik delillerin bütünlüğünün korunarak bunların güvenilirliğinin tesis edilmesi amacıyla kanunda daha teknik ve spesipik kavramlara yer verilmesi, uygulama kriterlerinin buna göre netleştirilerek ceza muhakemesi süreçlerinde görev alan kişilerin de bu yönde yeterli eğitim almasının sağlanması büyük önem taşımaktadır[35].

Ayrıca CMK 135'inci maddesi kapsamında yer alan iletişimin izlenmesi, dinlenmesi ve kayıt altına alınmasına ilişkin tedbir dijital/elektronik delillerin elde edilme yöntemleri arasında merkezi bir rol üstlenmeye başlamıştır. Bilhassa örgüt faaliyeti kapsamında siber nitelikli suçlar ika edilirken dijital/elektronik iletişim vasıtalarının yaygın bir şekilde kullanılması, uygulamada söz konusu tedbiri neredeyse "tek delil elde etme yöntemi" olarak karşımıza çıkarmaktadır[36]. Fakat bu koruma tedbirine başvurulması, temel haklara müdahale niteliği taşıdığından yalnızca ve yalnızca ölçülülük ilkesi gereğince akla gelen son çare (ultima ratio) olarak uygulanmalıdır[37]. Nitekim arama ve el koyma tedbirlerinden önce uygulanan iletişimin denetlenmesi yoluyla elde edilen dijital/elektronik verilerin usuli güvenceleri zayıflattığını ve delil güvenliği ile yargılamanın adilliğini tartışmalı hale getirdiğini belirtilmekte fayda bulunmaktadır[38]. Bu meselenin temelinde ise siber suçlar için dijital ortamlarda iz sürmenin zorlukları yatmakta olup delil elde yöntemi olarak bu tedbire başvurma eğilimi gün geçerek artmaktadır. Olması gereken, anayasal güvenceler ile soruşturmanın etkinliği arasındaki hassas dengenin korunmasından geçmektedir. Aksi halde müdahalenin uygulanması

---

[34] Osman Yaşar ve Cengiz Otacı, *Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu I. Cilt Madde 1-156,* (11. Baskı, Seçkin Yayıncılık 2025) 955.

[35] Resul Göksoy, *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması* (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü 2017) 161.

[36] Seydi Kaymaz, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (5. Baskı, Seçkin Yayıncılık, 2025) 23; Recep Doğan, "Ceza Muhakemesi Hukukunda İletişimin Denetlenmesi Tedbiri ve AİHM Yaklaşımı" (2024) 2 (73) *Adalet Dergisi* 129; Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme" (2007) 11 (1-2) *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 1095.

[37] Ersan Şen ve Tamer Berk Bayraklı, "CMK m.135'de Yer Alan İletişimin Denetlenmesi ve Süreleri" (Ersan Şen Hukuk ve Danışmanlık, 25 Ekim 2023) 1 https://sen.av.tr/tr/makale/CMK-m-135-de-yer-alan-iletisimin-denetlenmesi-ve-sureleri

[38] Murat Önok, "Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" in *İletişim Özgürlüğüne Müdahale* (Türkiye Barolar Birliği Yayınları 2011) 85.

keyfiyete açık hale gelecek ve hukuk devleti ilkesini zedeleyecektir. AİHM de Kruslin v. France [39] ayrıca Huvig v. France [40] yine Roman Zakharov v. Russia [41] kararlarında iletişimin denetlenmesi tedbirine ancak yeterli hukuki temel ve denetim mekanizması ve sınırlı süre uygulamasının bulunması halinde izin verilebileceğini vurgulamaktadır[42]. Öte yandan CMK 140'ıncı maddesinde düzenlenen teknik araçlarla izleme, kamuya açık alanlarda şüpheli veya sanığın faaliyetlerini belli katalog suçlar kapsamında gözlem altına almayı hedeflerken[43] CMK 139'uncu maddesinde yer alan gizli soruşturmacı tedbiri, şüphelinin haberi olmayacak şekilde bir kişinin örgüte veya suç yapılanmasına dahil olarak bilgi toplamasına imkan vermektedir. Her iki tedbir de temel haklara müdahale niteliği taşıdığından yalnızca kuvvetli şüphe ve başka suretle delil elde edememe şartlarıyla uygulanabilmektedir. Bununla birlikte, gizli soruşturmacı görevlendirilmesi yapısı gereği delil elde etme yöntemi olmasının ötesinde suç ortamına doğrudan müdahale anlamı taşıdığından istismar edilme potansiyelini de bünyesinde taşımaktadır[44]. Uygulamada ise bilhassa teknik araçlarla izleme tedbirinde kararların gerekçesizliği ve

[39] Kararın tam metni için bkz. *Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990) https://hudoc.echr.coe.int/?i=001-57626

[40] Kararın tam metni için bkz. *Huvig v France* App no 11105/84 (ECtHR, 24 April 1990) https://hudoc.echr.coe.int/?i=001-57627

[41] Kararın tam metni için bkz. *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) https://hudoc.echr.coe.int/eng?i=001-159324

[42] Furkan Kaan Yüksek, "AİHM İçtihatlarında Kişisel Verilerin Korunması (Karar İncelemesi)" (2023) 25 (1) *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 389 vd. Bununla birlikte yazar, Zakharov/Rusya kararında her sistemde bulunan insan kaynaklı açığın sırf mahkemenin Rus devletine yönelik sahip olduğu bakış açısı nedeniyle herhangi bir somut vakıaya dayanmaksızın ihlal oluşturduğu kabulünün yerinde olmadığını haklı olarak dile getirmektedir.

[43] Mesela, fotokapan gibi teknik araçlar genel güvenlik amacıyla değil, yalnızca belirli bir kişinin belirli bir zaman diliminde nerede bulunduğunu tespit etmek amacıyla kullanılabilmektedir. Pınar Bacaksız ve Tuğba Bayzit, "Yargı Kararları Işığında Ceza Muhakemesi Hukukunda Fotokapan Vasıtasıyla Elde Edilen Görüntülerin Kullanılması Sorununa İlişkin Değerlendirmeler" (2022) (185) *Terazi Hukuk Dergisi* 50.

[44] AİHM, V./Finlandiya ve Teixeira de Castro/Portekiz kararlarında özellikle gizli ajan ya da soruşturmacı kullanımıyla elde edilen delillerin "tuzak kurma (entrapment)" yasağına aykırı olmaması gerektiğini vurgulamakta ve ajanların pasif gözlemci rolünü aşarak provokatif faaliyet yürütmelerinin adil yargılanma hakkını ihlal edeceğini belirtmektedir. Teixeira de Castro/Portekiz kararının Tükçe çevirisi ve ayrıntılı açıklamalar için bkz. Fatih Birtek, "Teixeira de Castro/Portekiz Davası (44/1997/828/1034)" (2010) (91) *Türkiye Barolar Birliği Dergisi* 409.

izleme süresine dair belirsizlikler elde edilen delillerin hukuka uygunluk denetimini zayıflatmaktadır[45].

Bu başlık altında ifade edilmesi gereken diğer bir düzenleme, 2017 tarihli ve 680 sayılı Kanun Hükmünde Kararname'nin 27. maddesiyle 2559 sayılı Polis Vazife ve Salahiyet Kanunu'na (PVSK) eklenen Ek Madde 6'dır. Söz konusu hükümle polise sanal/siber ortamda kimlik bilgilerine ulaşma ve araştırma yapma yetkisi tanınmıştır. İlgili düzenleme, "Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir." şeklindedir. Bu hüküm, kolluğa yargı kararı olmaksızın internet ortamında geniş yetkiler tanınmakta ve fiilen "sanal devriye" yetkisini yasal zeminle buluşturmaktadır[46].

Ancak bu düzenleme başta özel hayatın gizliliği, haberleşme hürriyeti ve kişisel verilerin korunması hakkı olmak üzere birçok temel hakkı doğrudan etkileyen nitelikte olduğundan kısa süre içinde anayasal denetime konu olmuştur. Anayasa Mahkemesi, 19 Şubat 2020 tarihli ve E. 2018/91, K. 2020/10 sayılı kararıyla söz konusu hükmü iptal etmiştir[47]. AYM kararında düzenlemenin "belirlilik" ve "öngörülebilirlik" ilkelerine aykırı olduğu, yeterli yargısal denetim mekanizmaları içermediği ve kişisel verilerin korunmasına ilişkin anayasal güvenceleri sağlamadığı gerekçelerine yer vermektedir. Yüksek mahkemeye göre; bir kişinin sanal ortam verilerine müdahale için yalnızca kolluk kararıyla işlem yapılması, demokratik toplumda kabul edilebilir bir sınırlandırma olarak değerlendirilmemektedir. Bu sebeple temel haklara ölçüsüz müdahale niteliği taşıyan söz konusu hükmün hukuk devleti ilkesiyle bağdaşmadığına karar verilmiştir[48].

---

[45] Faruk Y. Turinay, "Ceza Muhakemesi Hukukunda Teknik Araçlarla İzleme" (2021) 12 (46) *Türkiye Adalet Akademisi Dergisi* 443.

[46] Ersan Şen ve Tamer Berk Bayraklı, "Polisin Sanal Ortamda Takibi ve Sanal Devriye Yetkisi" (Ersan Şen Hukuk ve Danışmanlık, 22 Aralık 2023) 1 https://sen.av.tr/tr/makale/polisin-sanal-ortamda-takibi-ve-sanal-devriye-yetkisi

[47] Kararın tam metni için bkz. https://www.resmigazete.gov.tr/eskiler/2020/04/20200430-8.pdf

[48] Mehmet Bedii Kaya, *Polisin Sanal Devriye Yetkisini İptal Eden Anayasa Mahkemesi Kararının Değerlendirilmesi,* https://mbkaya.com/hukuk/polis-sanal-devriye-siberkolluk-aym-iptal.pdf

Bu iptal kararı, yalnızca PVSK açısından değil, dijital delillere erişimle ilgili tüm ceza muhakemesi uygulamaları bakımından da önemli bir dönüm noktası teşkil etmektedir. Çünkü karar, dijital alanın delil temini amacıyla sınırsız ve denetimsiz biçimde kullanılmasına açıkça karşı çıkmakta olup bu tür müdahalelerin ancak kanuni, sınırlı ve denetlenebilir olması gerektiğini vurgulamaktadır. Dolayısıyla CMK'daki koruma tedbirleri yeniden yapılandırılırken AYM'nin bu içtihadı çerçevesinde dijital müdahale biçimlerine özgü açık hükümler konulması ve özellikle yargı denetiminin güçlendirilmesi zorunluluk arz etmektedir.

