İSTANBUL UNIVERSITY PRESS

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology,
JPLC 2025, 13 (2): 429–451

https://doi.org/10.26650/JPLC2025-1704863
Başvuru | Submitted 23.05.2025
Revizyon Talebi | Revision Requested 04.07.2025
Son Revizyon | Last Revision Received 03.11.2025
Kabul | Accepted 24.11.2025
Online Yayın | Published Online 18.12.2025

Araştırma Makalesi | Research Article

Açık Erişim | Open Access

Siber Suç Soruşturmasında Karşılaşılan Başlıca Sorunlar

Key Challenges in Cybercrime Investigations

Görkem Nazlı Çelik [1] & Sevil Atasoy [1]

[1] Üsküdar Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Adli Bilimler Bölümü, Bağımlılık ve Adli Bilimler, İstanbul, Türkiye

Öz

Siber suçlar, dijitalleşmenin hız kazanmasıyla birlikte hem nitelik hem de nicelik bakımından artış göstermiş, ceza adalet sistemlerini önemli ölçüde etkilemiştir. Adalet Bakanlığı'nın 2009 ile 2023 yılları arasındaki verileri Türkiye'de siber suç vakalarında keskin bir artış olduğunu ortaya koymaktadır. Ancak soruşturma süreçlerinin uzaması, kamu davası açılma oranlarının düşüklüğü ve mahkumiyet kararlarının sınırlı sayıda kalması, sistemdeki işleyiş sorunlarını gözler önüne sermektedir. Bu çalışma, Türkiye'de ceza muhakemesi sisteminin siber suçlarla mücadelede karşılaştığı yapısal ve işleyişe dair sorunları ortaya koymaktadır. Dijital delillerin toplanması, korunması ve analizine ilişkin teknik altyapı ve yasal çerçevede önemli eksiklikler bulunduğu; sürecin sıklıkla uzman yetersizliği ve koordinasyon eksikliği nedeniyle sekteye uğradığı tespit edilmektedir. Siber suçlarla ilgili kamuoyu farkındalığının yetersiz olması, mağdurların ihbar etmekte çekimser kalması, yasal çerçevenin hızlı gelişen teknolojilere ayak uyduramaması ve uluslararası iş birliği mekanizmalarının sınırlılığı da mücadeleyi zorlaştırmaktadır. Bu sorunların tespiti ve çok yönlü olarak ele alınması, ceza adalet sisteminin dijital çağda etkili işleyişi açısından büyük önem taşımaktadır. Çalışma, uluslararası kurum raporları ve ampirik çalışmalara yönelik alanyazın taraması üzerinden mücadeledeki hukuki, teknik ve operasyonel engelleri analiz ederek siber suçla mücadelede karşılaşılan sorunlara yönelik bütüncül bir yaklaşım sunmayı hedeflemektedir.

Abstract

Cybercrimes have increased in both quality and quantity with the acceleration of digitalization and have significantly affected criminal justice systems. The data of the Ministry of Justice between 2009 and 2023 reveal a sharp increase in cybercrime cases in Turkey. However, the prolongation of the investigation processes, the low rate of filing public lawsuits, and the limited number of convictions reveals operational problems in the system. This study examines the structural and operational problems faced by the criminal justice system in Turkey in the fight against cybercrimes. It has been determined that there are significant deficiencies in the technical infrastructure and legal framework for the collection, preservation, and analysis of digital evidence; the process is frequently hampered by a lack of expertise and coordination. In addition, insufficient public awareness of cybercrimes, the reluctance of victims to report, the failure of the legal framework to keep pace with rapidly developing technologies, and the limited availability of international cooperation mechanisms also make the fight difficult. Identifying and addressing these problems multifaceted is of great importance for the effective functioning of the criminal justice system in the digital age. This study aims to provide a holistic approach to the problems encountered in the fight against cybercrime by analyzing the legal, technical and operational obstacles in the fight, utilizing a literature review of empirical studies and international institution reports.

Anahtar Kelimeler Siber suç · ceza adaleti · dijital delil.

Keywords Cybercrime · criminal justice · digital evidence.

Atıf | Citation: Çelik, G. N. & Atasoy, S. (2025). Siber Suç Soruşturmasında Karşılaşılan Başlıca Sorunlar. *Ceza Hukuku ve Kriminoloji Dergisi–Journal of Penal Law and Criminology*, *13*(2), 429-451. https://doi.org/10.26650/JPLC2025-1704863

Sorumlu Yazar | Corresponding author: Görkem Nazlı Çelik gorkemnazli.celik@st.uskudar.edu.tr

Extended Summary

The crossborder and rapidly evolving nature of cybercrimes renders traditional definitions of crime and prosecution mechanisms inadequate, often resulting in impunity for many offenses. A comparative analysis of the Ministry of Justice's earliest and most recent data (2009–2023) reveals that although the number of investigations and prosecutions related to cybercrimes has multiplied since 2009, the number of convictions has remained disproportionately low. Moreover, the fact that a significant portion of public cases heard in 2023 were carried over from previous years serves as a strong indicator of widespread procedural delays. This study aims to identify the principal structural, legal, technical, and social challenges encountered in cybercrime investigations in Turkey. By synthesizing the findings in the existing literature, it provides a thematic and comparative framework regarding Turkey's capacity to combat cybercrime.

The research employs a document-based qualitative observation technique. Within this scope, academic articles, postgraduate theses, official reports, and international documents published in Turkish and English between 2009 and 2025 were reviewed. The findings of qualitative and quantitative field studies on criminal justice systems in different countries were comparatively analyzed, and common problem areas were grouped under three main themes: legal obstacles and regulatory differences, technical and operational challenges, and social and institutional barriers. Due to limitations in accessing primary field data, the study is based on secondary source analysis. In this respect, it offers a comprehensive synthesis of the existing literature specific to Turkey and provides a conceptual foundation for future empirical research.

The findings indicate that Turkey faces definitional ambiguities in cybercrime terminology, a lack of legislative adaptation to technological advances, insufficient technical capacity, and a shortage of specialized human resources. The definitions of cybercrimes regulated under Articles 243–246 of the Turkish Penal Code fail to encompass the emerging types of digital offenses. This situation increases definitional inconsistencies at the international level and complicates mutual legal assistance processes. Furthermore, Article 134 of the Turkish Code of Criminal Procedure, which governs searches and seizures of digital data, does not adequately cover new technological components such as mobile devices and cloud computing. This omission leads to ambiguity in both the evidence collection and the protection of fundamental rights. Divergent interpretations of this article in the literature have resulted in inconsistent judicial practices and, in some cases, inconclusive investigations.

Another major finding of the study is that technical challenges in obtaining and preserving digital evidence constitute a significant barrier to effective cybercrime prosecution. The volatile and easily alterable nature of digital data, the offenders' ability to conceal their identities, and the storage of data on servers located abroad complicate the processes of evidence collection and handling both technically and legally. The limited number of forensic IT experts in Turkey, the inadequacy of the technical infrastructure, and the insufficient training of personnel within the criminal justice system negatively affect the investigation processes. Moreover, the lack of technical expertise among many prosecutors and judges regarding the nature of digital evidence often leads to delays, misinterpretations, and in some cases, unjust acquittals.

The slowness and bureaucratic obstacles in international mutual legal assistance mechanisms are also identified as structural challenges. The requirement for multilingual document translation, lengthy approval procedures, and frequent procedural errors lead to the rejection or delay of requests. Although the Council of Europe's Convention on Cybercrime includes provisions aimed at expediting bureaucratic processes, its lack of enforceable sanctions weakens the effectiveness of current cooperation efforts. Turkey's nonaccession to the Second Additional Protocol further hampers the efficiency of crossborder digital evidence sharing.

At the societal level, the lack of public awareness regarding cybercrime constitutes another critical impediment. Many victims remain unaware that the violations they experience amount to criminal acts, or they refrain from filing complaints due to the complexity of the process. Commercial entities motivated by reputational concerns also avoid reporting cyber incidents, resulting in many crimes remaining unrecorded. Consequently, the visibility of cyber offenses diminishes, undermining the reliability of official data and statistical assessments. The overall findings demonstrate that the difficulties in combating cybercrime form a cyclical structure shaped by interacting legal, technical, and social factors. While definitional ambiguities restrict international cooperation, technical and personnel shortages slow down investigation processes, and the lack of public awareness perpetuates underre-

porting, reinforcing the cycle. Therefore, addressing these challenges requires not only legislative reform but also a multilayered and holistic policy approach.

In conclusion, effective cybercrime prevention and prosecution in Turkey necessitate a multidimensional strategy that integrates legal innovation, technical expertise, institutional collaboration, and international engagement—supported by public awareness and transnational cooperation. Addressing these systemic deficiencies will enable Turkey to advance toward a more resilient criminal justice system capable of responding effectively to the demands of the digital age.

Giriş

Bilgisayar ve bilişim teknolojileri, ilk kullanılmaya başladıkları 1940'lı yıllardan bugüne hızlı bir gelişim göstererek günlük yaşamın bir parçası haline gelmiştir. Günümüzde bilişim sistemlerinin vazgeçilmezi olan internet kullanımıysa, Türkiye'ye 1993 yılında başlamış olmasına rağmen; 2024 yılı TÜİK Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 16-74 yaş aralığındaki nüfusun %88,8'inin internet erişimi olduğunu göstermekte, bu da internetin toplumun büyük bir çoğunluğu tarafından yaygın olarak kullanıldığını ortaya koymaktadır[1]. Bilişim sistemleri ve internetin hem bu denli yaygın kullanımı hem de fiziksel dünyanın sınırlarını ortadan kaldırarak günlük hayatın tüm yönlerine hakim olabilmesi, sanal ortamda suç işleme fırsatlarını da beraberinde getirmektedir. Bazı siber güvenlik istatistikleri, 2021 yılında siber veri ihlallerinden kaynaklı saatte 97 kişinin mağdur olduğunu ortaya koyarken; IBM Veri İhlalleri Raporu, 2024 yılında bu ihlallerin maliyetinin ortalama 5 milyon dolara yaklaştığını rapor etmiştir[2]. Interpol'ün 2022 yılında yayınladığı Küresel Suç Trendleri Raporu'ysa, siber suçu küresel çapta suç tehdidinin yoğunlaştığı beş suç tipinden biri olarak değerlendirmekte ve dijitalleşmenin bu beş suç tipine ilişkin tehdidi arttırmasının yanı sıra, suç tiplerinin birbirlerini desteklediği kolaylaştırıcı bir etken olduğunu ifade etmektedir[3].

Tüm dünyada olduğu gibi Türkiye'de de siber suçların sayısındaki artış, bu suçlarda ceza adalet sistemine yansıyan sayıların da artmasına sebep olmaktadır. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nün internet sayfasındaki arşivde yer alan en eski istatistik olan 2009 yılı Adalet İstatistikleri'nin "bilişim alanında suçlar" başlığında (TCK m. 243-246) toplam 29 bin 967 şüpheli hakkında cumhuriyet başsavcılıkları tarafından soruşturma aşamasında işlem yapılmışken; bu sayı 2023 yılı Adalet İstatistikleri'nde 406 bin 124'e ulaşmıştır[4]. Ancak 2023 yılında istatistiklere yansıyan bu sayının yalnızca 85 bin 274'ü yıl içinde gelen şüphelilerden oluşurken, 320 bin 850 şüphelinin ise bir önceki yıldan devreden soruşturma dosyalarına ilişkin olduğu rapora yansımaktadır. 2023 yılında soruşturma evresinde toplam 116 bin 581 bilişim alanında suç[5] karara bağlanmış olmasına rağmen, bunların yalnızca 27 bin 740'ı hakkında kamu davası açılması kararı verilmiş olup, suçların yarısından fazlası hakkında kamu davası açılmasına yer olmadığına dair karar verilmiştir.

[1] Necmettin Yazıcı, 'Türk Ceza Hukukunda Bilişim Suçları (TCK. M. 243-244 ve 245)' (Yayımlanmamış Yüksek Lisans, Fatih Sultan Mehmet Vakıf Üniversitesi 2021) 11; TÜİK, 'Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2024' 25 Kasım 2024 tarihinde erişildi.

[2] Charles Griffiths, 'The Latest 2024 Cyber Crime Statistics' (AAG, 1 October 2024) 25 Kasım 2024 tarihinde erişildi; IBM, 'Cost of a Data Breach Report 2024' (2024) 28 Kasım 2024 tarihinde erişildi.

[3] Interpol, '2022 Interpol Global Crime Trends Summary Report' (2022) 3–4. Küresel Suç Trendleri Raporu'na göre siber suçların yanı sıra küresel çapta tehdit oluşturan diğer suç tipleri şu şekildedir: organize suç, terörizm, kaçakçılık ve yolsuzluk.

[4] Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, 'Adalet İstatistikleri 2009' (2009) 29 Ekim 2024 tarihinde erişildi; Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, 'Adalet İstatistikleri 2023' (2024) 07 Ekim 2024 tarihinde erişildi.

[5] Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, 'Adalet İstatistikleri 2023' (n 4). 2023 yılı Adalet istatistiklerine göre, Cumhuriyet başsavcılıklarında TCK uyarınca açılan soruşturma dosyalarında toplam suç sayısı 21 milyon 253 bin 325 olup; bu suçlardan 3 milyon 461 bin 514'ü hırsızlık (TCK 141-147), 2 milyon 437 bin 87'si dolandırıcılık (TCK 157-159), 2 milyon 459 bin 709'u şerefe karşı suçlar (TCK 125-131) ve 263 bin 54'ü özel hayata ve hayatın gizli alanına karşı suçlardan (TCK 132-140) oluşmaktadır. Ancak, bu suçlardan kaçında bilişim sistemlerinin aracı kılındığına dair ayrıntılı istatistik bulunmaması sebebiyle istatiksel değerlendirmeye dahil edilmemişlerdir.