III. UYGULAMADA KARŞILAŞILAN SORUNLAR

A. Dijital/Elektronik Delillerin Hukuki Değeri ve CMK m.134 Uygulamasında Yaşanan Sorunlar

Öncelikle ifade edelim ki hukuka aykırılıktan ari, maddi vakıayı yansıtma değeri yüksek, güvenilirliği ve bilimsel geçerliliği konusunda tereddüt bulunmayan dijital/elektronik delillerin tek başına delil olarak değerlendirilip hükme esas alınmasında kanaatimizce bir sakınca bulunmamaktadır. Bununla birlikte dikkat edilmesi gereken asıl husus, kanun koyucu tarafından açık bir normatif düzenleme yapılıncaya kadar dijital/elektronik delillerin başlı başına bir delil türü olarak değil, delil elde etme yöntemi olarak değerlendirilmesi gerektiği noktasında toplanmaktadır[49]. Nitekim adli bilişim incelemelerinin giderek artan yapısal ve teknik karmaşıklığına cevap verebilmek, dijital/elektronik delillerin bütünlüğünü korumak ve bu delillerin ceza adalet sürecinde daha güvenilir biçimde kullanılmasını sağlamak maksadıyla "Yeni Adli Bilişim İnceleme Süreci (YABİS)" modelinin geliştirilmesine yönelik çalışmalar yapılmaktadır[50]. Buna

[49] Sarsıkoğlu (n32) 449; Yusuf Başlar, "Elektronik Delilin Toplanması ve Muhafazası" (2020) 10 (1) *Hacettepe Hukuk Fakültesi Dergisi* 100. Son yazar, veri bütünlüğünün korunmasının muhafaza süreçlerinin güvenilirliğine bağlı olduğunu; bunun için de hash (veri bütünlük) değeri alma, imaj (birebir kopyalama) ve koruma zinciri (chain of custody) oluşturulması gibi teknik önlemlerin standart hale getirilmesi gerektiğini belirtmektedir.

[50] Ramazan Oğuz ve Recep Eryiğit, "Yeni Adli Bilişim İnceleme Süreci (YABİS)" (2024) 36 (2) *Fırat Üniversitesi Mühendislik Bilimleri Dergisi* 717. Nitekim dijital/elektronik deliller tespit edildikleri anda toplanmaya ve incelenmeye uygun olmayıp bu delillerin analizi ek zaman, emek ve uzmanlık gerektirmektedir. Ayrıntılı açıklamalar için bkz. Esther George, Michael Jameison ve Kemal Kumkumoğlu, *Siber Suçların Önlenmesi ve Bu Suçlarla Mücadele: Türkiye İçin Temel Bulgular ve Tavsiyeler* (Avrupa Konseyi 2023) 17.

göre; dijital/elektronik delillerin ceza muhakemesinde kullanılabilir olması, öncelikle hukuka uygun şekilde elde edilmesine bağlı olup bu delillerin toplanması ve muhafazası sırasında veri bütünlüğünün korunması büyük önem taşımaktadır. Aksi takdirde delillerin geçerliliği ve ispat fonksiyonu tartışmalı hale gelebilecektir[51]. Mesela Sky ECC haberleşme programından elde edildiği iddia edilen delillere ilişkin olarak öncelikle bu verilerin orijinal ya da ham halinin dosyada yer alıp almadığı dikkatle değerlendirilmesi gereken bir husustur. Aksi takdirde sunulan deliller (yazışmalar, görüntüler) yalnızca bir fotokopi belge niteliğinde olacak ve bu verilerin sonradan oluşturulup oluşturulmadığı ya da üzerinde herhangi bir değişiklik yapılıp yapılmadığı sağlıklı bir şekilde tespit edilemeyecektir[52]. TCK'nın bilişim alanında işlenen suçlar başlıklı bölümünde yer alan siber suçlarda da korunan hukuki değerin bilişim sistemlerinin güvenliği ve güvenilirliği olduğu ifade edilmektedir[53]. Ancak bu noktada siber suç tiplerinin teknolojik gelişmelerle birlikte sürekli değişkenlik göstermesinin durağan normatif yapıların etkinliğini zayıflatmakta olduğu ifade edilmelidir[54]. Kısacası, dijital/elektronik delillerin ceza muhakemesinde sağlıklı şekilde kullanılabilmesi sadece teknik araçlarla elde edilmeleriyle değil, aynı zamanda normatif düzlemde yer alan koruma tedbirlerine ilişkin hükümlere uygunlukla mümkün hale gelmektedir. Bu çerçevede koruma tedbirlerine ilişkin düzenlemelerin hem güncel dijital gelişmelere uyarlanması hem de uygulamada hukuki güvencelerle desteklenmesi normatif güncellenme ihtiyacının temel gerekçelerini teşkil etmektedir.

Buna göre; CMK 134'üncü maddesi, dijital/elektronik materyaller üzerinde yapılacak arama ve kopyalama işlemlerini düzenlemekteyse de uygulamada ciddi yapısal

---

[51] Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi" (2015) 3 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 256. Yazar, dijital/elektronik delillerin değiştirilme ve bozulmaya son derece elverişli yapısının dijital verileri ispat sürecinin en savunmasız bileşeni konumuna getirdiğini ifade etmektedir.

[52] Ersan Şen, Buğra Şahin ve Doğa Ceylan, "Sky ECC İletişim Sağlayıcısından Elde Edilen Delillerin Hukukiliği" (2025) 224 *Terazi Hukuk Dergisi* 129.

[53] Mehmet Bedii Kaya, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim" in Şeref Sağıroğlu ve Mustafa Şenol (eds), *Siber Güvenlik ve Savunma: Problemler ve Çözümler* (1. Baskı, Grafiker Yayınları 2019) 218.

[54] You Zhou and others, "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality" (2024) 19 *Asian Journal of Criminology* 422 https://doi.org/10.1007/s11417-024-09436-y

sorunlar barındırmaktadır. Öncelikle "kopyalama" kavramının teknik bir karşılığının bulunmaması, hangi işlemin kopyalama olarak değerlendirileceği konusunda farklı uygulamalara yol açmaktadır. Mesela, dijital/elektronik verinin doğrudan cihaz üzerinden incelenmesi hem delil güvenliği hem de özel hayatın gizliliği açısından tartışmalı sonuçlar doğurabilmektedir. Öte yandan maddede geçen "bilgisayar kütükleri" gibi teknik ifadelerin açık biçimde tanımlanmamış olması hem uygulayıcı hem de şüpheli açısından belirsizlik yaratmakta; bu terimlerin dijital/elektronik sistemlerin tanımıyla birlikte ele alınmaması kanunilik ilkesine zarar vermektedir Yine madde metninde yer alan "verilerin kâğıda yazdırılarak metne dönüştürülmesi" deyimi uygulamada çoğu zaman kolluğu zor durumda bırakmakta ve teknik gerçeklikle bağdaşmamaktadır. Bununla birlikte, taşınabilir cihazların tüm belleğine erişilmesi ölçülülük ilkesinin ihlali anlamına gelebilecek geniş müdahalelere sebep olmaktadır. Bu işlemlerde hash değeri alınması uygulamada yer yer gerçekleştirilmekteyse de bunun yasal bir zorunluluk olmaması delilin değiştirilebilirliğine dair ciddi şüpheler doğurmaktadır. Ayrıca hakim kararı alma zorunluluğu çoğu zaman şeklen yerine getirilmekte olup gerekçesiz kararlar zikredilen işlemlerin denetlenebilirliğini azaltmaktadır. Kanunda incelemenin kapsamının net çizilmemesi ve kayıt sisteminin eksikliği, dijital verilerin bütünlüğü ile kişisel verilerin korunmasını tehlikeye atan önemli boşluklar olarak görülmektedir[55].

B. Teknik Usullerle İlgili Belirsizlikler

Öncelikle ifade edelim ki teknik usullerdeki eksiklikler yalnızca yetersiz mevzuattan değil, aynı zamanda uygulamada karşılaşılan uzmanlık eksikliği ve standardizasyon sorunlarından kaynaklanmaktadır. Zira dijital teknolojilerin ceza muhakemesi süreçlerinde artan kullanımı, yalnızca yeni delil türlerinin ortaya çıkmasına değil, aynı zamanda mevcut usul hükümlerinin bu yapıya uyum sağlama zorunluluğuna da işaret etmektedir[56]. Özellikle dijital delillerin toplanması, korunması ve ceza

[55] Burak Çekiç, "Bilgisayar Verilerinde Arama, Kopyalama, El Koyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar" (2021) 11 (2) *Tekirdağ Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi* 180; Salih Keskin, "Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar" (2021) 2 (1) *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi* 651.

[56] Zhou and others, (n54) 423. Yazarlar, teknolojik ilerlemenin hızının çoğu zaman kanun yapım sürecinin önüne geçtiğini; bu durumun da mevcut hukuki çerçevelerin caydırıcılığı ve kolluk uygulamalarının etkinliğini azalttığını belirtmektedir.

muhakemesine dahil edilmesi süreçlerinde hukuka uygunluk, veri bütünlüğü ve delil güvencesi gibi ilkelerin sağlıklı biçimde işlerlik kazanabilmesi yürürlükteki ceza (muhakemesi) normlarının siber ortamlara uyarlanmasıyla mümkün olacaktır. Nitekim yalnızca birkaç ülkenin bile bu alanda gerekli kanuni düzenlemeleri yapmış olması tabiri caizse hukuki boşluklardan yararlanmak isteyen bilişim suçluları için bir nevi kurtarılmış bölge oluşturmaktadır[57]. Bu sebeple dijital/elektronik delillerin elde edilmesi süreçlerinde koruma tedbirlerine ilişkin düzenlemelere hem teknik hem de normatif anlamda riayet edilmesi yalnızca uygulama bakımından değil, aynı zamanda kavramsal ve kuramsal düzeyde de güncellenme ihtiyacının temelini oluşturmaktadır. Bu noktada koruma tedbirlerine ilişkin ceza (muhakemesi) normlarının güncellenmesi bir yönüyle temel hak ve özgürlükleri koruma işlevini sağlarken başka bir yönüyle de dijital/elektronik delillerin hukuki niteliğinin açık, güvenilir ve tartışmasız biçimde belirlenmesine hizmet edecektir[58]. Bununla birlikte, koruma tedbirlerini delil elde etme yöntemi olarak kabul eden bir yaklaşımla eğer ceza (muhakemesi) kurallarında dijital/elektronik deliller açıkça düzenlenmemişse bile bireysel hakları ihlal etmeyen ve hukuka uygun şekilde elde edilen bu türdeki delillerin delil serbestisi ilkesi gereğince kullanılmasına izin verildiği ifade edilmektedir[59].