2009 yılı istatistiklerine göre, bilişim alanında suçlar kapsamında hakkında kamu davası açılmış olan toplam suç sayısı 11 bin 393 iken, bu sayı 2023 yılında 92 bin 39'a yükselmiş ancak, bu suçların yalnızca 26 bin 193'ü söz konusu yıl içinde açılmıştır. 2023 yılında hakkında karar verilen bilişim alanındaki toplam sanık sayısı 14 bin 703 iken, bunların yalnızca 5 bin 810'u hakkında mahkumiyet kararı verilmiştir. Bilişim suçlarına yönelik istatiksel veriler karşılaştırıldığında, yıllar içinde ceza adalet sistemine yansıyan suç ve dosya sayısında artış olmasına rağmen, bu dosyaların sonucunda verilen mahkumiyet kararları belirgin biçimde az olduğu görülmektedir. Ayrıca, 2023 yılında bilişim alanında suç içeren dosyalar incelendiğinde, bunların önemli bir kısmının bir önceki yıldan devrettiği ve dolayısıyla, soruşturma ve kovuşturma süreçlerinin her birinin bir yıldan uzun sürdüğü sonucuna varılmaktadır. Bilişim alanındaki suçlarda ceza muhakeme sürecinin bu denli uzun sürmesiyle bu kadar az sayıda mahkumiyet kararı verilmesiyse, delillerin kaybolmasına, fail olmayan şüpheli ve sanıkların uzun süren yargılamalara maruz kalarak adil yargılanma hakkının zedelenmesine ve kamu kaynaklarının boşa harcanması gibi sorunlara sebep olabilmektedir.

Bununla birlikte, hukuki düzenlemelerdeki farklılıklar, uluslararası iş birliği eksiklikleri ve teknik zorluklar, siber suçlarla etkin mücadeleyi küresel çapta zorlaştırmaktadır. Siber suçların fiziksel sınırlardan bağımsız olarak işlenebilmesi, fail ve mağdurun farklı ülkelerde bulunabilmesi, dijital delillerin uçucu olması gibi nedenlerle, kolluk kuvvetleri ve yargı sistemleri bu suçları soruşturma ve cezalandırma konusunda büyük engellerle karşılaşmaktadır.

Bu çalışma, Türkiye'de siber suç soruşturmalarında karşılaşılan temel yapısal sorunları ortaya koymayı amaçlamaktadır. Belgelere dayalı nitel araştırma yöntemiyle yürütülen çalışmada, 2009–2025 yılları arasında yayımlanmış Türkçe ve İngilizce akademik ve kurumsal kaynaklar incelenmiş; bulgular karşılaştırmalı biçimde değerlendirilerek hukuki, teknik ve toplumsal engeller olmak üzere üç ana tema belirlenmiştir. Çalışma, ikincil kaynaklarla sınırlıdır. Çalışma, Türkiye'de siber suçla mücadeleye ilişkin mevcut literatüre tematik ve karşılaştırmalı bir çerçeve sunmayı amaçlamaktadır.

I. Siber Suçun Tanım ve Sınıflandırma

Siber suçların tanımını yapmak ve çerçevesini çizmek, hukuki düzenlemelerin sağlam bir zemine oturtulması, suçun boyutlarının belirlenmesi, müdahale ve önleme stratejilerinin geliştirilmesi, kriminolojik analizlerin yapılması ve istatistiksel verilerin oluşturulmasını sağlaması gibi nedenlerle önemli görülmektedir[6]. Dolayısıyla, tanım hem hukuki çerçevenin hem de uygulamaya ilişkin tüm kurumların temel hareket noktasıdır. Bu sebeple çalışmanın bu bölümünde siber suçun tanımına ve sınıflandırılmasına yönelik farklı yaklaşımlar ele alınmıştır.

Siber suç terimi, ilk olarak 1970'li yıllarda, "bilgisayar tarafından işlenen suçlar" olarak ortaya çıkmış olup, çoğunlukla bilgisayar suçu veya bilgisayarla ilgili suçlar kavramlarıyla ifade edilmiştir[7]. Zamanla bu suçların yaygınlaşmasıyla araştırma çevrelerinde bilgisayar suçu, dijital suç, elektronik suç, internet suçu, teknoloji suçu, sanal suç terimleri de kullanılmaya başlanmıştır[8]. Turhan da 2006 yılında gerçekleştirdiği bir çalışmasında, siber suç teriminin "bir bilgisayar sistemi veya ağı aracılığıyla bir bilgisayar sistemi veya ağında veya bir bilgisayar sistemi veya ağına karşı gerçekleştirilen eylemler" olarak tanımlanabileceğini, Avrupa Birliği'nin de bir bildirisinde bilgisayar suçunu bu anlamda tanımladığını ve aynı anlama gelen

[6] Thomas J Holt ve Adam M Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020) 4–5.

[7] Abdullah Aldoori, 'Uluslararası Hukukta Siber Suçla Mücadele' (Yayımlanmamış Yüksek Lisans, İstanbul Üniversitesi 2020) 5; ER. Leukfeldt ve Thomas J. Holt, *The Human Factor of Cybercrime* (Routledge 2020) 8; Oğuz Turhan, 'Bilgisayar Ağları Ile Ilgili Suçlar (Siber Suçlar)' (Planlama Uzmanlığı Tezi, TC BAŞBAKANLIK DEVLET PLANLAMA TEŞKİLATI MÜSTEŞARLIĞI 2006) 27.

[8] Brian K Payne, 'Defining Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020) 9.

siber suçun da kullanıldığını ifade etmiştir[9]. Ancak bilişim sistemlerinin ve internetin hızla gelişmesiyle birlikte, siber suç terimi bilgisayarın ötesinde daha geniş, materyal dünyadan farklı bir ortam olan siber uzayda gerçekleşen hukuka aykırı eylemleri kapsayan genel bir kavram olarak kullanılmaya başlanmıştır[10]. Buna rağmen, bu kavramın kapsamı ve sınırları konusunda hem akademik çevrelerde hem de uluslararası kuruluşlar arasında ortak bir uzlaşıya varılamamıştır. Bu bölümde, yaygın kullanılan bazı tanımlara ve suç tiplerinin sınıflandırılmasına değinilmiştir.

Siber suç üzerinde çalışmalar yürüten ve siber suçların önlenmesi için 1998 yılından bu yana aktif olarak rol alarak, devletlere siber suçla mücadele politikalarında rehberlik eden ve 2020 yılında suç amaçlı bilgi ve iletişim teknolojilerinin kullanımına karşı kapsamlı bir uluslararası sözleşme hazırlamak üzere özel bir komite görevlendiren Birleşmiş Milletler, siber terimini "internete bağlı bilgisayarların, iletişim altyapılarının, çevrim içi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem" şeklinde tanımlamakta, buradaki tüm hukuka aykırı eylemleri şemsiye bir terim olan siber suç olarak nitelendirmektedir[11]. Bu bağlamda, bilişim sistemlerine yönelik suçlar dar anlamda siber suçlar olarak tanımlanırken, bilişim sistemleri aracılığıyla işlenmesi kolaylaşan her türlü hukuka aykırı eylem geniş anlamda siber suç kapsamında değerlendirilmektedir[12].

Avrupa kıtası ve ötesinde demokrasiyi, insan haklarını ve hukukun üstünlüğünü teşvik etmek maksadıyla, 1949 yılında 46 üye devletle kurulan Avrupa Konseyi ise 23 Kasım 2001'de Budapeşte'de imzaya açtığı ve 2024 yılı itibariyle konsey üyesi ülkelerin yanı sıra, konsey üyesi olmayan toplam 76 ülkenin imzalayıp kabul ettiği, siber suç konusunda bağlayıcı nitelikteki ilk sözleşme olan Avrupa Konseyi Siber Suçlar Sözleşmesi'nde (ETS No. 185) ise teknoloji nötr bir yaklaşım benimseyerek sözleşme içinde siber suçun tanımını yapmaktan kaçınmış olup, siber suçları yalnızca sınıflandırma yoluna gitmiştir[13]. Sözleşmeye göre siber suçlar, "bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar", "bilgisayarla bağlantılı suçlar", "içerikle ilgili suçlar" ve "telif hakkıyla ilgili suçlar" olarak dört ana gruba ayrılmıştır. Ancak, bu kategorilerden "bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar", "bilgisayarla bağlantılı suçlar" ile "içerikle ilgili suçlar" korunan hukuki değer üzerinden bir sınıflandırmayken, "bilgisayar bağlantılı suçlar" suçun işlenmesinde kullanılan yönteme odaklanan bir ayrım olmakta; araştırma çevreleri tarafından kategoriler arası örtüşme olabileceği gerekçesiyle sınıflandırma tutarsız olarak değerlendirilmektedir[14]. Bu sebeple, öğretide siber suç sınıflandırmasında Avrupa Konseyi'nin dörtlü ayrımı yaygın olarak kabul görmemektedir. Sözleşmede tanıma yer verilmemesiyse yalnızca kavramsal tartışmalara değil; uluslararası iş birliği, delil toplama ve iade süreçlerinde yaşanan uyumsuzluklara da kaynaklık etmektedir.

Uluslararası kuruluşların üzerinde hemfikir olduğu bir siber suç tanımı bulunmaması sebebiyle, alanyazında da siber suçun tanımına yönelik farklı yaklaşımlar bulunmaktadır. Akdemir, Sungur ve Başaranel alanyazında sık kullanılan siber suç tanımlarını belirlemek üzere yaptıkları bir araştırmada, en sık atıf yapılan tanımların Thomas ve Loader tarafından "yasa dışı olan veya belirli taraflarca yasa dışı kabul edilen ve küresel elektronik ağlar aracılığıyla yürütülebilen bilgisayar aracılı faaliyetler" olarak yapılan tanım ile

[9] Turhan (n 7) 31.

[10] Kyung-Shick Choi, Claire S Lee ve Eric R Louderback, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020) 22.

[11] Burak Yağcı, 'Bilgi ve İletişim Teknolojilerinin Gelişmesiyle Değişen Siber Suç Tanımı ve Yaklaşımlar' (2023) 1 Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi) 150.

[12] Zakir Avşar ve Gürsel Öngören, Bilişim Hukuku (Türkiye Bankalar Birliği 2010) 48.

[13] Aldoori (n 7) 69; Council of Europe, 'The Council of Europe at a Glance' <https://www.coe.int/en/web/portal/the-council-of-europe-at-a-glance> 17 Ekim 2024 tarihinde erişildi; Murat Önok, 'Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği' (2013) 19 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 1229, 1241.

[14] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2012) 12; Yağcı (n 11) 159.

Gordon ve Ford tarafından "bir bilgisayar kullanılarak aracı kılınan veya işlenen suç" olarak yapılan tanımlamalar olduğunu ortaya koymuşlardır[15]. Bahsedilen bu iki tanım, yaygın kullanımlarına rağmen, hırsızlık suçunu işlemek için telefonun konum servislerinden faydalanılarak suçun gerçekleştirileceği adrese gitmek gibi her teknolojik araç kullanımını siber suç haline getirme riski doğurarak kavramsal belirsizlik yaratacağı gerekçeleriyle eleştirilmektedir.

Alanyazında siber suçtaki tanımsal belirsizlikleri giderebilmek üzere yapılan sınıflandırmalar ise, uygulama açısından büyük önem taşımaktadır. Bu kapsamda en yaygın yaklaşım, siber suçları "siber bağımlı suçlar" ve "siber destekli suçlar" olmak üzere ikili bir ayrıma tabi tutulmaktadır[16]. Siber bağımlı suçlar, yalnızca bilgisayar sistemleri veya iletişim teknolojileri kullanılarak, bir ağa bağlı bilgisayarların suç kapsamında hedeflendiği, ağ gizliliğine, bütünlüğüne ve/veya kullanılabilirliğine yönelik saldırıların söz konusu olduğu suçları ifade ederken; siber destekli suçlar, bilgisayarlar, hırsızlık, dolandırıcılık gibi geleneksel suçların bilişim sistemleri aracılığıyla işlenmesini ve işlenmesinin kolaylaştırılmasını kapsamaktadır[17]. Bir başka siber suç sınıflandırması ise, siber suçları "siber bağımlı suçlar", "siber etkin kılınan suçlar" ve "bilgisayar destekli suçlar" olmak üzere üç grupta ele almaktadır. Bu sınıflamaya göre, siber bağımlı suçlar yalnızca bilgisayar veya diğer iletişim teknolojileri kullanılarak işlenebilen suçları ifade ederken; siber etkin kılınan suçlar, geleneksel suçların bilgisayar teknolojileri aracılığıyla daha geniş kapsamda işlenmesini ifade etmekte; nihayet bilgisayar destekli suçlar ise, örneğin; bir cinayet zanlısının bilgisayarında bulunan konum kayıtları gibi, bilgisayarın suçun işlenmesinde doğrudan rol oynamadığı ancak suçun deliline katkı sağladığı durumları kapsamaktadır[18]. Bu sınıflandırma, ABD Adalet Bakanlığı tarafından da benimsenmiş olmasına rağmen, bilgisayar teknolojilerinin suçun tesadüfi unsuru olmasının veya soruşturma için faydalanılmasının, neredeyse her suç için mümkün olması ve adli bilişimi de siber suç kapsamına alarak tanımı çok genişlettiği gerekçesiyle eleştirilmektedir[19]. Bir diğer yaygın sınıflandırmaya göreyse, siber suçlar "bilgisayar entegrasyonu suçları", "bilgisayar destekli suçlar" ve "bilgisayar içerik suçları" biçiminde üç kategoriye ayrılmıştır[20]. Bu üçlü yaklaşım da literatürde geniş kapsamda kabul görmesine rağmen; hakaret, çocuk pornografisi gibi suçları kapsayan bilgisayar içerik suçlarının ancak bilişim sistemlerini aracı kılarak işlenmesi mümkün olduğu için bilgisayar destekli suçlar kategorisinin kapsamıyla örtüştüğü gerekçesiyle eleştirilmektedir[21].

Türkiye'de ise Türk Ceza Kanunu'nda siber suç kavramı doğrudan tanımlanmamıştır; ancak, alanyazında ve farklı resmi kurumlar tarafından yapılan siber suç veya bilişim suçu tanımları mevcuttur. Yaygın kullanılan ve Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'nın siber suçlar konusunda bilgilendirmek ve önlemek üzere oluşturduğu "SiberAy" tarafından yapılan bir tanım, "bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzay kaynaklı olarak çeşitli tehdit odaklarından gelen ve kanunlara göre suç kabul edilen eylemler" şeklindedir[22]. Siber suça dair resmi en güncel tanımlardan bir diğeri ise, 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda "Tanımlar" kısmında

[15] Naci Akdemir, Bülent Sungur ve Bürke Başaranel, 'Birleşik Krallıkta Siber Ekonomik Suçlara Yönelik Kolluk Faaliyetleri Sorunlarının İncelenmesi' (2020) Güvenlik Bilimleri Dergisi 111, 117; Kirsty Phillips ve diğerleri, 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' (2022) 2 Forensic Sciences 379, 382; Sarah Gordon ve Richard Ford, 'On the Definition and Classification of Cybercrime' (2006) 2 Journal in Computer Virology 13, 14; Yağcı (n 11) 152.

[16] Jonathan Clough, *Principles of Cybercrime* (Second Edition, Cambridge University Press 2015) 10; Mike McGuire and Samantha Dowling, 'Cyber Crime: A Review of the Evidence Research Report 75' (2013) 5 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf> 13 Ekim 2024 tarihinde erişildi.

[17] Mohamed Chawki ve diğerleri, *Cybercrime, Digital Forensics and Jurisdiction* (Springer International Publishing 2015) 5; Clough (n 16) 10; Emilio C Viano, *Cybercrime, Organized Crime, and Societal Responses* (Springer International Publishing 2017) 4.

[18] Clough (n 16) 11.

[19] Chawki vd. (n 17) 5.

[20] Viano (n 17) 5.

[21] Gercke (n 14) 12.

[22] SİBERAY, 'Siberay Sözlük' (Siber Suçlarla Mücadele Daire Başkanlığı) 26 Ekim 2024 terihinde erişildi; Yağcı (n 11) 154.

"bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar" olarak yer alan tanımdır[23]. Yargıtay Ceza Genel Kurulu ise doğrudan siber suç veya bilişim suçu terimlerini tanımlamaktan kaçınmış olup, yalnızca bilişim sözcüğünü "bilginin otomasyona tabi tutulması sonucunda işlenmesini, başka deyişle, verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması" olarak tanımlamıştır[24]. Siber suçun tanımını doğrudan yapmayan Yargıtay Ceza Genel Kurulu, 9 Haziran 2007 tarihli ve E.2007/6-36, K.2007/150 sayılı kararında ise; 5237 sayılı TCK sistematiği ile BM tasnifine paralel bir yaklaşım benimseyerek, siber suçları yalnızca bilişim ortamında işlenebilen suçları kapsayan dar anlamda siber suçlar ve bilişim sistemlerinden yararlanılarak işlenebilen her türlü suçu içeren geniş anlamda siber suçlar olarak iki gruba ayırmıştır[25].

Türk ceza hukuku doktrininde bilişim suçuna ilişkin en yalın ve sık başvurulan tanımlardan biri Dülger tarafından yapılmış olup, yazar bu suçları "verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar" olarak ifade etmektedir[26]. Yazar, kelimenin Türkçe olması bakımından bilişim suçu terimini tercih etmekte ve suçun tasnifine özgün bir yaklaşım getirerek bu suçları üç kategoriye ayırmaktadır. Birinci kategori, bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme fiillerini kapsayan "bilişim sistemlerine veya içeriğine (güvenliğine, verilerine, yazılmalarına ve bütünlüğüne) karşı işlenen suçlar"; ikinci kategori, bilişim sistemlerinin araç olarak kullanılmasıyla nitelik kazanan hırsızlık veya dolandırıcılık gibi "işlenmesinde bilişim sistemleri kullanımının nitelikli unsur oluşturduğu suçlar"; üçüncü kategori ise, haberleşmenin engellenmesi, hakaret veya haberleşmenin gizliliğini ihlal etme gibi "işlenmesinde bilişim sistemlerinin yalnızca araç olarak kullanıldığı suçlar" olarak yazar tarafından ifade edilmektedir[27]. Sandilaç ise, Türkiye'de bu tür suçları ifade etmek üzere "bilgisayar suçu", "internet suçu", "bilişim suçu" veya "siber suç" gibi pek çok terimin kullanılmasının kavramsal belirsizlik yarattığını vurgulamakta; bilişim suçu terimini kapsam olarak daha geniş bulmasına rağmen Avrupa Birliği müktesebatına uyum süreci ve Avrupa Konseyi terminolojisinde siber suç kavramının benimsenmesi nedeniyle Türkiye'de de bu terimin tercih edildiğine dikkat çekmektedir[28].

Kanaatimizce, Türk Ceza Kanunu'nda bilişim alanında suçlar başlığı altında bilişim sistemlerinin bütünlüğüne yönelen suçların düzenlenmesi ve TCK'nın muhtelif bölümlerinde bilişim sistemleri aracılığıyla işlenen suçların suçun nitelikli hali olarak düzenlenmesi ayrımı göz önüne alınarak, BM sınıflandırmasının Türk hukuk araştırmalarında uygulanması yerinde olacaktır. Bu çalışmada da Sandilaç'ın ifade ettiği üzere siber suçun küresel nitelikte daha yaygın kullanımından hareketle bilişim alanında gerçekleştirilen suçları ifade etmek üzere siber suç terimi tercih edilmiş olup; siber suç teriminin Yargıtay'ın da benimsediği Birleşmiş Millet ayrımından hareketle hem yalnızca bilişim ortamında işlenebilen suçları ifade eden dar anlamda siber suçları hem de bilişim sistemlerinden yararlanılarak işlenebilen her türlü suçu içeren geniş anlamda siber suçları bir bütün olarak kapsamak üzere kullanılmıştır. Bu çalışmada siber suçun tanımına ve sınıflandırmasına yer verilmesinin, çalışmanın ilerleyen bölümlerinde ele alınacak zorlukların anlaşılmasını kolaylaştıracağı ve bu zorlukların temel nedenlerini açıklamak açısından kritik bir öneme sahip olduğu görüşündeyiz.

[23] Ulaştırma ve Altyapı Bakanlığı, 'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020–2023' (2020) 17 Ekim 2024 tarihinde erişildi; Yağcı (n 11) 154.

[24] Mesih Gözüşirin, '5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları Ile Mücadeleye İlişkin Model Önerisi' (Yüksek Lisans, TC Kara Harp Okulu 2011) 4; Yazıcı (n 1) 7.

[25] Burak Cesur Aköz, 'Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları Ile Örnek Yargısal Kararların Analizi ve Mevzuat Örnekleri' (Bilgi Teknolojileri ve İletişim Kurumu 2018) 24; Avşar ve Öngören (n 12) 124–131; Ufuk Taşcı ve Ali Can, 'Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014' (2015) 25 Fırat Üniversitesi Sosyal Bilimler Dergisi 229, 231.

[26] Murat Volkan Dülger, 'Türk Ceza Hukukunda Bilişim Suçları' (Yüksek Lisans Tezi, İstanbul Üniversitesi 2004) 27; Gözüşirin (n 24) 4.

[27] Aldoori (n 7) 20; Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku (10. Bası, Seçkin 2023) 82.

[28] Nurullah Sandilaç, 'Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya' (2022) 4 Bilişim Hukuku Dergisi 81, 164–165.

II. Siber Suçla Mücadele Karşılaşılan Zorluklar

Siber suçla mücadele, geleneksel suçlarla mücadele yöntemlerinden farklı ve çok katmanlı bir yaklaşım gerektirmektedir. Dijital teknolojilerin hızlı gelişimi, suç tiplerinin çeşitlenmesine ve sınır ötesi niteliğinin artmasına yol açarken, mevcut hukuk sistemleri ve uygulayıcı kurumlar bu değişime ayak uydurmakta zorlanmaktadır. Bu bağlamda, "Türkiye'de siber suç soruşturma süreçlerinde karşılaşılan başlıca yapısal sorunlar nelerdir?" sorusuna yanıt vermek üzere hazırlanan çalışmada nitel araştırma yöntemlerinden belgelere dayalı gözlem tekniği uygulanmıştır. Veri kaynaklarını 2009 – 2025 yılları arasında Türkçe ve İngilizce yayımlanmış, nitel ve nicel saha araştırmalarından oluşan akademik makaleler, lisansüstü tezler, kitaplar, resmi raporlar vb. dokümanlar oluşturmaktadır. Dokümanlardan elde edilen bulgular içerik yönünden değerlendirilerek hukuki engeller ve mevzuat farklılıkları, teknik ve operasyonel zorluklar, ve toplumsal ve kurumsal engeller olmak üzere 3 ana temaya ayrılmıştır. Bu çalışma, mevcut literatürü bütüncül biçimde analiz ederek, gelecek çalışmalar için Türkiye'de siber suçla mücadeledeki zorluklara ilişkin karşılaştırmalı ve tematik bir çerçeve sunmayı amaçlamaktadır. Çalışma 2009 – 2025 yılları arasındaki akademik ve kurumsal yayınlarla sınırlıdır. Çalışmanın bir diğer sınırlılığını, yargı kararlarına veya ampirik saha verilerine erişimin kısıtlı olması sebebiyle ikincil kaynak değerlendirmeleri üzerine inşa edilmesi oluşturmaktadır.

Bu bölümde, farklı ülkelerden ceza adalet sistemi içinde görev yapan uzmanların siber suçlara ilişkin deneyimleri ve değerlendirmelerine dayanan saha araştırmalarından edinilen bulgular üzerinden söz konusu zorluklar hukuki engeller, teknik ve operasyonel zorluklar ile toplumsal ve kurumsal engeller olmak üzere üç ana başlık altında sistematik biçimde ele alınacaktır.

A. Hukuki Engeller ve Mevzuat Farklılıkları

Siber suçların tanımı ve düzenlenmesinde ülkeler arasında ciddi farklılıklar bulunmaktadır. Ortak bir tanımın bulunmayışı, yasal uyumsuzluklara ve soruşturmalarda güçlükler yaşanmasına neden olmaktadır. Bazı ülkelerde mevzuat eksikliği ya da dar kapsamlı düzenlemeler, faillerin sorumluluktan kaçmasına olanak tanımakta; bu durum, uluslararası iş birliğini zorlaştırmakta ve çifte cezalandırılabilirlik gibi ilkelerin uygulanmasını engellemektedir.

1. Tanımsal Belirsizliklerin Hukuki Süreçlere Etkisi

Siber suçlara ilişkin artan akademik çalışmalar ve uluslararası işbirliği çabalarına rağmen, üzerinde mutabık kalınan bir tanımın yapılamadığına siber suçun tanımı ve sınıflandırması bölümünde değinilmiştir. Tanım zorluklarının temelinde fiziksel dünyada net biçimde belirlenen coğrafi sınırların siber uzayda mevcut olmaması, hızlı, kolay, anonim ve coğrafi olarak birbirinden bağımsız pek çok fail tarafından işlenebilmesi gibi siber suça özel unsurların yer aldığı aktarılmaktadır[29]. Bunlara ek olarak, teknoloji sayesinde ileri düzey teknik bilgiye sahip kişilerin yanı sıra, çok daha geniş bir fail potansiyelinin olduğuna dikkat çekilmektedir[30]. Geleneksel suçlara kıyasla atipik bir yapıya sahip olan siber suçların, duyularla doğrudan algılanamaması, suçun konusunun maddi varlıklar yerine elektronlar, bitler ve baytlar gibi dijital unsurlar olmasının yanında bilişim teknolojilerinin kullanımı ve gelişmişliğinin ülkeden ülkeye değişmesi, suçun maddi unsurunun değerlendirilmesini ve ceza hukukunun klasik yapısı içerisinde tanımlanmasını zorlaştırmaktadır[31]. Siber suçların geleneksel suçların statik yapısı aksine dinamik bir yapıda olmasıysa, bilişim teknolojilerinin anlık değişimleriyle paralel olarak yeni suç işleme yöntemleri geliştirilmesine olanak tanımaktayken, hukuk

[29] Chawki vd. (n 17) 7.

[30] Chawki vd. (n 17) 10; Yağcı (n 11) 151.

[31] Payne (n 8) 11; Sandilaç (n 28) 164.

sistemleri bu değişime uyum sağlamakta güçlük çekmektedir[32].

Siber suçların küresel niteliği de tanım ve hukuki düzenleme sorunlarını derinleştirmektedir. Geleneksel suçlarda fail, mağdur ve olay yeri genellikle aynı fiziksel mekânda bulunurken, siber suçlar bu üç öğeyi birbirinden ayırmakta ve çoğu zaman suç üçgeninin unsurlarının başka şehir ya da ülkelerde bulunmasına imkân tanımaktadır[33]. Milisaniyeler içinde gerçekleşen bu eylemlerde, potansiyel mağdur kitlesi genişletmekteyken, suçun soruşturulması pek çok ülkenin adli işbirliğini zorunlu kılmaktadır[34]. Siber suçların bu denli hızlı gelişimi ve geniş etki alanı karşısında hukukun yavaş işleyen yapısının yetersiz kaldığı; yasal düzenlemelerin hazırlanması, yürürlüğe girmesi ve uygulanması süreçlerinin önemli ölçüde zorlaştırdığı da alanyazında belirtilmektedir[35].