Kanaatimizce bir dijital/elektronik delilin yalnızca delil olarak kabul edilmesinin yeterli olmadığı aynı zamanda bu delillerin elde edilmesi, muhafazası ve muhakemeye dahil edilmesi aşamalarında izlenmesi gereken adli bilişim protokollerinin eksikliği yahut standartlaşamaması sebebiyle söz konusu delillerin geçerliliğinin ve güvenilirliğinin ciddi şekilde zarar görebileceği nazarı dikkate alınmalıdır. Özellikle veri hacminin büyüklüğü, farklı formatlarda işlenmesi ve çeşitli cihazlar üzerinden erişilmesi delil süreçlerini teknik açıdan daha karmaşık hale getirmekte olup bu durum da koruma

---

[57] Siber suçlarla mücadelenin küresel çapta sağlanması gerekliliği hakkında ayrıntılı açıklamalar için bkz. Amelie M. Weber, "The Council of Europe's Convention on Cybercrime" (2003) 18 (1) *Berkeley Technology Law Journal* 425; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci" (2018) 4 (2) *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 36.

[58] Fatma Bilge Özcan, *Elektronik Delillerin Ceza Muhakemesi Bakımından İspat Değeri* (1. Baskı, Yetkin Yayınları 2024) 15.

[59] Osco Escobedo Miguel Angel and others, "Digital Evidence as a Means of Proof in Criminal Proceedings" (2024) 18 (4) *Revista de Gestão Social e Ambiental* 10 https://doi.org/10.24857/rgsa.v18n4-028

tedbirlerinin hem teknik yeterlilik hem de hukuki uygunluk bakımından yeniden değerlendirilmesini gerekli kılmaktadır[60]. Nitekim uluslararası alanda yayımlanan bir rehberde de vurgulandığı üzere; "ceza muhakemesinde dijital/elektronik delillerin toplanması ve işlenmesi için sağlam bir yasal altyapıya ihtiyaç duyulduğu" ifade edilmektedir[61]. Doalyısıyla bu nitelikteki delillerin ispata yarayabilmesi için teknik güvenlik kadar usule ilişkin normatif çerçevenin de açık ve somut olarak tanımlanması elzemdir. Kısacası dijital çağda ceza muhakemesi hukukunun karşılaştığı yeni ispat sorunlarına çözüm geliştirme açısından siber suçlara ilişkin koruma tedbirlerinin genel çerçevesinin belirlenmesi son derece önem arz etmekte olup dijital/elektronik delil kullanımının bireysel haklara saygı ilkesiyle dengelenmesi ve anılan tedbirlerin uygulanma sınırlarını tanımlayan net bir kanuni çerçeve geliştirilmesi gerekmektedir[62]. Söz konusu dijitalleşme ihtiyacının giderilmesi ve koruma tedbirlerinde hayata geçirilmesinin ilk adımının "dijital/elektronik delil" kavramının CMK'ya dahil edilmesi olduğunu düşünmekteyiz[63]. Ayrıca doktrinde, bilişim suçlarında teknik usullerle ilgili belirsizliklerin giderilmesi için uzmanlaşmış yapılar kurulması, adli kolluk ve bilirkişiler teknik olarak eğitilmesi, delil toplama süreci hızlandırılarak sistematik hale getirilmesi gerektiği haklı olarak ifade edilmektedir[64].

---

[60] Janice Goldstraw-White, *Legal and Policy Framework for Digital Forensics: A Resource for Practitioners* (Perpetuity Research and Consultancy International Ltd, University College London and the Institute Crime & Justice Policy Research 2022) 2.

[61] Council of Europe and INTERPOL, *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* (Council of Europe 2020) 14 https://www.coe.int/en/web/cybercrime

[62] Ivan Prysiazhniuk, "Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection" (2023) 5 *Visegrad Journal on Human Rights* 87 https://doi.org/10.61345/1339-7915.2023.5.11

[63] Dijital/elektronik delil kavramının tanımlanmasıyla alakalı doktrinde öneriler bulunmaktadır. Bunlardan bir tanesi de; *"... bir ceza davasında (maddi) gerçeği ortaya çıkarmak amacıyla delillere uygulanan ceza muhakemeleri gerekliliklerine uygun olarak elektronik yollarla kaydedilen veya elektronik biçimde sunulan hukuki olarak önemli bilgiler"* şeklindedir. Anna A. Dmitrieva and Pavel S. Pastukhov, "Concept of Electronic Evidence in Criminal Legal Procedure" (2023) 1 (1) *Journal of Digital Technologies and Law* 289 https://doi.org/10.21202/jdtl.2023.11

[64] Cengiz Apaydın, "Bilişim Suçlarında Etkin Soruşturma ve Yargılama" (Ceza Hukuku Bilinci, 14 Haziran 2025) 1 https://www.cezahukukubilinci.org/bilisim-suclarinda-etkin-sorusturma-ve-yargilama/ Yazar, ayrıca UYAP'ta bilişim veri havuzu oluşturulması, veri iletişimi ve şifre çözme gibi alanlarda hukuki düzenlemeler yapılması, deliller toplanmadan yetkisizlik kararı verilmesinin önlenmesi gerekliliğinden bahsetmektedir. Bu çalışmada sunulan öneriler, bilişim suçlarının etkili bir şekilde soruşturulması ve yargılanabilmesi için hukuki düzenlemelerin yanı sıra teknik altyapının da geliştirilmesinin önemini bir kez daha vurgulamaktadır.

C. Ölçülülük İlkesi ve Siber Suçlarda Müdahale Sınırı

Siber suçlarla mücadele edilirken temel hak ve özgürlüklerin korunması, ceza muhakemesi işlemlerinin hukuk devleti ilkeleri doğrultusunda yürütülmesi bakımından ölçülülük ilkesinin gözetilmesini zorunlu kılmaktadır[65]. Ölçülülük ilkesi, yalnızca müdahalenin meşru bir amaç taşıması (elverişlilik) ile sınırlı kalmayıp ayrıca zorunlu olması (gereklilik) ve uygulanan tedbirin elde edilmek istenen yararla orantılı olması (oranlılık) şartlarını da içermektedir. Bilhassa iletişimin denetlenmesi, dijital/elektronik veriye el konulması ya da teknik izleme yapılması gibi siber suçlarla mücadelede kullanılan koruma tedbirleri kişiilerin özel hayatı, haberleşme özgürlüğü ve siber ortamlarındaki faaliyetlerine doğrudan müdahale niteliği taşıdığından ölçülülük değerlendirmesinin öncelikle kanuni çerçevede ve devamında somut olay bazında da yapılmasını sonuçlamaktadır. Nitekim AKSSS 15'inci maddesinin 1'inci fıkrasında; taraf devletlerin bu sözleşme kapsamında alacakları önlemlerin, insan hakları ve temel özgürlüklerin korunmasını güvence altına alacak şekilde ve özellikle "ölçülülük ilkesine (principle of proportionality)" uygun biçimde düzenlenmesi gerektiği açıkça ifade edilmektedir. Bununla birlikte doktrinde AKSSS'nin öngördüğü soruşturma usullerinin temel hak ve özgürlüklere aykırı olduğunu savunan görüşler bulunduğu belirtilmektedir[66]. Bize göre; dijital/elektronik delil elde etme yöntemleri dahil olmak üzere tüm koruma tedbirlerinin sadece etkinlik temelli olarak değil, aynı zamanda bireysel hakların asgari düzeyde sınırlandırılması esasına dayanılarak uygulanması gerekmektedir. Bu perspektifin Türk ceza adalet sisteminin siber alanda da meşruiyetini koruyabilmesi açısından elzem olduğunu düşünmekteyiz.

---

[65] Martin Hussels, *Strafprozessrecht-schnell erfasst* (2nd edn, Springer 2008) 64; Nigar Samsa, *Kamu Haberleşme Hürriyeti Kapsamında İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Denetlenmesi* (Yüksek Lisans Tezi, Pamukkale Üniversitesi 2010) 10. Son yazar, temel hak ve özgürlüklerin mutlak biçimde sınırlandırılamayacağını; bunların "vazgeçilemez, devredilemez, biri diğerine tercih edilemez" yapıları ve karşılıklı etkileşim ve tamamlayıcılık ilişkisi nedeniyle bütüncül bir yapı oluşturduğunu haklı olarak ifade etmektedir. Bu bakımdan siber suçlarla mücadelede kullanılan araçların bireysel haklara etkisi yalnızca teknik değil, aynı zamanda anayasal düzeyde bir değerlendirmeyi de gerektirmektedir.

[66] Merve Erdem ve Gürkan Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri" (4. Uluslararası Bilişim Hukuku Sempozyumu, İzmir, 12-14 Mayıs 2016) 8.

IV. DİJİTAL KORUMA TEDBİRLERİNE YÖNELİK YENİ BİR YAKLAŞIM

A. CMK'ya Yeni Bir Bölüm Eklenmesi

CMK'da yer alan koruma tedbirlerine ilişkin düzenlemeler, esasen fiziksel delil elde etme yöntemlerlerine uygun olarak şekillenmiş olup dijital çağın ortaya çıkardığı yeni teknik ihtiyaçlar açısından yeniden değerlendirilme potansiyeli taşımaktadır[67]. Bilhassa CMK 134'üncü, 135'inci ve 140'ıncı madde hükümleri, günümüzde dijital/elektronik delil elde etme süreçlerinde yaygın olarak uygulansa da mevcut içerik yapısı itibarıyla uygulamada farklı yorumlara yol açabilmekte ve teknolojik gelişmeler doğrultusunda güncellenmeye açık bir yapı sergilemektedir[68]. Örnek verecek olursak; 134'üncü maddede geçen "kopyalama" ibaresi, dijital veri güvenliği açısından zorunlu olan hash alma, imaj alma veya orijinal veriyle birebir bütünlük karşılaştırması yapma gibi teknik prosedürleri içermemekte ve bu durum, dijital/elektronik delillerin güvenilirliğini gerek teknik gerekse de hukuki açıdan tartışmalı hale getirmektedir[69]. Benzer şekilde 135'inci madde, sadece içerik odaklı değerlendirmeye olanak tanımakta olup meta-veri, trafik bilgisi ve konum verisi gibi dolaylı ve fakat mahremiyet açısından kritik bilgiler hakkında açık bir sınır çizmemektedir[70]. Bununla birlikte, AİHM ve ABD

---

[67] Ali Boyracı, "Gizli Soruşturmacının Konuta Girme Yetkisi ve Bu Yetkinin Kapsamı Üzerine Bir İnceleme" (2024) 14 (2) *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 1239. Yazar, gizli soruşturmacının konuta girme yetkisinin Türk hukukunda düzenleme eksikliği nedeniyle tartışmalı bir alana işaret ettiğini ve bu konudaki yasal boşluğun uygulamada farklı yorumlara sebebiyet verdiğini; Alman hukukunda ise bu konuda açık bir hüküm öngörülerek yetki sınırlarının net biçimde çizilmiş olduğunu ifade etmektedir.