Bu bağlamda, ceza adalet sistemi alanında yapılan pek çok saha çalışması da siber suçun üzerinde uzlaşı sağlanmış uluslararası bir tanım olmamasının, suça müdahale etmekten sorumlu uzmanların suçun anlamı konusunda görüş birliği sağlayamadığını göstermektedir. Nitekim Hadlington, Lumsden ve Black'in İngiltere'de yürüttüğü araştırmada, polis memurlarının siber suçun kapsamını farklı şekillerde yorumladıkları görülmüştür[36]. Benzer şekilde Paoli, sekiz farklı ülkeden polisle yaptığı çalışmada, aynı olguların farklı ülkelerde farklı terimlerle ifade edildiğini ve bu anlamsal farklılıkların uluslararası düzeyde işbirliğini zorlaştırdığını belirtmektedir[37]. Çelik'in ceza adalet sisteminden siber suç alanında uzman beş meslek grubuyla yürüttüğü çalışmadaysa, Türkiye'de siber suç ve bilişim suçu terimlerinin anlamına yönelik fikir birliği olmadığı gibi, bu terimlerin farklı olguları ifade etmek üzere kullanıldığı ortaya konmaktadır[38]. Lavorgna da organize siber suçlara ilişkin araştırmasında, ortak bir tanım bulunmamasının, küresel çapta bu suçlara dair güvenilir istatistiklerin tutulmasını engellediğini vurgulamaktadır[39].

Türkiye bağlamında, dar anlamda siber suçlar Türk Ceza Kanunu'nun 3. Kitabının 10. Bölümünde "Bilişim Alanında Suçlar" başlığı altında (TCK m. 243 – 246) düzenlenmiş bulunmaktadır. Bunun yanı sıra, bazı suçlar açısından suçun bilişim sistemleri aracı kılınarak işlenmesi suçun nitelikli hali olarak düzenlenmiş olup geniş anlamda siber suçları ifade etmektedir[40]. TCK'da bilişim suçunun doğrudan bir tanımının yer almadığına ve tanımsal belirsizliği gidermek üzere resmi kurumlar, Yargıtay ve ceza hukuku doktrininde farklı kapsamlarda bilişim suçu tanımı yapıldığına "Siber Suçun Tanımı ve Sınıflandırılması" bölümünde değinilmiştir. Bu belirsizliğin suçun maddi unsurlarını tespit etmede güçlüğe sebep olmasının yanı sıra, bazı yazarlar TCK

[32] Baki Yiğit Çakmakkaya ve Teoman Akpınar, 'Bilişim Suçları İle Mücadelede Karşılaşılan Sorunlar' (2018) 4 Balkan and Near Eastern Journal of Social Sciences 123; Gözüşirin (n 24) 30.

[33] Chawki vd. (n 17) 5; Taşcı ve Can (n 25) 231.

[34] John Bandler ve Antonia Merzon, *Cybercrime Investigations: A Comprehensive Resource for Everyone* (First Edition, CRC Press/ Taylor & Francis Group 2020) 17; Gözüşirin (n 24) 31; Hamid Jahankhani, Ameer Al-Nemrat ve Amin Hosseinian-Far, 'Cybercrime Classification and Characteristics', *Cyber Crime and Cyber Terrorism Investigator's Handbook* içinde (Elsevier 2014) 149–164 ; Abraham D Sofaer ve Seymour E Goodman, 'Cyber Crime and Security The Transnational Dimension', *Hoover Institution's National Security Forum Series* içinde (Hoover Institution Press 2001) 1; Taşcı ve Can (n 25) 231.

[35] Chawki vd. (n 17) 5; Sandilaç (n 28) 153–154; Taşcı ve Can (n 25) 231.

[36] Lee Hadlington ve diğerleri, 'A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime' (2021) 15 Policing: A Journal of Policy and Practice 34 .

[37] Stefano De Paoli ve diğerleri, 'A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists' (2021) 15 Policing: A Journal of Policy and Practice 1429 .

[38] Görkem Nazlı Çelik, 'Ulusal ve Uluslararası Ceza Hukukunda Siber Suç ve Türkiye'de Siber Suç Soruşturmasının İşleyişi' (Yayımlanmamış Doktora, Üsküdar Üniversitesi 2025) 111–133.

[39] Anita Lavorgna, 'Organized Crime and Cybercrime' Adam M Holt Thomas J. and Bossler (ed), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde(Springer International Publishing 2020) 130.

[40] TCK m.142/2-e (nitelikli hırsızlık) ve TCK m. 158/1-f (nitelikli dolandırıcılık) suçlarında "bilişim sistemlerinin kullanılması suretiyle" işlenmesi madde metninde daha ağır ceza verilmesini gerektiren nitelikli hal olan düzenlemelere örnek olarak verilebilir. Bu maddelerin yanı sıra, TCK m. 226 (müstehcenlik) veya TCK m. 227 (fuhuş)'de suçun konusu olarak "görüntü, yazı ve sesleri içeren ürünler"den bahsedilmesi bilişim sistemlerinin aracı kılınmasını gerektirdiği gibi, özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında yer alan (TCK m. 132 – 138) suçlar açısından da kişilerin fiziksel dünyada olduğu kadar sanal ortamda da mahremiyetlerinin ve özel hayatlarının gizliliğinin korunması bu bölümde yer alan suçların koruduğu hukuki yararlardan olması sebebiyle bu suçlar da geniş anlamda siber suç kavramı içinde yer almaktadır.

243. maddesinin gerekçesinde yer alan "verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkanı veren manyetik sistemler" şeklindeki bilişim sistemi tanımını, kavramı açıklamada yetersiz ve daraltıcı nitelikte olduğu ve gelişen teknolojinin ortaya çıkardığı yeni sistemleri kapsamına dahil edemediği gerekçesiyle de eleştirmektedir[41].

Ceza Muhakemesi Kanunu ise bilişim sistemlerine yönelik koruma tedbirlerini "bilgisayar kütükleri ve programlarında arama, kopyalama ve elkoyma" başlıklı 134. maddede düzenlemekte; buna ek olarak "telekomünikasyon yoluyla yapılan iletişimin denetlenmesi" başlıklı CMK 135. madde ise internet üzerinden yapılan iletişime yönelik bir koruma tedbiri olarak uygulanmaktadır. Alanyazında, özellikle CMK 134. maddenin kapsamı ve uygulanabilirliği tartışılmakta[42]; maddenin yalnızca bilgisayar kütüklerinde arama ve el koymaya yönelik olmasıyla bulut bilişim, akıllı telefon ve diğer modern bilişim sistemlerinden delil toplama süreçlerinde yetersiz kaldığı ifade edilmektedir[43]. Bu bağlamda bazı yazarlar, "bilgisayar" kavramının geniş kabul edilmesi gerektiğini ve veri işleme, saklama ve iletme özelliğine sahip tüm cihazların bu kapsamda değerlendirilmesi gerektiğini savunmaktadır[44]. Keskin'in değerlendirmesine göre, maddede yer alan "bilgisayar kütükleri" ifadesi "log" yani kayıtları ifade etmekte olup[45]; bu durum bilgisayar veri tabanları ve bilişim sistemlerini kapsadığı şeklinde yorumlanabilmektedir[46]. Ancak yazara göre, bu ifadenin cep telefonu, kamera, hafıza kartı, televizyon veya taşınabilir bellek gibi cihazlara da genişletilerek uygulanması, ceza hukukunda kanunilik ilkesi gereğince ve Anayasa'nın 13. maddesinde yer alan temel hak ve özgürlüklerin kanunla sınırlanması ilkesine aykırılık oluşturabilmektedir. Keskin'in görüşündeki doktrindeki diğer yazarlarsa arama, kopyalama ve elkoymanın yalnızca bilgisayar, bilgisayar kütükleri ve programlarıyla sınırlı olacak biçimde kanun maddesinde düzenlendiğini; aksinin maddenin genişletici yorumlanması olacağı için hukuka aykırılık teşkil görüşünü desteklemektedir[47]. Dijital delillerin niteliğine ilişkin çalışmalar ise, adli bilişimin yalnızca bilgisayar temelli delillerle sınırlandırılmasının CMK 134/1'in düzenlenmesi açısından eksik bir yaklaşım olduğu görüşündedir[48]. Maddenin uygulanmasına ilişkin olarak ise Melemez, CMK m. 134 kapsamında verilen arama kararlarında, şüphelinin bilgisayar, cep telefonu ve diğer dijital cihazlarında arama yapılabileceğine dair genel ifadeler kullanıldığına değinmektedir[49]. Türkiye'de yapılan saha araştırmalarında da ceza adalet sistemi uzmanları, Türk Ceza Kanunu (TCK) ve CMK'daki mevcut düzenlemelerin güncel siber suç tiplerini karşılamada yetersiz kaldığını, dijital delillerin hukuka uygun biçimde elde edilmesinde güçlük yaşandığını ve uluslararası adli yardım taleplerinin, çoğu zaman "çifte cezalandırılabilirlik" koşulunun sağlanmaması

[41] Nagihan Gün, 'Türk Ceza Hukukunda Bilişim Suçları' (Yüksek Lisans, Çankaya Üniversitesi 2020) 299.

[42] Alanyazında, CMK 134. maddede "bilgisayar kütükleri" ifadesi kullanılmasının sınırlayıcılığının yanı sıra; ilgili maddenin her suçta uygulanabileceği, doğrudan bilişim suçları yönünden başka türlü delil elde edilememesi halinde bu maddedeki koruma tedbirlerine başvurulmasının dijital delillerin kaybına sebep olabileceği, ilgili koruma tedbirine yönelik uygulama yönetmeliğinin bulunmaması sebebiyle uygulamanın kanuniliğinin belirsiz olması, maddede elkonulan yasadışı içeriklerin bir kopyasının şüpheliye verilmesinin suçun işlenmeye devam edebileceği veya mağdurun özel hayatının gizliliğini ihlal edebileceği endişeleri, madde kapsamında elkonulan verilerin saklanma ve imha koşullarının belirsizliği gibi konularda hukuki değerlendirmeler de söz konusudur. Ancak çalışmanın odağına sadık kalabilmek amacıyla, yalnızca siber suç soruşturmalarında uygulamada karşılaşılan yapısal zorluklarla doğrudan ilişkili bulgulara yer verilmiştir. Bu tercihte, alanyazındaki saha araştırmalarında da uygulamaya yansıyan sorunların öncelikli olarak vurgulanması belirleyici olmuştur.

[43] Khalil Afandak, 'Ceza Muhakemesinde Dijital Deliller' (Yayımlanmamış Doktora, Ankara Üniversitesi 2021) 131–132; Zeynel Abidin Ayhan, 'Ceza Muhakemesi Hukukunda Dijital Deliller' (Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi 2022) 178; Yusuf Başlar, 'Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri' (2013) Uyuşmazlık Mahkemesi Dergisi 82, 86.

[44] Burak Melemez, 'Mesajlaşma Uygulamaları Ile Bulut ve Sosyal Medya Ortamlarından Sayısal Delillerin Elde Edilmesi' (2023) 167 Türkiye Barolar Birliği Dergisi 83, 87.

[45] Salih Keskin, 'Bilisim Suclarında CMK 134. Maddesindeki Hükümlerin Uygulamasında Yaşanan Aksaklıklar' (2021) 11 Kirikkale University Journal of Social Sciences 649, 651–652.

[46] Ayhan (n 41) 176.

[47] Dülger (n 27) 640; Muharrem Özen ve Gürkan Özocak, 'Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)' (2015) 1 Ankara Barosu Dergisi 41, 62–68.

[48] Afandak (n 41) 131–132; Ayhan (n 41) 178; Başlar (n 41) 86.

[49] Melemez (n 42) 106.

gerekçesiyle reddedildiğini belirtmişlerdir[50].

2. Yargı Yetkisi Sorunları

Teknolojik gelişmelerin hızla ilerlemesiyle birlikte, bazı dijital eylemler hak ihlali niteliği taşımasına rağmen birçok ülkede mevcut yasalarda henüz açık biçimde suç olarak tanımlanmamıştır. Siber suçlara ilişkin ortak hukuki düzenlemelerin bulunmaması, özellikle sınır aşan suçların soruşturulmasında ülkeler arası iş birliğini sekteye uğratmaktadır[51]. Ancak, suçta ve cezada kanunilik ilkesi, herhangi bir eylemin soruşturulup cezalandırılabilmesi için, o eylemin işlendiği ülkenin ceza mevzuatında suç olarak yer almasını gerekli kılmaktadır. Bu bağlamda bazı ülkeler, siber suçlara ilişkin kapsamlı düzenlemeler yapmış olsalar da yapılan bir çalışmaya göre; 201 ülkenin yalnızca 79'unda siber suçlara dair özel mevzuat bulunduğu tespit edilmiştir[52]. Birçok ülkede siber uzaydaki hak ihlalleri henüz hukuka aykırı kabul edilmezken, siber suç düzenlemesi bulunan ülkelerde ise suç olarak tanımlanan eylemlerin kapsamının ciddi biçimde farklılık gösterdiği aktarılmaktadır[53]. Özellikle, Snapchat gibi kendiliğinden silinen mesajlaşma uygulamalarının kullanımı, Bitcoin gibi kripto paraların bankacılık sistemlerinin yerini alan para transfer sistemleri haline gelmesi veya sürücüsüz araçlar gibi yapay zeka tabanlı bilişim sistemlerinin yaygınlaşması, bu araçlarla işlenen fiillerin mevcut ceza normlarıyla ne ölçüde örtüştüğü konusunda ciddi belirsizlikler yaratmaktadır[54]. Bu belirsizlik, elde edilen dijital delillerin hukuka uygunluğunu tartışmalı hale getirmenin yanı sıra, ceza adaleti ile insan hakları arasındaki dengenin korunmasını zorlaştıran bir unsur olarak görülmektedir[55].

Siber suçlarda, geleneksel suçların aksine, failler suç eylemlerini otomatikleştirerek neredeyse tüm internet kullanıcılarını kapsayan bir potansiyel mağdur havuzuna erişim sağlayabilmelerine rağmen, ceza hukukunda geçerli olan ülkesellik prensibi, devletlerin yargılama yetkisini kendi coğrafi sınırları içerisinde bulunan kara, hava ve sularıyla sınırlandırmakta; çoğu durumda hem mağdur hem de fail aynı yargı bölgesinde ikamet ediyorsa yeterli yardım ve destek sağlayabilmektedirler[56]. Suçun unsurlarının birden fazla ülkede gerçekleştiği durumlarda, hangi ülkenin hukukunun uygulanacağı ve yargılama yetkisinin kimde olacağına ilişkin belirsizliklerin yanı sıra, delil elde etme, el koyma ve faillerin iadesi gibi adli işlemlerde ülkelerin farklı prosedürlere sahip olması da sürecin etkinliğini önemli ölçüde azaltmaktadır[57]. Ayrıca, delil elde etme, el koyma ve faillerin iadesi gibi adli işlemlerde ülkelerin farklı prosedürlere sahip olması, sürecin etkinliğini azaltan etkenler olarak görülmektedir.

Yasal düzenlemelerin yetersiz olduğu ülkelerse, siber suçlular için yaptırıma uğrama riski olmadan eylemlerini gerçekleştirebildikleri fiili birer "güvenli sığınak" hâline gelmektedir[58]. Bu duruma örnek teşkil

[50] Çelik (n 38) 117–118; Abdullah Taner Demiroğlu, 'Stratejik İstihbaratın Önemi: Bilişim Suçları Uygulaması' (Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi 2015) 96–97.

[51] Coleman Mckoy, 'Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level' (Doktora, Walden University 2021) 24 13 Ekim 2024 tarihinde erişildi.

[52] EFG Ajayi, 'Challenges to Enforcement of Cyber-Crimes Laws and Policy' (2016) 6 Journal of Internet and Information Systems 1. Araştırmada söz konusu 201 ülke BM üyesi ülkeler olup; bu ülkelerden 193'ü BM tam üyesi, 2 gözlemci ülke ve 6 kısmi tanınan ülkedir.

[53] Tatiana Tropina, 'Cyber-Policing: The Role of the Police in Fighting Cybercrime', European Police Science and Research Bulletin – Police Science and Police Practice in Europe, Special Conference Edition (2017) 289 <https://www.cepol.europa.eu/sites/default/files/Special%20Conference%20Edition%20Nr.%202.pdf> 13 Ekim 2024 tarihinde erişildi.

[54] Trong Van Nguyen, Tung Vu Truong ve Cuong Kien Lai, 'Legal Challenges to Combating Cybercrime: An Approach from Vietnam' (2022) 77 Crime, Law and Social Change 231, 231–252; David S Wall, 'Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing' R Brownsword, E Scotford and K Yeung (eds), *The Oxford Handbook on the Law and Regulation of Technology* içinde (Oxford University Press 2017) .

[55] Tropina (n 51) 289.

[56] Aldoori (n 7) 96; Thomas J Holt, Joshua D Freilich ve Steven M Chermak, 'Exploring the Subculture of Ideologically Motivated Cyber-Attackers' (2017) 33 Journal of Contemporary Criminal Justice 212, 7 ; Holt ve Bossler (n 6) 392; Jin R Lee, 'Cyberpolicing', Oxford Research Encyclopedia of Criminology and Criminal Justice içinde(Oxford University Press 2022) 7.

[57] Aldoori (n 7) 97; Pelin Topçuoğlu, 'Türk Ceza Kanunu Kapsamında Bilişim Sistemine Girme Suçu' (Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2022) 75; Van Nguyen, Truong ve Lai (n 52) 233.

[58] Aldoori (n 7) 93; Lee (n 54) 12; Van Nguyen, Truong and Lai (n 52) 233.

eden vakalardan biri, "love bug" virüsünü yayan Onel de Guzman'ın yargılanma ve Filipinler'den ABD'ye iadesi sürecidir. Filipinler'de virüs üretmek ve yaymak suç olarak tanımlanmadığı için Guzman, kredi kartı dolandırıcılığından yargılanmış ancak bu suça dair de delil yetersizliği sebebiyle serbest bırakılmak zorunda kalmıştır[59]. Ayrıca, yine aynı sebeple suçlunun iadesi için hem talep eden hem de talep edilen ülkede fiilin suç sayılmasını şart koşan çifte cezalandırılabilirlik ilkesi sağlanmadığı gerekçesiyle Filipinler'den ABD'ye iadesi de gerçekleştirilememiştir.

Türkiye'deki mevcut yasal düzenlemeler, suçun işlendiği yer ilkesine dayandığından, failin, mağdurun veya delillerin farklı ülkelerde bulunduğu durumlarda etkin bir muhakeme yürütmek adli yardımlaşmayı gerekli kılmaktadır.

B. Teknik ve Operasyonel Zorluklar

Siber suçlarla mücadelede dijital delillerin elde edilmesi ve korunması ciddi zorluklar içermektedir. Delillerin uçucu olması, şifreleme ve bulut teknolojileriyle gizlenebilmesi, faillerin anonim hareket etmesi bu zorluklar arasındadır. Türkiye'de ise adli bilişim eğitimi, teknik altyapı ve uzman personel eksiklikleri sorun yaratmaktadır. Ayrıca, uluslararası veri paylaşımı ve adli yardımlaşma süreçlerinin yavaşlığı, sınır aşan suçlara karşı etkin mücadeleyi engellemekte ve soruşturma makamlarını bu yollara başvurmaktan alıkoymaktadır.

1. Dijital Delilleri Elde Etme ve Korumadaki Zorluklar

Siber suçlarda ana olay yerinin bilişim sistemleri olmasıyla deliller genellikle bu ortamda aranmakla birlikte, dijital delillerin uçucu niteliği şifreleme ve belirli yazılımlar yoluyla bunların kolayca gizlenmesine veya yok edilmesine imkan tanımakta; büyük hacimlerdeki veriler küçük fiziksel alanlarda depolanabilmekte veya soruşturmanın yetki alanı dışında kalan coğrafi bölgelerdeki sunucularda barındırılan bulut hizmetlerine aktarılabilmektedir[60]. Faillerin proxy sunucuları, sahte e-posta adresleri, IP adreslerini gizleyici araçlar ile anonim e-posta hizmetleri gibi teknolojileri yaygın kullanarak kimliklerine ya da işledikleri suçlara dair herhangi bir iz bırakmamaları, siber suçların tespit ve takibini geleneksel suçlara kıyasla önemli derecede güçleştirmektedir[61]. Bu durum, şüpheliye ulaşabilmek için yapılan soruşturmalarda ciddi zorluklar yaratırken, suçluların anonim olarak hareket edebilmesi, faillerin işledikleri suçlarla ilgili sorumluluk hissetmeden eylemlerini gerçekleştirmelerine de olanak tanımaktadır[62].

Yeni siber suç işleme yöntemleri ortaya çıktıkça, dijital suç mahallerindeki delillere yönelik işlemler adli bilişim uzmanlığı gerektirdiği için kolluğun toplanan delilleri çıkarma, analiz etme ve işlemekten oluşan siber suçlara yanıt verme gibi görevleriyse daha da zorlaşmaktadır[63]. Leppanen ve Kankaanranta'nın Finlandiya'da polis memurlarıyla yaptığı çalışma, dijital delillerin doğasından kaynaklı zorlukların soruşturmaları güçleştirdiğini ortaya koymaktadır[64]. Bazı çalışmalar da adli bilişim alanında yeterli eğitimi olmayan genel kolluk personelinin siber suç soruşturmalarında görev almasının, dijital delillerin doğru şekilde toplanamaması ve

[59] Aldoori (n 7) 93.

[60] Clough (n 16) 7–8; Alisdair A Gillespie, *Cybercrime - Key Issues and Debates* (Routhledge 2016) 8.

[61] Clough (n 16) 7–8; Gözüşirin (n 24) 31.

[62] Taşcı ve Can (n 25) 231. "Normalde cinsel organın gerçek yaşamda gösterilmesi, çok ahlaki karşılanmazken ve toplumda büyük bir kesim bu davranışı yapmaya cesaret edemezken, sanal ortamda yapılan sohbetlerde kişiler cinsel organlarını yüzünü gizleyerek çok rahatlıkla yapabilmektedirler."

[63] Hakan Hekim ve Oğuzhan Başıbüyük, 'Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları' (2013) 4 Uluslararası Güvenlik ve Terörizm Dergisi 135, 153; Mckoy (n 49) 24; De Paoli and others (n 37) 1434; Taşcı ve Can (n 25) 242.

[64] Anna Leppänen ve Terhi Kankaanranta, 'Cybercrime Investigation in Finland' (2017) 18 Journal of Scandinavian Studies in Criminology and Crime Prevention 157, 157.

soruşturmaların gecikmesi üzerinde önemli bir etken olduğunu vurgulamaktadır[65].

Birçok ülkede dijital delillerin toplanmasına dair özel yasal düzenlemelerin bulunmaması nedeniyle, bilişim sistemlerinde geleneksel arama ve elkoyma tedbirleri uygulanmaya çalışılmaktadır[66]. Bu durum, hem temel haklara müdahale niteliği taşıyan bu koruma tedbirlerinin hukuki dayanağının yetersiz kalmasına hem de bilişim sistemlerine özgü usuller içermemesi nedeniyle delil eksikliklerine yol açabilmektedir. Ayrıca, uluslararası nitelikteki soruşturmalarda delillerin korunması ve hızlandırılmış paylaşımına dair bir yasal çerçeve veya teamül hukuku bulunmadığından, süreçler genellikle ikili antlaşmalarla yürütülmektedir[67]. Ancak, bu antlaşmaların varlığı durumunda dahi, delillerin toplanıp talep edilen ülkeye gönderilmesi, talep edilen devletin iç mevzuatında öngörülen usuller izlenerek gerçekleştirildiği için sürecin tamamlanması uzun zaman alabilmektedir[68].

2. Mücadelede Personel ve Teknik Altyapı Eksikliği

Siber suçlar hızla gelişen bir alan olup, kolluk kuvvetlerinin bu suçlarla etkili mücadele için sürekli ve nitelikli eğitim almasını zorunlu kılmaktadır[69]. Ancak mevcut araştırmalar, polis teşkilatlarında verilen siber suç eğitimlerinin çoğunlukla yetersiz kaldığını, geleneksel suç türlerine odaklandığını ve güncel teknolojik gelişmeleri yeterince kapsayamadığını ortaya koymaktadır[70]. Harkin ve Whelan'ın Avustralya'da polis memurları üzerinde yürüttükleri çalışma, polis teşkilatlarının kamu taleplerine yanıt verme çabalarına rağmen siber suçlarla mücadelede yetersiz kaldığını göstermektedir[71]. Benzer şekilde, Hadlington ve diğerlerinin İngiltere'de ön safha polis memurlarıyla yaptığı araştırma, memurların büyük çoğunluğunun siber suçlara ilişkin verilen eğitimleri yetersiz bulduğunu göstermektedir[72]. ABD'de yürüttükleri çalışmada Bossler ve Holt da benzer biçimde, siber suç olaylarına ilk müdahalede bulunan kolluk personelinin eğitim eksikliği sebebiyle siber vakaların doğrudan uzman birimlere yönlendirilmesi gerektiğini düşündüklerini ortaya koymaktaysa da uzman birimlerin sınırlı kaynakları nedeniyle bunun pratikte uygulanamayacağı ifade edilmektedir[73]. Ayrıca yapılan bazı çalışmalar, eğitim yetersizliklerinin kolluğun siber suçları değerlendirirken medya söylemleri, yaş, deneyim ve ahlaki tutum gibi bireysel faktörlerden etkilenmesine yol açabildiğini göstermektedir[74]. Bu bağlamda, pedofili ve çocuk pornografisi gibi suçlar "ideal mağdur" algısı nedeniyle öncelikli değerlendirilirken, diğer siber suç türleri ikinci planda kalabilmektedir[75].

---

[65] Lee (n 54) 13; Andrew Staniforth, 'Police Investigation Processes: Practical Tools and Techniques for Tackling Cyber Crimes', *Cyber Crime and Cyber Terrorism Investigator's Handbook* içinde (Elsevier Inc 2014).

[66] Ajoy PB, 'Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis' (2023) SSRN Electronic Journal 5.

[67] Europol ve Eurojust, 'Common Challenges in Combating Cybercrime As Identified by Eurojust and Europol' (2019) 15 <https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf> 13 Ekim 2024 tarihinde erişildi.

[68] Ajoy (n 64) 4; Europol ve Eurojust (n 65) 15; Sofaer ve Goodman (n 34) 16; Tropina (n 51) 288.

[69] Mckoy (n 49) 29.

[70] Abdelkhalek Ibrahim Alastal ve Ashraf Hassan Shaqfa, 'Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool' (2023) 11 Journal of Data Analysis and Information Processing 121, 132 ; José de Arimatéia da Cruz, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020) 386 ; Mckoy (n 49) 29; Scott R Senjo, 'An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data' (2004) 17 Security Journal 55, 17 .

[71] Diarmaid Harkin ve Chad Whelan, 'Perceptions of Police Training Needs in Cyber-Crime' (2022) 24 International Journal of Police Science and Management 66, 73–74.

[72] Hadlington vd. (n 36) 38.

[73] Alastal ve Shaqfa (n 68) 132; Adam M Bossler and Thomas J Holt, 'Patrol Officers' Perceived Role in Responding to Cybercrime' (2012) 35 Policing: An International Journal of Police Strategies & Management 165, 172; Mckoy (n 49) 73; De Paoli vd. (n 37) 1453–1454.

[74] Cassandra Cross ve Thomas Holt, *Responding to Cybercrime: Results of a Comparison between Community Members and Police Personnel* (Australian Institute of Criminology 2021) 4 <https://www.aic.gov.au/publications/tandi/tandi635>; Hadlington vd. (n 36) 37; Senjo (n 68) 67.