[68] Pelin Özkaya, *Adli Bilişimde Özel Araştırma ve Soruşturma Yöntemleri* (1. Baskı, Seçkin Yayıncılık 2022) 136; Seda Yağmur Sümer, "Ceza Muhakemesinde Mobil Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları" (2022) 87 (1) *İzmir Barosu Dergisi* 111. Son yazar, mobil cihazlara yönelik CMK 134'üncü maddesi kapsamındaki elkoyma işleminin uygulamadaki yaygınlığı ve hak ihlali potansiyeli göz önünde bulundurulduğunda bireyler açısından ciddi sonuçlar doğurabilecek ölçüde müdahaleci bir nitelik taşıdığını ifade etmektedir. Nitekim el konulan mobil/akıllı telefon bakımından yapılan müdahaleye ilişkin kanun hükmünde bir hukuki denetim yolu öngörülmemektedir. Bu eksiklik, müdahalelerin denetlenebilirliğini zayıflatmakta ve insan haklarına ilişkin temel güvenceler açısından ciddi sakıncalar doğurmaktadır.

[69] George, Jameison ve Kumkumoğlu (n50) 36, 42. Yazarlar, CMK 134'üncü maddesinin yetersizliği konusunda herkesin hemfikir olduğu yönünde görüş beyan etmektedir.

[70] Feyza Elif Canbaz Karacif, "İletişimin Tespiti Kayıtları (HTS) ve Haberleşme Özgürlüğü" (2024) 14 (1) *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi* 240. Yazar, HTS kayıtlarının talep edilebilmesi için şüphe konusu fiilin ilgili düzenlemede yer alan suç tiplerinden biri kapsamında değerlendirilmesinin (kataloğa girmesinin) zorunlu olmadığını belirtmektedir.

Yüksek Mahkemesi içtihatlarında bu tür verilerin özel hayat kapsamında değerlendirilmesi gerektiği açıkça vurgulanmaktadır. Zikredilen gerekçelerle halihazırdaki CMK hükümlerinde normatif güncelleme ihtiyacının iki düzlemde ele alınması gerektiğini düşünmekteyiz. İlki, mevcut maddelerin teknik terminolojiyle güçlendirilmesidir (mesela hash/imaj alma tanımı, dijital iz protokolü, dijital/elektronik delil zinciri gibi). Diğeri ve en önemlisi de kanuna yeni bir "Dijital Koruma Tedbirleri" bölümü eklenerek dijital/elektronik sistemlere özel erişim, analiz ve müdahale usullerinin müstakil biçimde düzenlenmesidir. Bu kapsamda önerilebilecek temel değişikliklerden ilk olanı ise CMK 134'üncü maddesinin ek fıkralarla zenginleştirilmesi ve şu hükmün açıkça yazılmasıdır: *"Bilgisayar veya bilişim sistemlerinde yapılacak arama ve kopyalama işlemlerinde dijital/elektronik delilin bütünlüğünün korunması amacıyla hash değeri alınır. Elde edilen kopya, orijinal veri ile bütünlük karşılaştırmasına tabi tutulur. Bu işlem, bir tutanakla tespit edilir."* Aynı şekilde CMK 135'inci ve 140'ıncı maddelere eklenecek teknik ifadeler, müdahalenin sınırlarını açık biçimde çizerek uygulamada ortaya çıkabilecek yorum farklılıkları ve ölçülülük ilkesine aykırı müdahalelerin önüne geçilmesini sağlayacaktır. Bu tür güncellemeler kanaatimizce klasik ceza muhakemesi hukukunda delil serbestisi ilkesinin güvenilirlik boyutunu karşılayacağı gibi dijital ceza muhakemesi bağlamında da hukuki öngörülebilirliğin teminine katkı sunacaktır[71].

A. Müdahale Türlerinin Sınıflandırılması

Koruma tedbirleri, dijitalleşmenin muhakeme pratiğini dönüştürmesiyle birlikte ceza muhakemesi hukukunun yapısal olarak en esnek ve güncellenmeye en açık alanı olarak dikkat çekmektedir[72]. Nitekim ceza muhakemesinde bireylerin hak ve özgürlükleri açısından koruma tedbirlerinin çok daha ön planda olduğu; bu sebeple koruma tedbirlerine ilişkin düzenlemelerin bir ülkenin hukuk düzenine ilişkin kanaat

[71] Arslan (n51) 253. Yazar, dijital/elektronik delillerin hukuka uygun yollardan elde edilmesinin zorunlu olduğunu ve konuya ilişkin CMK 134'üncü ila 138'inci madde hükümlerinin tadil edilmesinde fayda bulunduğunu haklı olarak ifade etmektedir. Ayrıca uygulamadaki sorunların çözümü açısından bir "adli bilişim kurumu" kurulmasının isabetli olacağını vurgulamaktadır.

[72] Faruk Yasin Turinay, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması" (2021) 70 (2) *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 476. Yazar, sadece son birkaç yıldaki gelişmelere bakıldığında dahi koruma tedbirlerinde önemli değişiklikler yapıldığını belirtilmektedir.

oluşturulmasında ölçüt oluşturduğu doktrinde ifade edilmektedir[73]. Bu niteliğinden dolayı koruma tedbirlerine dair genel prensiplere anayasalarda yer verilmektedir. Gerçekten de "ceza muhakemesi devletin anayasasının sismografı" olarak anayasal düzenin değişimlerini ve hassasiyetlerini her an yansıtmaktadır. Buna göre; koruma tedbirlerinin yalnızca teknik olarak değil, aynı zamanda içerik ve müdahale biçimi açısından da yeniden tanımlanması ve sınıflandırılması gerekmektedir. Bununla birlikte, doktrinde koruma tedbirlerinin sınıflandırılmasında işlevi, uygulama şekli (gizli/açık), niteliği (zorlayıcı/zorlayıcı olmayan), tarihsel konumu (geleneksel/modern) ve adli ya da idari karakteri gibi çok sayıda ölçüte dayalı yaklaşımlar benimsenmekte olduğu görülmektedir[74]. Mesela henüz bir suç işlenmeden risk odaklı olarak gerçekleştirilen dijital müdahalelerin büyük çoğunluğu, idari faaliyet niteliği taşımaktadır[75]. Bu tür uygulamalarda kişi üzerinde herhangi bir suç şüphesi oluşmadan yapılan teknik izleme veya veri toplama faaliyetleri önleme tedbiri kapsamında değerlendirilmektedir. Halihazırdaki CMK ise koruma tedbirlerini büyük ölçüde fiziksel müdahale üzerinden kurgulamış olduğundan dijital/elektronik sistemlere yönelik özel nitelikleri dikkate almamaktadır. Oysa ki dijital/elektronik delillerin görünmez, yaygın ve sistem içi müdahaleye açık bir özelliği bulunmaktadır[76]. Bu durum klasik koruma tedbiri anlayışının dijital/elektronik delil kavramı karşısında yetersiz kalmasına sebep olmaktadır.

Bu çerçevede dijital/elektronik koruma tedbirlerinin müdahale biçimi, erişim yöntemi ve gizlilik düzeyine göre sınıflandırılması hem hukuk uygulayıcıları bakımından normatif rehberlik oluşturacak hem de yargı denetiminin niteliğini güçlendirecektir[77]. Zira dijital/elektronik veri elde etme süreçlerinde hukuka uygunluk ve delil bütünlüğünün korunması adil yargılama ilkesi açısından vazgeçilmez nitelikte olup her bir

---

73 Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku Cilt I* (11. Baskı, Adalet Yayınevi 2016) 523.

74 Turinay (n72) 477; Ünver ve Hakeri (n73) 524.

75 Hakan Karakehya, "Suçu Önleyici Kolluk Faaliyetleri" in Filiz Tepecik (ed), *Suç Önleme Modelleri* (Anadolu Üniversitesi Yayınları 2016) 57.

76 Council of Europe, *Electronic Evidence Guide Version 3.0* (Cybercrime Programme Office, Strasbourg, 4 April 2022) 17 https://kanuni.taa.gov.tr/assets/dosyalar/Dijital_Delil_Kilavuzu_WEB.pdf

77 Ayrıntılı açıklamalar için bkz. Turinay (n72) 477.

dijital/elektronik müdahale türünün ayrı usul ve güvencelerle tanımlanması büyük önem arz etmektedir. Tarafımızca önerilen sınıflandırma modeli, dijital/elektronik müdahaleleri üç ana başlıkta toplamaktadır. Bunlar; görünür müdahale, uzaktan müdahale ve sistem-içi izleme şeklinde tezahür etmektedir. Görünür müdahale, fiziksel varlığı olan cihazlarda (mesela, bilgisayar ve telefon gibi) yapılan açık arama ve kopyalama işlemlerini[78] ifade ederken uzaktan müdahale, kişilerin bilgileri haricinde dijital/elektronik sistemlerine erişilmek suretiyle veri elde edilmesini[79] belirtmektedir. Sistem-içi izleme ise özel yazılımlar ya da teknik araçlar kullanılarak dijital/elektronik sistemlerin sürekli takip edilmesi ve veri akışının kayıt altına alınmasını[80] ifade etmekte olup halihazırda tarafların iletişime devam ettiği bir cihazın deşifre edilmesi, iletişimin gerçekleştiği programa anlık olarak gizli girilmesi ve buradan veri elde edilmesi, CMK'da öngörülmemektedir[81]. Bu ayrımın yalnızca terminolojik olarak değil, aynı zamanda ölçülülük ve yargı denetimi ilkelerinin uygulanması açısından da belirleyici nitelikte olduğunu düşünmekteyiz. Zira delil serbestisi ilkesi, tüm delillerin koşulsuz olarak hükme esas alınabileceği anlamını taşımamaktadır[82]. Dolayısıyla dijital/elektronik delil elde etme süreçlerinde müdahalenin kapsamı genişledikçe hak ihlali riski artmakta olup bu sebeple uygulayıcıların müdahalenin düzeyini ve biçimini somut olayın niteliğine göre değerlendirmesi zorunluluk arz etmektedir[83]. Mesela görünür müdahale klasik fiziksel arama ile benzerlik gösterirken sistem-içi izlemenin çok daha derin ve sürekli bir mahremiyet ihlali potansiyeli ihtiva etmesi sebebiyle daha sıkı teminatlara tabi olması da gerekmektedir. Fransa'da benzer bir yaklaşım, Ceza Muhakemesi Usulü Kanunu'nda (CPP, m. 706-102 ve devamı) "informatik sistemlere gizli erişim ve izleme" başlığı altında

---

78 Mesela, CMK 134'üncü maddesi gereğince yapılan bilgisayar disk görüntüsü alma işlemi bu şekildedir.

79 Mesela, uzaktan bağlantıyla ekran görüntüsü alma işlemi bu şekildedir.

80 Mesela, bilişim sistemine tuş kaydedici (keylogger) ya da casus yazılım yerleştirme bu şekildedir.

81 Şen, Şahin ve Ceylan (n52) 129.