[75] Bossler ve Holt (n 71) 169; Cross ve Holt (n 72) 4; Jeffrey Nowacki ve Dale Willits, 'An Organizational Approach to Understanding Police Response to Cybercrime' (2019) 43 Policing: An International Journal 63, 66 .

Öte yandan, siber suçların düşük maliyetle işlenebilmesine karşın, bu suçların soruşturulmasında gereken teknoloji ve uzmanlığın yüksek maliyetlerine kaynak yetersizliklerinin de eklenmesinin müdahaleleri zorlaştırdığı pek çok araştırmada vurgulanmaktadır[76]. Çok uluslu soruşturmalarda adli yardımlaşma için yapılan çeviriler ve suçluların iadesine ilişkin lojistik giderler gibi ek masraflar, sürecin maliyetini arttıran unsurlar olarak görülmektedir[77]. Bu nedenle, özellikle maddi zarar açısından düşük etkili suçların yeterli öncelik alamadığı veya soruşturma dışı bırakıldığı bazı araştırmalarda aktarılmaktadır[78].

Türkiye'de yapılan araştırmalar da benzer şekilde, Emniyet Teşkilatı'nda siber suçlarla mücadele birimleri ve adli bilişim alanında uzmanlaşmış personelin sayıca yetersiz olduğunu ve verilen eğitimlerin sınırlı olduğunu vurgulamaktadır[79]. Özellikle savcıların, adli bilişimle ilgili temel bilgilere yeterince sahip olmamaları nedeniyle açık kaynak incelemeleri gibi konuları dahi kolluk birimlerine havale ettikleri ve teknik bilgilerindeki eksiklikler nedeniyle bazı dosyaların matbu biçimde kovuşturmaya yer olmadığına dair kararlar ile sonuçlandırıldığı öne sürülmektedir[80]. Eğitimlerin sürdürülebilirliğinin sağlanamaması ve farklı personelin farklı dönemlerde eğitime gönderilmesinin, bilgi birikiminin kurumsallaşmasına engel olurken; eğitimli personelin farklı illerde veya birimlerde görevlendirmelerinin yapılmasının uzmanlaşmayı güçleştirdiği ve güncel siber suç işleme yöntemlerine yönelik stratejik planlama yapılmasını zorlaştırdığı ifade edilmektedir[81]. Ek olarak, bazı çalışmalarda, bulut depolama sistemleri, kripto para borsaları, sosyal medya platformları gibi günümüzde aktif kullanılan teknolojilerden sayısal delil elde etmeye ilişkin teknik altyapıya dair yetersizlikler olduğu vurgulanmaktadır[82].

3. Uluslararası Veri Paylaşımı ve Adli Yardımlaşma Engelleri

Siber suçların sınır aşan niteliği, ülkeler arasında etkin ve hızlı işleyen adli yardımlaşma mekanizmalarının varlığını zorunlu kılmaktadır. Ancak, farklı hukuk sistemleri ile prosedürel uygulamalar arasındaki uyumsuzluklar bu süreçlerin yavaş ve verimsiz ilerlemesine sebep olabilmektedir. Avrupa Konseyi Siber Suç Sözleşmesi her ne kadar adli yardımlaşma ve delil paylaşımına ilişkin hükümler içerse de, uluslararası düzeyde bağlayıcı ve etkili bir mekanizma olmaması nedeniyle delil talepleri çoğunlukla ikili antlaşmalar üzerinden yürütülmektedir[83]. Melemez'e göre, kullanıcı verilerinin büyük kısmını elinde bulunduran ABD merkezli şirketlere yöneltilen adli yardım taleplerinin artması, ABD'deki adli yardımlaşma süreçlerini yavaşlatarak dijital delil elde etme sürecinin etkinliğini azaltmaktadır[84]. Adli yardımlaşma süreçlerinin bürokratik engeller, evrak çevirileri ve çok katmanlı onay prosedürleri nedeniyle uzayarak siber suçların hızlı müdahale gerektiren doğasıyla çeliştiği; ayrıca taraf devletlerin bu süreçlere ilişkin yeterli veri ve istatistiklere sahip olmamalarının bu sürecin etkinliğinin izlenmesi ve geliştirmesini daha da güçleştirdiği vurgulanmaktadır[85].

Türkiye'de ise, uluslararası prosedürlere başvurma ihtiyacını azaltmak ve iç hukukun soruşturmalardaki etkinliğini artırmak amacıyla 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar

[76] Ajayi (n 50) 8; Ajoy (n 64) 5; Maggie Brunner, 'Challenges and Opportunities in State and Local Cybercrime Enforcement' (2019) 10 J. National Security & Policy 563, 564; Europol ve Eurojust (n 65) 16.

[77] Demiroğlu (n 48) 97; Ajayi (n 50) 8; Brunner (n 74) 564.

[78] Mckoy (n 49) 23; Brunner (n 74) 565; Wall (n 52) 11.

[79] Aldoori (n 7) 92; Çakmakkaya ve Akpınar (n 32) 126; Ali Durdu, 'Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı (Gaziantep İli Örneği)' (Yüksek Lisans Tezi, Gaziantep Üniversitesi 2015) 91.

[80] Çakmakkaya ve Akpınar (n 32) 126.

[81] Çelik (n 38) 36; Demiroğlu (n 48) 97; Önok (n 13) 1233.

[82] Onur Ceran, 'Adli Bilişim Araştırmalarına Küresel Bir Bakış: Bibliyometrik Analiz Ile Yayın Trendleri ve Araştırma Yönelimleri' (2025) 13 Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji 859, 862; Melemez (n 42) 117.

[83] Ajayi (n 50) 10.

[84] Melemez (n 42) 113.

[85] Aldoori (n 7); Melemez (n 42) 114.

Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun'a ek madde 4 ile günlük kullanıcı sayısı 1 milyonu aşan sosyal ağ sağlayıcılara Türkiye'de temsilcilik bulundurma yükümlülüğü getirilmiştir. Bu düzenlemeyle, Türkiye'de dijital içeriklerin kaldırılması ve delil taleplerinin daha hızlı işlemesi hedeflemektedir. Ancak uygulamaya ilişkin olarak, temsilcilik bulundurmayan sağlayıcılar nedeniyle mahkeme kararlarının uygulanamadığı; temsilciliği olan bazı şirketlerin ise merkez ülkelerinin hukuk sistemine atıfta bulunarak "çifte cezalandırılabilirlik" ilkesini gerekçe gösterip talepleri reddettiği belirtilmektedir[86]. Türkiye'de ceza adalet sistemi uzmanlarıyla görüşmelerden oluşan bir araştırma da ülkelerin ve platformların delil taleplerine yaklaşımlarında suçun niteliğine göre farklılıklar bulunduğu inancını ortaya koymakta; çocuk istismarı, fuhuş ve insan kaçakçılığı gibi ağır suçlarda sosyal ağ sağlayıcıları ve yabancı makamların daha işbirliğine yatkınken, hakaret ve dolandırıcılık gibi suçlarda çifte cezalandırılabilirlik gerekçesiyle talepleri sıklıkla reddettiklerini ifade etmektedirler[87]. Ayrıca Türkiye, Avrupa Konseyi Siber Suçlar Sözleşmesi'ni (AKSSS) imzalayarak iç hukukuna aktarmış olmakla birlikte; 2022 yılında imzaya açılmış olan, geliştirilmiş iş birliği ve elektronik delillerin açıklanmasına yönelik hükümleri düzenleyen sözleşmenin "2 No'lu Ek Protokol"ünü (CETS No. 224) ise henüz imzalamamıştır. Bu protokole henüz taraf olunmaması, özellikle dijital delil taleplerinin hızla paylaşılması, gerçek zamanlı veri erişimi gibi kritik süreçlerde hızlı iş birliği yapılamayarak geleneksel delil iş birliği usullerine başvurulmasını mecbur kılmakta ve soruşturmaların zamanında ve etkili biçimde yürütülmesini engellemektedir.

C. Toplumsal ve Kurumsal Engeller

Siber suçların düşük görünürlüğü ve bildirilmesinin yetersiz olması, bu alandaki mücadeleyi ciddi şekilde zorlaştırmaktadır[88]. Fail ve mağdurun fiziksel olarak karşı karşıya gelmemesi, anonim kimliklerle hareket edilebilmesi ve dijital ortamın sağladığı görünmezlik, suçların tespitini güçleştirmekte; kolluk kuvvetlerini yalnızca dijital izler üzerinden delil toplamaya zorlamaktadır[89]. Araştırmalar, siber suç mağdurlarının önemli bir kısmının yaşadıkları olayın suç niteliği taşıdığını fark edemediklerini veya hangi makama başvurmaları gerektiğini bilmediklerini göstermektedir[90]. Mağdurların güvenlik birimlerine duydukları güvensizlik, zaman kaybı endişeleri, maddi kayıplarını küçük görmeleri ve adli makamların olaya kayıtsız kalacağı yönündeki inançlarının da suç bildiriminde bulunmalarını zorlaştırdığı belirtilmektedir[91]. Özellikle çevrimiçi dolandırıcılık vakalarında, mağdurların bu inançları sebebiyle resmi şikayette bulunmaktan kaçındıkları aktarılmaktadır[92].

Ticari işletmelerin ise, marka değeri ve itibar kaybı riski ile özel verilere yönelik güven eksikliği nedeniyle şikâyette bulunmaktan kaçındıkları; bu durumun ise, mağdur katılımının ve sektörel iş birliğinin gerekli olduğu siber suçlarla mücadeleyi daha da zorlaştırdığı bazı yazarlar tarafından vurgulanmaktadır[93].

[86] Çakmakkaya ve Akpınar (n 32) 125.

[87] Çelik (n 38) 116–119.

[88] Guillaume Lovet, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges', Virus Bulletin Conference (2009) 69 <https://www.virusbulletin.com/conference/vb2009/abstracts/fighting-cybercrime-technical-juridical-and-ethical-challenges/> 26 Ekim 2024 tarihinde erişildi.

[89] Joanna Curtis ve Gavin Oxburgh, 'Understanding Cybercrime in "Real World" Policing and Law Enforcement' (2023) 96 The Police Journal: Theory, Practice and Principles 573, 583 .

[90] Alastal ve Shaqfa (n 68) 132–133; Kezban Alatıç Taş, 'Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi' (Yüksek Lisans Tezi, Çukurova Üniversitesi 2010) 66; Curtis ve Oxburgh (n 87) 578; Mckoy (n 49) 25; Dale Willits ve Jeffrey Nowacki, 'The Use of Specialized Cybercrime Policing Units: An Organizational Analysis' (2016) 29 Criminal Justice Studies 105, 108 .

[91] Alatıç Taş (n 88) 66; Cameron SD Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' (2015) 9 International Journal of Cyber Criminology 55; Colin Manning, 'Old Laws, New Crimes: Challenges of Prosecuting Cybercrime in Ireland' [2016] SSRN Electronic Journal 15.

[92] Harkin ve Whelan (n 69) 66–76; Lee (n 54) 7; Sandilaç (n 28) 185.

[93] Alatıç Taş (n 88) 67; Manning (n 89) 15; Tropina (n 51) 287–294; Lee (n 54) 14.

Delil temininde kurumların katılımına ilişkin olarak ise, yapılan bir saha araştırmasında bankaların belge taleplerine tutarsız yanıtlar vermesinin siber suç soruşturmalarında delile ulaşma sürecini uzattığı ifade edilmiş olup; Gümüş, bu sorunun temel nedeninin muhakeme organlarıyla kurum ve kuruluşlar arasında ortak bir delil paylaşım altyapısı bulunmaması olduğunu belirtmektedir[94].

III. Tartışma

Bu çalışma, siber suçla mücadelede uygulamada karşılaşılan zorlukları konu edinen nitel ve nicel ampirik çalışmalar üzerinden Türkiye özelinde siber suçlarla mücadelenin mevcut durumunu ortaya koymak amacıyla gerçekleştirilmiştir. Siber suçların tanımına yönelik farklı görüşlere yer verilmiş olup, uzlaşı sağlanan bir tanım bulunmamasının siber suçla mücadelenin temelinde yatan en önemli etken olduğu değerlendirilmiştir. Çalışmanın alanyazın incelemesinden elde edilen veriler, siber suçla mücadelenin yalnızca teknik bir güvenlik meselesi olmadığını, aynı zamanda hukuki, kurumsal ve toplumsal boyutları iç içe geçmiş çok katmanlı bir politika alanı olduğunu göstermektedir. Bu bağlamda, siber suçla mücadelede karşılaşılan zorluklar hukuki, teknik ve toplumsal olmak üzere üç temaya ayrılmıştır.

Siber suçla mücadelede karşılaşılan zorluklara yönelik alanyazındaki çalışmalardan edinilen bulgular, tanımsal belirsizliklerin ve yargı yetkisinden kaynaklı sorunların küresel çapta siber suçla mücadeledeki en temel engeller olduğunu ortaya koymaktadır. Yapılan çalışmalar suçun kapsamına dair farklı yorumların bulunması ve uluslararası düzeyde kabul gören yaygın bir tanımın bulunmayışının, suçun tespit edilmesi ve kovuşturulması süreçlerinde aksaklıklara sebep olduğunu göstermektedir. Mevzuat eksikliklerinden faydalanan siber suç failleri yargısal dokunulmazlığa sahip olabilecekleri, siber suç mevzuatının yetersiz olduğu güvenli sığınak ülkelere sığınabilmektedir. Bu durum, Türkiye açısından ceza hukukunun temel ilkelerinden olan çifte cezalandırılabilirlik ilkesinin uygulanmasının önüne geçerek soruşturmaların yarım kalmasına veya kovuşturmanın işlevsiz hale gelmesine sebep olmaktadır.