82 Arslan (n51) 257. Yazar, burada nazarı dikkate alınması gereken hususun, söz konusu delillerin "olayı temsil edici, müşterek, akılcı ve gerçekçi" nitelikte ve bilhassa "hukuka uygun yollardan elde edilmiş" olması zorunluluğu olduğu vurgusu yapmaktadır. Bu noktada ise dijital/elektronik koruma tedbirlerinin tanımlanması ve sınıflandırılması önemli hale gelmektedir.

83 CMK 134'üncü maddesi gibi kapsamlı yetkiler içeren koruma tedbirlerinin uygulanmasında kademeli müdahale anlayışının benimsenmesi gerektiği ifade edilmektedir. Neslihan Ateş Benek, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" (2022) 10 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 405.

sınıflandırılmaktadır[84]. Almanya'da Anayasa Mahkemesi, bilgi ve iletişim sistemlerine müdahaleyi anayasal koruma altına alarak yüksek derecede mahremiyete sahip verilerin sistematik olarak izlenmesinin sadece çok istisnai hallerde ve sağlam hukuki gerekçelerle mümkün olabileceğini belirtmektedir[85]. Kanaatimizce bu sınıflandırma önerisi, hem CMK'da yapılacak olası düzenlemeler için zemin oluşturmakta hem de uygulayıcılar açısından hangi tedbirin hangi koşullarda uygulanabileceğini açıklığa kavuşturmaktadır. Özellikle teknik araçlarla müdahale edilen dijital sistemlerde bu tedbirlerin önceden tanımlanmış kategorilerle ilişkilendirilmesi, keyfi uygulamaların önüne geçilmesi ve ölçülülük ilkesinin hayata geçirilmesi açısından önem taşımaktadır.

B. Yargısal Denetimin Güçlendirilmesi

Dijital çağda ceza muhakemesi süreçleri yalnızca delil toplama tekniklerinin gelişimiyle değil, aynı zamanda hukuki denetim mekanizmalarının etkinliğiyle de sınanmaktadır. Çünkü bireylerin anayasal haklarına doğrudan etkide bulunduğundan koruma tedbirlerinin dijital/elektronik ortamlarda uygulanmasında hukuk devleti ilkesinin gerektirdiği anayasal güvencelerin eksiksiz biçimde işletilmesi zorunluluk arz etmektedir. Özellikle kişisel verilerin kolayca ve yaygın şekilde işlenebildiği dijital/elektronik sistemlerde koruma tedbirlerinin yalnızca teknik değil, aynı zamanda

---

[84] *"Bir teknik cihaz ilgili tarafların rızası olmaksızın, bir bilgisayar sisteminde depolandığı, bir otomatik veri işleme sisteminin kullanıcısı için bir ekranda görüntülendiği, kullanıcı tarafından girildiği veya çevre birimleri tarafından alındığı ve iletildiği şekilde, bilgisayar verilerine erişmek, bunları kaydetmek, saklamak ve iletmek amacıyla herhangi bir yerde tatbik edilebilir. Cumhuriyet savcısı veya soruşturma hakimi, bu maddenin birinci fıkrasında sözü edilen teknik cihazın uygulanmasını sağlayan teknik işlemleri gerçekleştirmek üzere 157. maddede öngörülen listelerden birinde yer alan yetkili gerçek veya tüzel kişiyi görevlendirebilir. Cumhuriyet savcısı veya soruşturma hakimi ayrıca, I. Kitabın IV. Başlığının I. Bölümünde öngörülen usullere uygun olarak, ulusal savunma gizliliğine tabi Devlet kaynaklarının kullanılmasını emredebilir. 706-102-1. maddede belirtilen sistemin kullanımına izin veren kararda bu işlemlerin kullanımını haklı kılan suç, otomatik veri işleme sistemlerinin tam yeri ve ayrıntılı açıklaması ile işlemlerin süresi belirtilir."* Code de procédure pénale, art 706-102 https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000038270752/#LEGISCTA000038270761

[85] 28 Şubat 2008 tarihli kararın tam metni için bkz. Bundesverfassungsgericht, "1 BvR 370/07" (2008) https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html Nitekim Almanya'da dijital/elektronik delillere yönelik müdahaleler, Federal Anayasa Mahkemesi'nin bu kararıyla şekillenmiştir. Söz konusu kararda bireylerin bilgi ve iletişim sistemlerine yönelik gizli erişimlere karşı korunmasının "bilgi ve iletişim sistemlerinin gizliliği" başlığı altında anayasal düzeyde yeni bir temel hak olarak tanınması gerektiği ifade edilmektedir. Ayrıca bkz. European Digital Rights, "Germany: New Basic Right to Privacy of Computer Systems" (27 February 2008) https://edri.org/our-work/edrigramnumber6-4germany-constitutional-searches/

yargısal denetim yolları ile de sınırlandırılması temel hakların korunması açısından hayati niteliktedir. Ayrıca ifade edelim ki dijitalleşmenin yoğun anonimlik üretme kapasitesi, yalnızca bireylerin gizliliği üzerinde değil, bununla beraber kolluk kuvvetlerinin adli süreçlere etkili katkı sunmasını da güçleştirmekte olup söz konusu durum hukuk devletinde denge kurma çabasını etik ikilemlerle karşı karşıya getirmektedir[86].

Bu bağlamda Alman ceza hukuku doktrini, dijitalleşmenin soruşturma süreçlerinde doğrudan etkili olduğunu açıkça kabul etmekte ve bu etkiyi özellikle bağlantı verilerinin ve dijital izlerin toplanmasına yönelik yetkilerin genişlemesi üzerinden değerlendirmektedir. Nitekim Hellmann'a göre; dijitalleşme sonucu ortaya çıkan geniş veri aktarım olanakları, ceza soruşturması makamlarının erişebileceği bilgi alanını ciddi ölçüde genişletmektedir[87]. Bu tespitten yola çıkarak sadece (dijital/elektronik) delil elde etme kapasitesinin artışından değil, bununla beraber ve bilhassa bu kapasitenin nasıl sınırlandırılacağı sorusu da güncel ceza muhakemesi sistemlerinin gündeminde olduğu ifade edilmelidir. Nitekim Alman Ceza Muhakemesi Kanunu'nda (StPO) §100g (iletişim bilgilerinin tespit edilmesi) ve §100h (ilgilinin bilgisi haricindeki sair tedbirler) gibi maddeler, dijital veri aktarımı ve uzaktan erişime ilişkin açık düzenlemeler içermekte; her bir müdahale türü için gerek içerik gerekse kapsam açısından ayrık ve somut denetim kriterleri öngörmektedir[88]. Esasında bu normatif netlik dijital/elektronik verilere müdahale yetkisinin hukuk devleti ilkesiyle uyumlu biçimde sınırlandırılmasını sağlamakta olup ölçülülük ve öngörülebilirlik prensiplerinin somut bir karşılığını oluşturmaktadır.

Türk ceza muhakemesi hukukunda ise mesela CMK 134'üncü, 135'inci ve 140'ıncı maddeleri dijitalleşmenin ortaya çıkardığı veri çeşitliliği ve müdahale düzeylerini ayrıştıracak teknik bir çerçeveden henüz yoksun bulunmaktadır. Ayrıca doktrinde bireysel hak ve özgürlüklere müdahale niteliği taşıyan koruma tedbirleri CMK'da ayrıca ve açıkça düzenlenmiş olduğundan burada yer verilmeyen bir tedbire başvurulmasının

---

86 Zhou and others (n54) 424.

87 Hellmann (n29) 121.

88 Feridun Yenisey, Salih Oktar ve Ayla Oktar, *Alman Ceza Muhakemesi Kanunu Strafprozeßordnung (StPO) ve Kabahatlerde Para Yaptırımına İlişkin Yönerge (RiStBV)* (3. Baskı, Beta Yayıncılık 2020) 130.

Anayasa'nın 13'üncü maddesi hükmü uyarınca imkan dahilinde olmadığı belirtilmektedir[89]. Kanaatimizce Alman ceza muhakemesi hukukundaki yapısal ayrımlar ve normatif açıklık, Türk ceza muhakemesi hukukunun güncel reform ihtiyacını destekleyen önemli bir mukayeseli örnek sunmaktadır. Yine AİHM, içtihatlarında temel hak ve özgürlükleri koruma sorumluluğunu sistematik ve normatif bir çerçeveye oturtmaktadır. Dijital çağda devletlerin bireyler üzerindeki gözetim yetkileri ve iletişimin denetlenmesine ilişkin olarak da özel hayatın gizliliği ile haberleşme özgürlüğü ve adil yargılanma hakkı çerçevesinde değerlendirmelerde bulunduğu görülmektedir[90]. Mesela, Klass and Others v. Germany[91]; Roman Zakharov v. Russia[92]; Szabó and Vissy v. Hungary[93] gibi kararlarında esasınsa siber suçlarla ilgili koruma tedbirleri bakımından dört temel güvencenin sağlanmasını şart koşmaktadır. Bunlar; kanuni dayanak, öngörülebilirlik, etkili yargısal denetim ve yeterli gerekçelendirme olarak karşımıza çıkmaktadır. Söz konusu güvencelerin Türk ceza (muhakemesi) hukukuna da yansıtılması

---

89 Şen, Şahin ve Ceylan (n51) 129; Canbaz Karacif (n70) 235.

90 Bu hakların korunmasının sadece bireysel mahremiyeti değil, ayrıca demokratik toplum düzenini de ilgilendirmektedir. Nitekim, *"ifade hürriyetinin fiili bir değer kazanabilmesi haberleşme hürriyetinin gerçek anlamda kullanılabilmesiyle gerçekleşmekte ve bu iki hürriyet bir bütünün parçaları olarak değerlendirilmektedir."* Bkz. Kayıhan İçel ve Yener Ünver, *Kitle Haberleşme Hukuku* (Beta Yayınları 2005) 21; nakleden, Samsa (n65) 11.

91 Kararın tam metni için bkz. *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978) https://hudoc.echr.coe.int/eng?i=001-57510 Kararda gizli gözetim faaliyetlerinin demokratik toplumlarda belirli hallerde meşru olabileceği kabul edilmekle birlikte, bu tür müdahalelerin keyfiliği önleyecek açık, öngörülebilir ve denetlenebilir kanuni teminatlar altında gerçekleşmesi gerektiği vurgulanmaktadır. Mahkemeye göre; güvenlik gerekçesiyle uygulanan iletişimin denetlenmesine ilişkin tedbirler, bireylerin temel haklarını sınırlayabilir nitelikte olduklarından (ulusal güvenlik, kamu düzeni veya suçla mücadele gibi) meşru bir amaçla, (erişilebilir ve öngörülebilir) hukuki bir dayanakla, ölçülülük ve etkili yargısal denetim mekanizmasına tabi olmaları halinde uygulanmaktadır.

92 Kararın tam metni için bkz. *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) https://hudoc.echr.coe.int/eng?i=001-159324 Karar, bu gözetim düzenlemelerinin Avrupa İnsan Hakları Sözleşmesi (AİHS) 8'inci maddesi bağlamında nasıl denetlenmesi gerektiğine dair önemli örnekler sunmaktadır.

93 Kararın tam metni için bkz. *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) https://hudoc.echr.coe.int/eng?i=001-160020 Mahkeme, söz konusu yaklaşımını daha da somutlaştırarak Macaristan'daki toplu ve önleyici gözetim yetkilerinin ölçülülük ve gerekli denetim mekanizmalarından yoksun olduğunu belirterek ihlal kararı vermektedir. Ayrıca *Libert v. France* kararında da özel sektör işverenlerinin çalışanların dijital iletişimlerini izlemesi olayında bireyin özel hayatına yapılan müdahalenin açık bir yasal düzenlemeye dayanması, kapsamının belirli sınırlar içinde tutulması ve ilgili kişilerin bilgilendirilmesi esasına göre gerçekleştirilmesi gerektiğini ifade etmekte olup sadece devletlerin değil, özel hukuk kişilerince yapılan müdahalelerinin de AİHS standartlarına tabi olduğunu ortaya koymaktadır. Kararın tam metni için bkz. *Libert v France* App no 588/13 (ECtHR, 22 February 2018) https://hudoc.echr.coe.int/rus/?i=001-181273

ve özellikle CMK 134'üncü, 135'inci ve 140'ıncı maddeleri kapsamında uygulanacak dijital/elektronik koruma tedbirleri için özel güvenlik katmanları inşa edilmesi gerektiği düşüncesindeyiz[94]. Böylece söz konusu denetim mekanizmaları yalnızca yargı kararlarının hukuka uygunluğunu değil, aynı zamanda koruma tedbirlerinin uygulanma düzeylerinde özenli davranılmasını sağlayacak bir disiplin oluşturacaktır.

Ezcümle ceza muhakemesinde dijital/elektronik delillerin elde edilmesine yönelik koruma tedbirlerinin hukuk devleti ilkesiyle bağdaşabilmesi için uygulama yetkisinin sınırlandırılması, denetimin güçlendirilmesi ve hesap verebilirliğin sağlanması elzemdir. Eğer bu denge sağlanmazsa teknik kapasite ne kadar yüksek olursa olsun, müdahalelerin meşruiyeti sorunu ile karşı karşıya kalınacaktır. Yukarıdaki başlıklarda tartışılan yapısal eksiklikler ve mukayeseli örnekler de göstermektedir ki dijital/elektronik koruma tedbirlerinin hukuki çerçevesi yalnızca teknik bir düzenleme meselesi değil, aynı zamanda hukuk devleti ilkesinin işlerliğine ilişkin bir sınav alanı da oluşturmaktadır. Bu manada adil (dürüst) yargılanma hakkı, kişinin yargılamanın esasına ilişkin delillere ulaşmasını ve bunlara göre savunma hakkını kullanabilmesini kapsamakta olup kişinin ulaşamadığı ve tartışamadığı bir delile dayanılarak hüküm kurulamayacağını sonuçlamaktadır[95]. Dolayısıyla Türk ceza muhakemesi hukukunda koruma tedbirlerine ilişkin normatif düzenlemeler dijitalleşme gerçekliğiyle uyumlu hale getirilmeli, dijital/elektronik delillerde de kanunilik ilkesi mutlak surette gözetilmelidir[96]. Ayrıca müdahalenin sınırları açıkça belirlenmeli, her düzeyde denetim mekanizmaları etkili bir şekilde işletilmeli ve keyfi uygulamaların önüne bu yollarla muhakkak geçilmelidir. Mevzuatta yapılacak her güncelleme de yalnızca kolluk ve yargı uygulamalarına rehberlik etmekle kalmamalı; bunun yanında anayasal hak ve özgürlükler temelinde dengeleyici ve hesap verilebilir bir ceza muhakemesi kültürünün inşasına da katkı sunmalıdır.

---

[94] Uygulamada mesela, HTS kayıtları haricinde olaya ilişkin başka bir delile ulaşılamayan durumlarda bu kayıtların tek başına yeterli görülmesi mümkün değildir. HTS verileri, ispata elverişli diğer delillerle doğrulanmadıkça bağımsız bir delil olarak hükme esas alınamamakta ve dolayısıyla hakkında sadece bu kayıtlara dayalı suç isnadı bulunan şüpheli, "şüpheden sanık yararlanır/in dubio pro reo" ilkesi gereği cezalandırılmamaktadır. Canbaz Karacif (n70) 244.

[95] Şen, Şahin ve Ceylan (n52) 131.

[96] Aynı yönde, Arslan (n51) 257.

SONUÇ VE ÖNERİLER

Ceza muhakemesi sistemleri, dijitalleşmenin getirdiği yapısal dönüşümler karşısında sadece teknik araçların kullanımına değil, bununla birlikte ve bilhassa usuli güvencelerin korunmasına yönelik kanuni düzenlemelere de gereksinim duymaktadır. Hem dijital/elektronik delillerin toplanması ve muhafazası süreçlerinde ortaya çıkan meseleler hem de koruma tedbirlerinin dijital ortamlarda uygulanabilirliğine dair açık düzenlemelerin eksikliği, ceza adalet sisteminin bütüncül ve çağdaş bir reforma yönelmesini zorunlu kılmaktadır. Bu çerçevede dijital/elektronik delillerin hukuki değeri, ölçülülük (elverişlilik, gereklilik, oranlılık) ilkeleri ve koruma tedbirlerinin dijitalleşme ihtiyacı salt uygulamaya yönelik değil, aynı zamanda kavramsal, kuramsal, kanuni ve anayasal temelli bir güncelleme ihtiyacına işaret etmektedir. Nitekim karşılaşılan çoğu meselelerin merkezinde de ceza (muhakemesi) hukuku kurallarını dijital çağa uyarlama ihtiyacı bulunmaktadır.

Mukayeseli hukuk örnekleri Almanya, Fransa ve ABD gibi devletlerin dijital/elektronik delillere dair kanuni çerçeveleri farklı modellerle yapılandırdığını, bilhassa Fransa'da[97] arşivleme yükümlülüklerinin[98] delilin geçerliliği ile doğrudan bağlantılı olarak düzenlendiğini, Almanya'da dijital mahremiyetin anayasal düzeyde yeni

[97] "Ceza Muhakemesi Kanunu-Code de procédure pénale (CPP)" dijital/elektronik delillerin toplanması ve ceza muhakemesinde kullanılması konusunda ayrıntılı hükümler içermektedir. Bilhassa dijital/elektronik iletişim verilerine erişim sağlanması, belli katalog suçlar kapsamında ve yargı denetimi altında mümkün olabilmektedir. Kanun'un 60-2. maddesi adli kolluk görevlilerine, kamu veya özel kurum ve kişilerden maddi gerçeğin ortaya çıkarılmasına katkı sağlayacak her türlü bilgi, belge ve kişisel veriyi gerektiğinde sayısal (dijital/elektronik) formatta talep etme yetkisi tanımaktadır. Bu hüküm sadece veri temini açısından değil, aynı zamanda usul güvenceleri bakımından da önem teşkil etmektedir. *"Ön soruşturma ihtiyaçları kapsamında adli kolluk görevlileri kişilerden, özel ya da kamuya ait kurum ve kuruluşlardan, ... ellerinde bulundurdukları ve gerçeğin ortaya çıkarılmasına yardımcı olabilecek belgeleri, bilgileri veya kişisel verileri sayısal (dijial/elektronik) format da dahil olmak üzere teslim isteyebilir."* Code de procédure pénale, art 60-2 https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/ Zikredilen kanun, dijital delillerin elde edilmesinde gereklilik, ölçülülük ve yargısal denetim prensiplerini ön plana almakta olup bireylerin temel hak ve özgürlüklerini korumayı amaçlamaktadır. Sabine Marcellin and Pauline Ascoli, "The Archiving of Electronic Documents under French Law" (2010) 7 *Digital Evidence and Electronic Signature Law Review* 108.

[98] Dijital/elektronik delillerin saklanması ve arşivlenmesi süreçleri Fransız hukukunda önem taşımaktadır. Özellikle kamu kurumlarının ve özel hukuk kişilerinin dijital/elektronik belgelerin bütünlüğünü ve değiştirilemezliğini sağlamak üzere kanuni arşivleme yükümlülükleri bulunmaktadır. Bu durum, söz konusu delillerin muhakeme sürecinde güvenilirliğini sürdürmesi bakımından temel bir işlev görmektedir. Antoine Meissonnier and Françoise Banat-Berger, "French Legal Framework of Digital Evidence" (2015) 25 (1) Records Management Journal 96 https://doi.org/10.1108/RMJ-07-2014-0031

bir temel hak olarak tanındığını ve ABD'de Carpenter kararı[99] ile konum verileri dahil olmak üzere meta-verilerin[100] anayasal koruma kapsamına alındığını göstermektedir. Zira teknolojik ilerlemeler yargının daha önce gündeminde olmayan teknolojilerle ilgili olarak kanunları yorumlamakta zorlanmasına yol açmakta olup özellikle ceza muhakesinde uygulanan koruma tedbirleri üzerinde önemli etkiler doğurmaktadır. Diğer taraftan Avrupa İnsan Hakları Mahkemesi'nin içtihatları da dijital gözetim ve iletişim denetimi gibi müdahale araçlarının yalnızca ve yalnızca demokratik toplumda gerekli olduğu hallerde, açık kanuni dayanakla ve etkili yargı denetim mekanizmasıyla birlikte uygulanabileceğini ortaya koymaktadır. Tüm bu değerlendirmeler, kanaatimizce dijital/elektronik delillerin ceza muhakemesi süreçlerinde hak ettiği düzeyde yer bulabilmesi amacıyla gerek ulusal hukuk sistemlerinde kanun seviyesinde açıklığa kavuşturulmaları gerekse de temel hak ve özgürlüklerin korunmasına dair evrensel ilkelerle uyumlu biçimde sınırlandırılmaları gerektiğini ortaya çıkarmaktadır. Bu gerekliliğin çalışmada Türkiye özelinde yapılan normatif analiz açısından da yön gösterici nitelikte olduğunu düşünmekteyiz.