Türkiye özelinde, Türk Ceza Kanunu'nun bilişim alanında suçlar başlığı altında 243. – 246. maddeleri arasında düzenlenen suçlar ve bu suçların soruşturulmasında başvurulan temel koruma tedbiri olan Ceza Muhakemesi Kanunu 134. maddesinin güncel teknolojilere uyum sağlamaktan uzak olduğu alanyazında belirtilmektedir. CMK m. 134'ün "bilgisayar kütüklerinde arama ve elkoyma" olarak düzenlenmesi alanyazındaki pek çok çalışma tarafından mobil cihazlar, bulut bilişim gibi güncel teknolojik unsurlardan elde edilecek delillerin hukuki niteliğini belirsiz hale getirdiği gerekçesiyle eleştirilmekte, bazı çalışmalardaysa güncel teknolojilerden delil elde edilmesini sağlayacak biçimde ilgili maddenin yorumlanması önerilmektedir. Alanyazında CMK 134. maddeye ilişkin görüşlerde uzlaşı olmaması, maddenin uygulama açısından yetersiz kaldığının açık bir göstergesi olmaktadır. Düzenlemenin şu anki haliyle uygulanması güncel teknolojilerden delil edilemeyerek soruşturmaların sonuçsuz kalmasına veya genişletici yorum yapılarak güncel teknolojilerden delil elde edilerek temel hak ve hürriyetlerin ihlal edilmesine sebep olabilmektedir.

Alanyazındaki pek çok çalışma, teknik altyapının güncel teknolojilerden delil elde etmeye uygun olmaması ve uzman kolluk sayısının yetersizliğinin de siber suçla mücadeleyi zorlaştıran etkenlerden olduğunu göstermektedir. Siber suçların anonim karakteri, sınır ötesi nitelikleri ve dijital delillerin uçucu doğası gibi geleneksel suçlardan ayrılan özellikleri klasik delil toplama yöntemlerini ciddi biçimde sınırlamaktadır. Buna ek olarak, özellikle kolluk üzerinde yapılan çalışmalar genel kolluk birimlerinin adli bilişim delillerini toplamada yetersiz olduğunu ve bu eksikliği gidermeye yönelik eğitimlerin yüzeysel düzeyde kalarak, siber suçların soruşturulmasına yönelik ihtiyaçlara uyum sağlayamadığını ifade etmektedir. Bu eksiklik sonucundaysa, adli bilişim incelemelerinin hepsinin uzman kolluğa yönlendirildiği ancak uzman kolluğun ise, sayı

[94] Çelik (n 38) 138; Çetin Gümüş, 'Bilişim Suçlarıyla Mücadelede Polisin Eğitimi' (Yayınlanmamış Doktora Tezi, Fırat Üniversitesi 2008) 261.

olarak tüm dosyaları yürütebilecek kapasitede olmadığı belirtilmektedir. Türkiye'deki saha araştırmaları da benzer biçimde bu eksikliğe vurgu yapmakta ve adli bilişim veya siber suç konularında ceza adalet sistemi uzmanlarına yönelik düzenli eğitimlerin olmadığına dikkat çekmektedir. Alanyazındaki çalışmalarda dikkat çeken bir unsur, örneklemin polis veya kolluk görevlileri olmasıdır. Siber suç soruşturmalarını yürüten savcılar veya yargılamasını gerçekleştiren hakimlerin teknik bilgi seviyelerine dair neredeyse hiç çalışma bulunmaması, soruşturma ve kovuşturma süreçlerinin verimliliğini tespit etmeyi ve uygulamada karşılaşılan zorluklar arasında değerlendirmeyi zorlaştırmaktadır.

Uluslararası düzeyde iş birliği süreçlerinde ise hukuki ve bürokratik engellerin süreleri uzattığı ve çoğu zaman iş birliğini işlevsiz kıldığı alanyazında vurgulanmaktadır. Evrak çevirisi, usul hataları, çoklu kurumsal onay süreçleri gibi nedenlerle delil paylaşımının geciktiği, delil paylaşımının ikili anlaşmalara bağlı olarak sağlandığı da göz önüne alındığında siber suçların hızlı müdahale gerektiren doğasıyla çeliştiği alanyazında değerlendirilmektedir. Her ne kadar Avrupa Konseyi Siber Suç Sözleşmesi'nde bu süreçleri hızlandırmaya yönelik düzenlemeler barındırsa da sözleşmenin uygulanmadığı hallere yönelik yaptırım gücünün bulunmaması bu maddelerin işlevselliği açısından eleştirilmektedir. Ayrıca, Türkiye'nin 2 No'lu Ek Protokol'e henüz taraf olmaması dijital delil paylaşımı süreçlerini yavaşlatan önemli bir faktör olarak öne çıkmaktadır.

Siber suçların toplumsal bağlamda düşük görünürlüğü hem istatistiksel veri üretimini hem de siber suçla mücadele politikalarının geliştirilmesini süreçlerini sınırlamaktadır. Alanyazın, mağdurların çoğu zaman olayın suç teşkil ettiğinin farkına varamadıklarını veya farkına varsalar bile maddi zararlarını düşük görmeleri, güvenlik birimlerine güvensizlik duymaları veya yargı süreçlerine yönelik olumsuz algıları sebebiyle suç bildiriminde bulunmaktan kaçındıklarını belirtmektedir. Ticari işletmeler nezdindeyse, marka değerlerini koruma kaygısıyla suç bildiriminde bulunmaktan kaçındıkları ifade edilmektedir. Alanyazın incelemesinde ifade edilen bulguları barındıran çalışmalar bulunmaktaysa da Türkiye'de bu konuda yeterli ampirik çalışmaya erişilememiştir. Türkiye'de, "karanlık sayılar" olarak ifade edilen resmi suç istatistiklerine yansımayan suç olgularının tespitine ilişkin saha araştırmalarının yetersiz olması, siber suçların gerçek boyutunu tespit etmeyi zorlaştırmaktadır. Yalnızca resmi istatistiklere dayanan veriler üzerinden değerlendirmeler gerçekleştiğinde bazı siber suç mağduriyetleri daha görünür hale gelirken, bazılarıysa görünmez kalmaktadır. Bu bağlamda, mağdur yaklaşımının daha verimli incelenerek, veri temelli politikaların üretilebilmesi için Türkiye'de siber suç mağduriyetlerine yönelik daha fazla araştırma yapılması gerekmektedir.

Bu araştırma bütüncül olarak değerlendirildiğinde, siber suçla mücadelede karşılaşılan zorlukların birbirini besleyen yapısal bir döngü oluşturduğu görülmektedir. Tanımsal belirsizlikler uluslararası işbirliğini sınırlamakta, teknik ve personel yetersizlikleri soruşturma süreçlerini yavaşlatmakta ve toplumsal farkındalık eksikliği bildirimsizlik ve veri eksikliğine yol açarak hukuki ve teknik reformların etkisini zayıflatmaktadır. Türkiye bağlamında da geçerli olan bu döngüye müdahale yalnızca yasal düzenleme değişiklikleriyle değil, çok katmanlı bir yaklaşımla ancak mümkün olabilir.

IV. Muhakeme Süreçlerinin Geliştirilmesi İçin Çözüm Önerileri

Siber suçlarla etkin mücadele için öncelikle ulusal ve uluslararası düzeyde hukuki çerçevenin güçlendirilmesi gereklidir. Mevzuat farklılıklarını azaltmak adına Siber Suçlar Sözleşmesi gibi uluslararası belgelerin kapsayıcılığı genişletilmeli ve daha fazla ülkenin taraf olması sağlanmalıdır. Siber suçlara yönelik daha caydırıcı yaptırımlar içeren düzenlemeler ile mahkeme kararlarının ve adli iş birliği süreçlerinin hızlandırılmasına yönelik yasal düzenlemelerin hayata geçirilmesi, yargı süreçlerinin etkinliğine katkı sunacaktır. Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi) ve 2 No'lu Ek Protokol, dijital delil paylaşımı ve sınır ötesi soruşturmalar konusunda uluslararası ölçekte en kapsamlı düzenlemelerdendir. Türkiye'nin de

Siber Suçlar Sözleşmesi'nin imzacısı olmasının yanı sıra, 2 No'lu Ek Protokolü de en kısa sürede imzalaması ve iç hukuka aktarması, uluslararası adli süreçlerde hız kazanılması bakımından faydalı olacaktır.

Uluslararası iş birliği mekanizmalarının güçlendirilmesi, siber suçlarla mücadelede temel unsurlardan bir diğeridir. Bu çerçevede, bilgi ve istihbarat paylaşımının daha sistematik hale getirilmesi, Interpol, Europol, Eurojust ve UNODC gibi uluslararası kuruluşlarla iş birliğinin artırılması önem taşımaktadır. Özellikle sınır aşan soruşturmalarda adli yardımlaşma süreçlerinin hızlandırılması ve siber suçluların iadesine ilişkin prosedürlerin kolaylaştırılması gereklidir. Uluslararası düzeyde ortak operasyon merkezlerinin ve hızlı müdahale ekiplerinin kurulması, olaylara zamanında müdahale edebilmek açısından önemlidir. Kamu-özel sektör iş birliği çerçevesinde, teknoloji şirketleri ile kolluk birimleri arasındaki koordinasyonun artırılması da bu mücadelede kritik rol oynamaktadır. Türkiye'de uluslararası iş birliğini kolaylaştırmak üzere kurulmuş olan 7/24 iletişim noktalarının yaygınlaştırılması ve etkinliğinin artırılmasıyla, bankalar ve siber güvenlik şirketleri gibi özel sektör paydaşlarıyla stratejik iş birliklerinin geliştirilmesi bu bakımdan önemli bir adımdır.

Siber suçların ortaya çıkarılması ve delillendirilmesi süreçlerinde dijital adli bilişim kapasitesinin güçlendirilmesi büyük önem arz etmektedir. Bu doğrultuda, dijital delillerin toplanması, saklanması ve analizine ilişkin uluslararası standartların geliştirilmesi gerekmektedir. Bulut teknolojileri ve şifreleme sistemlerine ilişkin teknik ve hukuki çözümler üretilmeli; adli bilişim incelemeleri için ulusal düzeyde merkezi analiz birimlerinin kurulması teşvik edilmelidir. Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nun da yeni teknolojiler ve suç işleme yöntemleri göz önüne alınarak güncellenmesi, soruşturma kapsamındaki işlemlere yönelik uygulama yönetmeliklerinin kapsamlı biçimde düzenlenmesi muhakeme süreçlerinin hukuki dayanağını oluşturması bakımından gereklidir.

Kolluk kuvvetleri ile yargı mensuplarıysa, siber suçlarla etkin biçimde mücadele edebilmek için kapsamlı ve sürekli eğitim programlarına ihtiyaç duymaktadır. Bu kapsamda, siber suç alanında uzmanlaşmış polis ve savcıların yetiştirilmesine yönelik eğitim programları oluşturulmalı, teknik eğitimlerin kapsamı genişletilmelidir. Özellikle hâkim ve savcılara dijital delillerin hukuki niteliği ve adli bilişim süreçleri hakkında bilgi sunan özel eğitim modülleri hazırlanmalı; bu alanda görev yapan personelin düzenli olarak teknik gelişmelerle güncellenmesi sağlanmalıdır. Bu kapsamda, Adalet Akademisi'nde hakim ve savcılara yönelik düzenli eğitimlerin yaygınlaştırılmasının yanı sıra; özellikle hukuk fakültelerinde, bilişim hukukuna yönelik derslerin müfredata dahil edilmesi, hukukçuların dijital delillerin hukuki boyutu, siber suç tipleri ve bu alandaki güncel sorunlara ilişkin temel bilgi ve farkındalık kazanmalarını sağlaması açısından değerlendirilmelidir.

Mücadele kapasitesinin artırılabilmesi için ilgili kurumların teknik ve finansal kaynakları da güçlendirilmelidir. Bu bağlamda, ilgili birimlere yeterli bütçe tahsis edilmeli, teknik altyapı modernize edilmeli ve nitelikli uzman personel istihdamı artırılmalıdır. Yapay zeka destekli analiz sistemleri ile büyük veri teknolojilerinin kullanımı teşvik edilmeli, kamu-özel sektör iş birlikleri kapsamında teknik destek ve fon sağlanmasına yönelik yapılar kurulmalıdır. Türkiye bağlamında, siber suçlarla mücadele eden tüm kamu kurumlarının teknik donanım, yazılım lisansları ve personel ihtiyacına yönelik ihtiyaç analizi gerçekleştirilerek, merkezi ve sürekli bir bütçe planlaması yapılması, siber suçları tespit etme ve bu suçla mücadele açısından gerekli teknik altyapının sağlanması bakımından faydalı olacaktır.

Siber suçlarla mücadelede önleyici politikalar da en az cezai süreçler kadar önemlidir. Toplumun genelinde farkındalık oluşturulması amacıyla bilinçlendirme kampanyaları düzenlenmeli ve bireylere yönelik temel siber güvenlik eğitimleri yaygınlaştırılmalıdır. Bireylerin ve işletmelerin koruyucu güvenlik önlemleri almaları teşvik edilmeli, siber suç mağdurlarının şikâyet mekanizmalarını etkin şekilde kullanabilmelerini sağlayacak sosyal ve hukuki destek sistemleri oluşturulmalıdır. Ayrıca, özel sektör kuruluşlarının veri ihlallerini bildirme yükümlülükleri güçlendirilmelidir. Türkiye'de ise, ilkokul düzeyinden başlayarak yaşa uygun temel siber güvenlik eğitimleri müfredata dahil edilmeli; kamu spotlarının yaygınlaştırılmasının yanı sıra,

belediyeler ve sivil toplum kuruluşlarıyla işbirliği yapılarak toplumsal farkındalık çalışmalarının yaygınlaştırılması değerlendirilmelidir.

Bu öneriler, siber suçlara karşı çok düzeyli ve bütüncül bir yaklaşımı teşvik etmektedir. Ancak uygulamada başarının sağlanabilmesi, özellikle uluslararası iş birliği mekanizmalarının daha hızlı ve etkin biçimde işletilmesine bağlıdır. Bu nedenle, teknik yeterliliğin artırılmasının yanı sıra, karşılıklı güvene dayalı ve standartlaştırılmış iş birliği protokollerinin geliştirilmesi büyük önem taşımaktadır.