---

[99] 22 Haziran 2018 tarihli kararın tam metni için bkz. Supreme Court of The United States, "Carpenter v. United States" (2018) https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf Bu karar, dijital verilerin korunması açısından dönüm noktası teşkil etmektedir. Mahkeme, son yıllardaki teknolojik gelişmelerin kişisel bilgileri kolluk kuvvetleri için önceki yıllara göre kat kat daha erişilebilir hale getirdiği kabulü üzerinden bireylerin cep telefonu konum verilerinin dördüncü değişiklik kapsamında makul bir gizlilik beklentisi oluşturduğunu ve bu verilerin mahkeme kararı olmaksızın elde edilmesinin anayasal hak ihlali teşkil ettiğini belirtmektedir. Doalyısıyla karar, dijital çağda bireylerin konum bilgilerinin korunması ve devletin bu tür verilere erişiminin sıkı birt yargısal denetim altında olması gerektiğini ortaya koymaktadır. Ayrıntılı açıklamalar için bkz. Aparna Bhattacharya, "The Impact of Carpenter v. United States on Digital Age Technologies" (2020) 29 Southern California Interdisciplinary Law Journal 489; Jay Evans, "Say Cheese: Facial Recognition Technology in a Post-Carpenter World" (2 February 2021) SSRN http://dx.doi.org/10.2139/ssrn.3777997 Son yazar, mahkemelerin yüz tanıma teknolojisi kullanılarak yapılacak herhangi bir aramadan önce aramanın bir arama emri gerektirip gerektirmediğini belirleyebileceği yeni bir analitik çerçeve olan Carpenter Testi'nin yüz tanıma teknolojisinin oluşturduğu tehditlerle bu teknolojinin polise sunduğu faydaları dengeleyeceğini belirtmektedir.

[100] Bu noktada ifade edelim ki meta-veri *(metadata),* içerikten bağımsız olmakla beraber verinin ne zaman, nerede, kim tarafından ve hangi araçla üretildiği gibi niteliklerini tanımlamakta olduğundan ceza muhakemesi bağlamında bilhassa dijital (elektronik) delillerin toplanması ve iletişimin denetlenmesi süreçlerinde **kişisel mahremiyet açısından çok hassas ve değerli olabilmektedir.** Çağatay Yüksel, *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK Md. 134)* (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü 2022) 21. Bu sebeple AİHM içtihatlarında da vurgulandığı üzere meta-verilerin elde edilmesi ve işlenmesi süreçlerinin kanuni ve anayasal güvenceler eşliğinde yürütülmesi bir gereklilik olarak karşımıza çıkmaktadır.

Nitekim dijital çağda ceza muhakemesi sadece teknolojik gelişmelere adapte olma zorunluluğuyla değil, eş zamanlı olarak bireysel hak ve özgürlükleri koruma sorumluluğuyla da yeniden şekillenmektedir. Bilhassa siber suçların kendine has özellikleri, geleneksel ceza muhakemesi müesseselerinin sınırlarını zorlamakta olup mevcut koruma tedbirlerinin delil elde etme ve işleme süreçlerinde eksikliklerini net biçimde gözler önüne sermektedir. Bu çerçevede CMK'da yer alan koruma tedbirlerine ilişkin düzenlemeler, dijital/elektronik ortamlarda uygulanan koruma tedbirleri bakımından hem kavramsal hem de sistematik açıdan güncellenme potansiyeli barındırmaktadır.

Bu çalışma, özellikle Türk ceza muhakemesi hukuku bağlamında dijital dönüşümün etkilerini teknik, normatif, anayasal ve karşılaştırmalı hukuk düzeylerinde ele alan bütüncül bir perspektif sunmayı amaçlamaktadır. AİHM içtihatları ile Almanya, Fransa ve ABD gibi hukuk düzenlerinin verileri ışığında önerilen sınıflandırma modeli (görünür müdahale-uzaktan müdahale-sistem içi izleme) sadece teorik bir çerçeve sunmamakta, hukuk uygulayıcıları bakımından yol gösterici pratik bir referans noktasına da işaret etmektedir.

Yapılması gereken mevzuat güncellemeleri hash alma, imaj oluşturma, meta-veri ayrımı, dijital arşiv yükümlülüğü ve usuli denetim sistematiği gibi teknik bileşenlerin yanı sıra, anayasal güvencelerle uyumlu bir normatif çerçeve oluşturulmasını da zorunlu kılmaktadır. Bu noktada "Dijital Koruma Tedbirleri" başlıklı özel bir düzenleme ile CMK'nın dijital çağın gerekliliklerine göre yeniden yapılandırılması, kanaatimizce hukuki güvenliği ve öngörülebilirliği sağlamakla kalmayacak ayrıca hukuk devletinin temel taşlarından biri olan bireysel hak ve özgürlüklerin korunmasını da güçlendirecektir.

Koruma tedbirlerinin CMK'ya dijital uyarlamayla entegre edilmesi, hem bireysel hak ve özgürlüklerin korunması hem de ceza adalet sisteminin işlevselliği açısından ertelenemez bir ihtiyaç olduğunu düşünmekteyiz. Bununla birlikte, söz konusu entegrasyon sürecinin esnek ve güncellenebilir bir sistem kurulmasını sağlarken temel hak ve özgürlüklerin özüne dokunmayan, ölçülülük ve yargısal denetim ilkelerine dayalı bir yapıyla yürütülmesi elzem niteliktedir. Nitekim ceza muhakemesi, "anayasanın sismografyası" olarak hukuki sistemin en hassas denge alanlarından birine karşılık

gelmektedir. Dolayısıyla her teknik ve kanuni değişikliğin anayasal dengeye saygı temelinde tasarlanması gerekmektedir.

Gerçekten de dijitalleşmenin ceza muhakemesi üzerindeki etkisi salt araçsal bir dönüşüm değil, aynı zamanda hukukun temel ilkelerinin yeniden tanımlanmasını ve güvenceye bağlanmasını gerektiren yapısal bir kırılma olarak tezahür etmektedir. Bu dönüşüm sürecinde kanun koyucunun görevi sadece teknolojiyi yakalamak değil, ayrıca bireylerin haklarını koruyacak dengeleyici ve hesap verilebilir nitelikte kuralları üretmek olmalıdır. Bu yönüyle çalışma, Türk ceza muhakemesi sistemine özgü ihtiyaçları gözetmek suretiyle hem teoriye hem uygulamaya katkı sağlayan ve nihayetinde Türk ceza muhakemesi hukukunda dijitalleşmeye uyum sürecine rehberlik edecek özgün ve güncel bir normatif çerçeve ortaya koymaktadır.

KAYNAKÇA

Akarslan H, *Bilişim Suçları* (2. Baskı, Seçkin Yayıncılık 2015).

Akyeşilmen N, "Siber Uzay ve İnsan Hakları: Dijital Çağda İnsan Haklarını Korumak" *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik* (1. Baskı, Orion Kitabevi 2018).

Aliusta C ve Benzer R, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci" (2018) 4 (2) *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 35-42.

Apaydın C, "Bilişim Suçlarında Etkin Soruşturma ve Yargılama" (Ceza Hukuku Bilinci, 14 Haziran 2025) 1 https://www.cezahukukubilinci.org/bilisim-suclarinda-etkin-sorusturma-ve-yargilama/

Arslan Ç, "Dijital Delil ve İletişimin Denetlenmesi" (2015) 3 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 253-266.

Ateş Benek N, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" (2022) 10 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 367-411.

Bacaksız P ve Bayzit T, "Yargı Kararları Işığında Ceza Muhakemesi Hukukunda Fotokapan Vasıtasıyla Elde Edilen Görüntülerin Kullanılması Sorununa İlişkin Değerlendirmeler" (2022) (185) *Terazi Hukuk Dergisi* 50-59.

Başlar Y, "Elektronik Delilin Toplanması ve Muhafazası" (2020) 10 (1) *Hacettepe Hukuk Fakültesi Dergisi* 77-107.

Bertel C and Venier A, *Einführung in die neue Strafprozessordnung* (2nd edn, Springer 2006).

Bhattacharya A, "The Impact of Carpenter v. United States on Digital Age Technologies" (2020) 29 *Southern California Interdisciplinary Law Journal* 489-513.

Birtek F, "Teixeira de Castro/Portekiz Davası (44/1997/828/1034)" (2010) (91) *Türkiye Barolar Birliği Dergisi* 409-430.

Boyracı A, "Gizli Soruşturmacının Konuta Girme Yetkisi ve Bu Yetkinin Kapsamı Üzerine Bir İnceleme" (2024) 14 (2) *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 1239-1304.

Canbaz Karacif F E, "İletişimin Tespiti Kayıtları (HTS) ve Haberleşme Özgürlüğü" (2024) 14 (1) *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi* 233-256.

Casey E, *Digital Evidence and Computer Crime* (3rd edn, Elsevier 2011).

Centel N ve Zafer H, *Ceza Muhakemesi Hukuku El Kitabı,* (7. Baskı, Beta Yayıncılık 2021).

Chandra R and Prasad P W C, "Cyber Warfare: Challenges Posed in a Digitally Connected World: A Review" in Subhas Chandra Mukhopadhyay, S.M. Namal Arosha Senanayake and P. W. Chandana Withana (eds), *Innovative Technologies in Intelligent Systems and Industrial Applications* (Lecture Notes in Electrical Engineering, vol 1029, Springer 2023) https://doi.org/10.1007/978-3-031-29078-7_16

Chen S and others, "The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China" (2021) 10 (12) *ISPRS International Journal of Geo-Information* https://doi.org/10.3390/ijgi10120802

Council of Europe, *Electronic Evidence Guide Version 3.0* (Cybercrime Programme Office 2022) https://kanuni.taa.gov.tr/assets/dosyalar/Dijital_Delil_Kilavuzu_WEB.pdf

Council of Europe and INTERPOL, *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* (Council of Europe 2020) https://www.coe.int/en/web/cybercrime

Çatlı M, "Yapay Zekanın Anayasası: 'Akıllı Anayasa' Üzerine" (2023) 1 (70) *Adalet Dergisi* 369-383.

Çekiç B, "Bilgisayar Verilerinde Arama, Kopyalama, El Koyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar" (2021) 2 (1) *Tekirdağ Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi* 153-185.

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

Demirci Ö, *Bilişim Suçları ve Soruşturma Yöntemleri* (1. Baskı, Seçkin Yayıncılık 2022).

Dmitrieva A A and Pastukhov P S, "Concept of Electronic Evidence in Criminal Legal Procedure" (2023) 1 (1) *Journal of Digital Technologies and Law* https://doi.org/10.21202/jdtl.2023.11

Doğan R, "Ceza Muhakemesi Hukukunda İletişimin Denetlenmesi Tedbiri ve AİHM Yaklaşımı" (2024) 2 (73) *Adalet Dergisi* 121-163.

Du H and Yang S J, "Temporal and Spatial Analyses for Large-Scale Cyber Attacks" in V. S. Subrahmanian (ed), *Handbook of Computational Approaches to Counterterrorism* (Springer, 2013) https://doi.org/10.1007/978-1-4614-5311-6_25

Dülger M V, *Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri (Search, Copy and Seizure Measures on Information Systems)* (24 Şubat 2021). http://dx.doi.org/10.2139/ssrn.3792260

Dülger M V, *Bilişim Suçları ve İnternet İletişim Hukuku* (10. Baskı, Seçkin Yayıncılık 2023).

Dülger M V ve Taşkın Ş C, *Ceza Muhakemesi Hukuku* (2. Baskı, Seçkin Yayıncılık 2024).

Erdem M ve Özocak G, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri" (4. Uluslararası Bilişim Hukuku Sempozyumu, İzmir, 12-14 Mayıs 2016).

Ersoy Y, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları" (1994) 49 (3) *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* 149-183.

Evans J, "Say Cheese: Facial Recognition Technology in a Post-Carpenter World" (2 February 2021) SSRN http://dx.doi.org/10.2139/ssrn.3777997

George E, Jameison M ve Kumkumoğlu K, *Siber Suçların Önlenmesi ve Bu Suçlarla Mücadele: Türkiye İçin Temel Bulgular ve Tavsiyeler* (Avrupa Konseyi 2023).

Godin B, "Innovation Without the Word: William F. Ogburn's Contribution to the Study of Technological Innovation" (2010) 48(3) *Minerva* https://www.jstor.org/stable/41821527

Goldstraw-White J, *Legal and Policy Framework for Digital Forensics: A Resource for Practitioners* (Perpetuity Research and Consultancy International Ltd, University College London and the Institute Crime & Justice Policy Research 2022).

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

Göksoy R, *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması* (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü 2017).

Hellmann U, *Strafprozessrecht* (2nd edn, Springer 2006).

Herman A P, "An Answer to Criticisms of the Lag Concept" (1937) 43 (3) *American Journal of Sociology* https://www.jstor.org/stable/2768630

Martin Hussels, *Strafprozessrecht-schnell erfasst* (2nd edn, Springer 2008).

İçel K ve Ünver Y, *Kitle Haberleşme Hukuku* (Beta Yayınları 2005).

Karakehya H, "Suçu Önleyici Kolluk Faaliyetleri" in Filiz Tepecik (ed), *Suç Önleme Modelleri* (Anadolu Üniversitesi Yayınları 2016).

Kaya M B, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim" in Şeref Sağıroğlu ve Mustafa Şenol (eds), *Siber Güvenlik ve Savunma: Problemler ve Çözümler* (1. Baskı, Grafiker Yayınları 2019)

Kaya M B, *Polisin Sanal Devriye Yetkisini İptal Eden Anayasa Mahkemesi Kararının Değerlendirilmesi,* https://mbkaya.com/hukuk/polis-sanal-devriye-siberkolluk-aym-iptal.pdf

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

Keskin S, "Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar" (2021) 2 (1) *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi* 649-667.

Ketizmen M, "İnternet Bankacılığı Aracılığıyla Başkalarının Hesaplarında Usulsüz İşlemler Yapılması Suretiyle Yarar Sağlanmasında Suçun Mağduru" (2024) 4 (2) *Kırıkkale Hukuk Mecmuası* 1001-1015.

Kshetri N, "Diffusion and Effects of Cyber-Crime in Developing Economies" (2010) 31 (7) *Third World Quarterly* https://doi.org/10.1080/01436597.2010.518752

Marcellin S and Ascoli P, "The Archiving of Electronic Documents under French Law" (2010) 7 *Digital Evidence and Electronic Signature Law Review* 108-113.

Meissonnier A and Banat-Berger F, "French Legal Framework of Digital Evidence" (2015) 25 (1) *Records Management Journal* https://doi.org/10.1108/RMJ-07-2014-0031

Oğuz R ve Eryiğit R, "Yeni Adli Bilişim İnceleme Süreci (YABİS)" (2024) 36 (2) *Fırat Üniversitesi Mühendislik Bilimleri Dergisi* 717-724.

Osco Escobedo M A and others, "Digital Evidence as a Means of Proof in Criminal Proceedings" (2024) 18 (4) *Revista de Gestão Social e Ambiental* https://doi.org/10.24857/rgsa.v18n4-028

Önok M, "Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" in *İletişim Özgürlüğüne Müdahale* (Türkiye Barolar Birliği Yayınları 2011).

Özbek V Ö, *Polis Hukuku, İnternet Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler ve Hukuka Aykırı Müdahalelere Karşı Korunma Çareleri,* (2. Baskı, Seçkin Yayıncılık 2023).

Özbek V Ö, Doğan K ve Bacaksız P, *Ceza Muhakemesi Hukuku* (17. Baskı, Seçkin Yayıncılık 2024).

Özcan F B, *Elektronik Delillerin Ceza Muhakemesi Bakımından İspat Değeri* (1. Baskı, Yetkin Yayınları 2024).

Özkaya P, *Adli Bilişimde Özel Araştırma ve Soruşturma Yöntemleri* (1. Baskı, Seçkin Yayıncılık 2022).

Öztürk B, Eker Kazancı B ve Soyer Güleç S, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri* (5. Baskı, Seçkin Yayıncılık 2022).

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

Park S, *Der Schutz personenbezogener Daten im Strafverfahren: Eine rechtsvergleichende Untersuchung zum deutschen und US-amerikanischen Recht* (1st edn, Nomos 2021).

Prysiazhniuk I, "Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection" (2023) 5 *Visegrad Journal on Human Rights* https://doi.org/10.61345/1339-7915.2023.5.11

Sabillon R, Cano J, Cavaller V and Serra J, "Cybercrime and Cybercriminals: A Comprehensive Study" (2016) 4 (6) *International Journal of Computer Networks and Communications Security* https://www.proquest.com/scholarly-journals/cybercrime-cybercriminals-comprehensive-study/docview/1874038161/se-2?accountid=15875

Samsa N, *Kamu Haberleşme Hürriyeti Kapsamında İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Denetlenmesi* (Yüksek Lisans Tezi, Pamukkale Üniversitesi 2010).

Sapan O, *Ceza Muhakemesinde Yapay Zeka Kullanımı* (1. Baskı, Adalet Yayınevi 2024).

Sarsıkoğlu Ş, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı" (2015) 6 (22) *Türkiye Adalet Akademisi Dergisi* 427-454.

Schroeder F-C and Verrel T, *Ceza Muhakemesi Hukuku* (tr Salih Oktar, 1. Baskı, Yetkin Yayınları 2019).

Sieber U, *İnternetteki Suçlar ve Suçun İnternette Takibi* (Editör: Yener Ünver, 1. Baskı, Seçkin Yayıncılık 2014).

Sümer S Y, "Ceza Muhakemesinde Mobil Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları" (2022) 87 (1) *İzmir Barosu Dergisi* 61-119.

Şahbaz İ, "Koruma Tedbiri Olarak İletişimin Denetlenmesi" in Süheyl Donay ve Aysun Altunkaş (eds), *Ceza Yargılama Hukukunda Son Gelişmeler Sempozyumu* (1. Baskı, Seçkin Yayıncılık 2016).

Şahin C, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme" (2007) 11 (1–2) *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 1095-1112.

Şahin C ve Göktürk N, *Ceza Muhakemesi Hukuku,* (15. Baskı, Seçkin Yayıncılık 2024).

Şen E ve Bayraklı T B, "CMK m.135'de Yer Alan İletişimin Denetlenmesi ve Süreleri" (Ersan Şen Hukuk ve Danışmanlık, 25 Ekim 2023) https://sen.av.tr/tr/makale/CMK-m-135-de-yer-alan-iletisimin-denetlenmesi-ve-sureleri

Şen E ve Bayraklı T B, "Polisin Sanal Ortamda Takibi ve Sanal Devriye Yetkisi" (Ersan Şen Hukuk ve Danışmanlık, 22 Aralık 2023) https://sen.av.tr/tr/makale/polisin-sanal-ortamda-takibi-ve-sanal-devriye-yetkisi

Şen E, Şahin B ve Ceylan D, "Sky ECC İletişim Sağlayıcısından Elde Edilen Delillerin Hukukiliği" (2025) 224 *Terazi Hukuk Dergisi* 128-134.

Şentürk C, "Ceza Muhakemesi Hukuku Özelinde Yargıda Dijitalleşme" (2021) 25 (2) *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 755-785.

Şentürk Akaner C, *Bir Koruma Tedbiri Olarak Online Arama ve Türk Hukukunda Uygulanabilirliği* (1. Baskı, Seçkin Yayıncılık 2022).

Tezcan D, Erdem M R ve Önok R M, *Teorik ve Pratik Ceza Özel Hukuku* (22. Baskı, Seçkin Yayıncılık 2024).

Turinay F Y, "Ceza Muhakemesi Hukukunda Teknik Araçlarla İzleme" (2021) 12 (46) *Türkiye Adalet Akademisi Dergisi* 413-454.

Turinay F Y, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması" (2021) 70 (2) *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 475-541.

Ünver Y ve Hakeri H, *Ceza Muhakemesi Hukuku Cilt I* (11. Baskı, Adalet Yayınevi 2016).

Weber A M, "The Council of Europe's Convention on Cybercrime" (2003) 18 (1) *Berkeley Technology Law Journal* 425-446.

Yaşar E, *Maddi ve Şekli Suç Hukuku Boyutlarıyla Klasik Ceza Muhakemesine Alternatif Usuller* (1. Baskı, Seçkin Yayıncılık 2022).

Yaşar O ve Otacı C, *Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu I. Cilt Madde 1-156*, (11. Baskı, Seçkin Yayıncılık 2025).

Yeldan D, *Siber Suçlar* (2. Baskı, Seçkin Yayıncılık 2023).

Yenisey F, Oktar S ve Oktar A, *Alman Ceza Muhakemesi Kanunu Strafprozeßordnung (StPO) ve Kabahatlerde Para Yaptırımına İlişkin Yönerge (RiStBV)* (3. Baskı, Beta Yayıncılık 2020).

Yenisey F ve Nuhoğlu A, *Ceza Muhakemesi Hukuku* (12. Baskı, Seçkin Yayıncılık 2024).

Yıldırım A ve Kılıç A, "Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Silahların Eşitliği İlkesi" (2021) 9 (2) *Ceza Hukuku ve Kriminoloji Dergisi* 341-411.

Yılmaz S, *Türk Ceza Hukuku Sisteminde Siber Suçlar* (2. Baskı, Adalet Yayınevi 2023).

Yüksek F K, "AİHM İçtihatlarında Kişisel Verilerin Korunması (Karar İncelemesi)" (2023) 25 (1) *Dokuz Eylül Üniversitesi Hukuk Fakültesi* Dergisi 371-420.

Yüksel Ç, *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK Md. 134)* (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü 2022).

Zhou Y and others, "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality" (2024) 19 *Asian Journal of Criminology* 423 https://doi.org/10.1007/s11417-024-09436-y

Zhuo J and others, "The Spatiotemporal Patterns and Driving Factors of Cybercrime in the UK during the COVID-19 Pandemic" (2024) 11 *Humanities and Social Sciences Communications* https://doi.org/10.1057/s41599-024-04051-9