Sonuç

Bu çalışma, Türkiye'de siber suç soruşturmalarında karşılaşılan yapısal, hukuki, teknik ve toplumsal engeller incelemiştir. Belgelere dayalı nitel araştırma yöntemiyle yürütülen analiz, mevcut yasal düzenlemelerin teknolojik gelişmelerin gerisinde kaldığını, kurumsal kapasitenin yetersiz olduğunu ve toplumsal farkındalığın sınırlı düzeyde seyrettiğini ortaya koymaktadır. Bulgular, Türk Ceza Kanunu'nun 243–246. maddelerinde yer alan siber suç tanımlarının güncel dijital suç türlerini kapsamakta yetersiz olduğunu; Ceza Muhakemesi Kanunu'nun 134. maddesinin ise güncel teknolojilere uygulanabilirlik bakımından belirsizlikler içerdiğini göstermektedir. Bu eksiklikler hem delil toplama sürecinde hem de temel hakların korunmasında hukuki tutarsızlıklara neden olmakta; farklı yorumlara açık mevzuat, uygulamada eşitsiz ve kimi zaman sonuçsuz soruşturmalara yol açmaktadır.

Teknik düzeyde, adli bilişim altyapısının yetersizliği, uzman personel eksikliği ve kolluk kuvvetlerinin sınırlı eğitimi, dijital delillerin doğru biçimde elde edilmesini ve analiz edilmesini güçleştirmekte; soruşturma süreçlerinde gecikmelere ve delillerin hatalı değerlendirilmesine neden olabilmektedir. Uluslararası alanda ise, karşılıklı adli yardımlaşma mekanizmalarındaki bürokratik engeller, çok dilli prosedürler ve Türkiye'nin Avrupa Konseyi Siber Suç Sözleşmesi'ne ilişkin İkinci Ek Protokol'e taraf olmaması, sınır ötesi delil paylaşımının etkinliğini sınırlamaktadır.

Toplumsal açıdan değerlendirildiğinde, siber suçlara ilişkin farkındalığın düşük olması, mağdurların yaşadıkları ihlalleri bildirmemelerine ve birçok siber olayın kayıtlara geçmemesine neden olmaktadır. Kurumsal aktörlerin itibar kaygısıyla olayları raporlamaktan kaçınması da bu görünmezliği derinleştirmekte, istatistiksel verilerin güvenilirliğini azaltmaktadır.

Sonuç olarak, Türkiye'de siber suçla mücadele, hukuki, teknik ve toplumsal faktörlerin birbirini beslediği döngüsel bir yapı içinde şekillenmektedir. Bu nedenle, siber suçların etkin biçimde önlenmesi ve kovuşturulması yalnızca mevzuatın güncellenmesiyle değil; adli bilişim kapasitesinin güçlendirilmesi, insan kaynağının uzmanlaştırılması, uluslararası iş birliğinin kurumsallaştırılması ve kamuoyu farkındalığının artırılmasıyla mümkün olacaktır. Hukuki yenilik, teknik uzmanlık ve toplumsal bilinç ekseninde geliştirilecek bütüncül bir politika yaklaşımı, Türkiye'nin dijital çağın gerekliliklerine uyum sağlayan, daha dirençli bir ceza adalet sistemine ulaşmasının temel anahtarıdır. Bununla birlikte, bu çalışmada yer verilen öneriler nihai çözümler değil, yol gösterici adımlar olup; siber suçlarla etkin mücadeleye yönelik daha ayrıntılı ve uygulamaya yönelik çalışmaların geliştirilmesi gerekmektedir.

Etik Kurul Onayı: Bu çalışma için Üsküdar Üniversitesi Girişimsel Olmayan Araştırmalar Etik Kurulu'ndan izin alınmıştır (Tarih: 23.02.2023, Karar No: 6135134).
Hakem Değerlendirmesi: Dış bağımsız.
Yazar Katkısı: Çalışma Konsepti/Tasarım- S.A., G.N.Ç.; Veri Toplama- G.N.Ç.; Veri Analizi/Yorumlama- G.N.Ç.; Yazı Taslağı- G.N.Ç.; İçeriğin Eleştirel İncelemesi- S.A.; Son Onay ve Sorumluluk- S.A., G.N.Ç.
Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Ethics Committee Approval: Ethical approval for this study was obtained from the Üsküdar University Non-Interventional Research Ethics Committee (Date: 23 February 2023, Decision No: 6135134).
Peer Review: Externally peer-reviewed.
Author Contributions: Conception/Design of Study- S.A., G.N.Ç.; Data Acquisition- G.N.Ç.; Data Analysis/Interpretation- G.N.Ç.; Drafting Manuscript- G.N.Ç.; Critical Revision of Manuscript- S.A.; Final Approval and Accountability- S.A., G.N.Ç.
Conflict of Interest: The authors have no conflict of interest to declare.
Grant Support: The authors declared that this study has received no financial support.

Yazar Bilgileri / Author Details

Görkem Nazlı Çelik (Doktor)
[1] Üsküdar Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Adli Bilimler Bölümü, Bağımlılık ve Adli Bilimler, İstanbul, Türkiye
0000-0002-1077-5745 gorkemnazli.celik@st.uskudar.edu.tr

Sevil Atasoy (Profesör Doktor)
[1] Üsküdar Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Adli Bilimler Bölümü, Bağımlılık ve Adli Bilimler, İstanbul, Türkiye
0000-0002-0236-0267 atasoy@uskudar.edu.tr

Bibliyografya | Bibliography

Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, 'Adalet İstatistikleri 2009' (2009) 29.10.2024 tarihinde erişildi.

Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü, 'Adalet İstatistikleri 2023' (2024) 07.10.2024 tarihinde erişildi.

Afandak K, 'Ceza Muhakemesinde Dijital Deliller' (Yayımlanmamış Doktora, Ankara Üniversitesi 2021).

Ajayi EFG, 'Challenges to Enforcement of Cyber-Crimes Laws and Policy' (2016) Vol.6(1) Journal of Internet and Information Systems.

Ajoy PB, 'Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis' (2023) *5(2): 74-79* Sch Int J Law Crime Justice.

Akdemir N, Sungur B ve Başaranel B, 'Birleşik Krallıkta Siber Ekonomik Suçlara Yönelik Kolluk Faaliyetleri Sorunlarının İncelenmesi' (2020) Özel Sayı (International Security Congress Special Issue), Güvenlik Bilimleri Dergisi, 113-134.

Aköz BC, 'Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları İle Örnek Yargısal Kararların Analizi ve Mevzuat Örnekleri' (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu 2018).

Alastal AI ve Shaqfa AH, 'Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool' (2023) 11 Journal of Data Analysis and Information Processing 121.

Alatış Taş K, 'Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi' (Yüksek Lisans Tezi, Çukurova Üniversitesi 2010).

Aldoori A, 'Uluslararası Hukukta Siber Suçla Mücadele' (Yayımlanmamış Yüksek Lisans, İstanbul Üniversitesi 2020).

Avşar Z ve Öngören G, *Bilişim Hukuku* (Türkiye Bankalar Birliği 2010).

Ayhan ZA, 'Ceza Muhakemesi Hukukunda Dijital Deliller' (Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi 2022).

Bandler J ve Merzon A, *Cybercrime Investigations: A Comprehensive Resource for Everyone* (First Edition, CRC Press/ Taylor & Francis Group 2020).

Başbüyük İ, 'Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması' (2013) S:15, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 1583-94.

Başlar Y, 'Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri' (2013) Uyuşmazlık Mahkemesi Dergisi 82.

Bossler AM ve Holt TJ, 'Patrol Officers' Perceived Role in Responding to Cybercrime' (2012) 35 Policing: An International Journal of Police Strategies & Management 165.

Brown CSD, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' (2015) 9(1), International Journal of Cyber Criminology, 55-119.

Brunner M, 'Challenges and Opportunities in State and Local Cybercrime Enforcement' (2019) 10 J. National Security & Policy 563.

Çakmakkaya BY ve Akpınar T, 'Bilişim Suçları İle Mücadelede Karşılaşılan Sorunlar' (2018) 4 Balkan and Near Eastern Journal of Social Sciences 123.

Çelik GN, 'Ulusal ve Uluslararası Ceza Hukukunda Siber Suç ve Türkiye'de Siber Suç Soruşturmasının İşleyişi' (Yayımlanmamış Doktora, Üsküdar Üniversitesi 2025).

Ceran O, 'Adli Bilişim Araştırmalarına Küresel Bir Bakış: Bibliyometrik Analiz Ile Yayın Trendleri ve Araştırma Yönelimleri' (2025) 13 Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji 859.

Chawki M ve diğerleri, *Cybercrime, Digital Forensics and Jurisdiction* (Springer International Publishing 2015).

Choi K-S, Lee CS ve Louderback ER, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020).

Clough J, *Principles of Cybercrime* (Second Edition, Cambridge University Press 2015).

Council of Europe, 'The Council of Europe at a Glance' <https://www.coe.int/en/web/portal/the-council-of-europe-at-a-glance> 17.10.2024 tarihinde erişildi.

Cross C ve diğerleri, 'Trends & Issues in Crime and Criminal Justice Responding to Cybercrime: Results of a Comparison between Community Members and Police Personnel' (2021) *Trends & issues in crime and criminal justice* no. 635. Canberra: Australian Institute of Criminology. <https://www.aic.gov.au/publications/tandi/tandi635> 13.10.2024 tarihinde erişildi.

Curtis J ve Oxburgh G, 'Understanding Cybercrime in "Real World" Policing and Law Enforcement' (2023), *96*(4),The Police Journal: Theory, Practice and Principles 573-592.

de Arimatéia da Cruz J, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020).

de Arimatéia da Cruz J, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020).

De Paoli S ve diğerleri, 'A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists' (2020) Volume 15, Issue 2, *Policing: A Journal of Policy and Practice* 1429-1445.

Demiroğlu AT, 'Stratejik İstihbaratın Önemi: Bilişim Suçları Uygulaması' (Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi 2015).

Dülger MV, 'Türk Ceza Hukukunda Bilişim Suçları' (Yüksek Lisans Tezi, İstanbul Üniversitesi 2004).

Dülger MV, *Bilişim Suçları ve İnternet İletişim Hukuku* (10. Bası, Seçkin 2023).

Durdu A, 'Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı (Gaziantep İli Örneği)' (Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi 2015).

Europol ve Eurojust, 'Common Challenges in Combating Cybercrime As Identified by Eurojust and Europol' (2019) <https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf> 13.10.2024 tarihinde erişildi.

Gercke M, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2012) <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> 21.10.2024 tarihinde erişildi.

Gillespie AA, *Cybercrime - Key Issues and Debates* (Routhledge 2016).

Gordon S ve Ford R, 'On the Definition and Classification of Cybercrime' (2006) 2 Journal in Computer Virology 13.

Gözüşirin M, '5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları Ile Mücadeleye İlişkin Model Önerisi' (Yüksek Lisans Tezi, TC Kara Harp Okulu 2011).

Griffiths C, 'The Latest 2024 Cyber Crime Statistics' (*AAG*, 1 October 2024) <https://aag-it.com/the-latest-cyber-crime-statistics/> 25.11.2024 tarihinde erişildi.

Gümüş Ç, 'Bilişim Suçlarıyla Mücadelede Polisin Eğitimi' (Yayınlanmamış Doktora Tezi, Fırat Üniversitesi 2008).

Gün N, 'Türk Ceza Hukukunda Bilişim Suçları' (Yüksek Lisans, Çankaya Üniversitesi 2020).

Hadlington L ve diğerleri, 'A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime' (2021) Volume 15, Issue 1, Policing: A Journal of Policy and Practice, 34-43.

Harkin D ve Whelan C, 'Perceptions of Police Training Needs in Cyber-Crime' (2022) 24(1), International Journal of Police Science and Management, 66-76.

Hekim H ve Başıbüyük O, 'Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları' (2013) 4(2), Uluslararası Güvenlik ve Terörizm Dergisi, 135-158.

Hinduja S, 'Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams' Volume: 27 Issue: 3, Policing: An International Journal of Police Strategies & Management, 341-357.

Holt TJ ve Bossler AM, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Springer International Publishing 2020).

Holt TJ, Freilich JD ve Chermak SM, 'Exploring the Subculture of Ideologically Motivated Cyber-Attackers' (2017), 33(3),Journal of Contemporary Criminal Justice, 212-233.

IBM, 'Cost of a Data Breach Report 2024' (2024) <https://www.ibm.com/reports/data-breach> 28.11.2024 tarihinde erişildi.

Interpol, '2022 Interpol Global Crime Trends Summary Report' (2022) 21.10.2024 tarihinde erişildi.

Jahankhani H, Al-Nemrat A ve Hosseinian-Far A, 'Cybercrime Classification and Characteristics', *Cyber Crime and Cyber Terrorism Investigator's Handbook* içinde (Elsevier Inc 2014).

Keskin S, 'Bilisim Suclarında CMK 134. Maddesindeki Hükümlerin Uygulamasında Yaşanan Aksaklıklar' (2021) 11 Kirikkale University Journal of Social Sciences 649.

Lavorgna A, 'Organized Crime and Cybercrime' Adam M Holt Thomas J. and Bossler (ed), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020).

Lee JR, 'Cyberpolicing', *Oxford Research Encyclopedia of Criminology and Criminal Justice* (Oxford University Press 2022).

Leppänen A ve Kankaanranta T, 'Cybercrime Investigation in Finland' (2017) 18(2), Journal of Scandinavian Studies in Criminology and Crime Prevention, 157-175.

Leukfeldt ER. ve Holt TJ., *The Human Factor of Cybercrime* (Routledge 2020).

Leukfeldt R, Veenstra S ve Stol W, 'High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands' (2013) 7(1), International Journal of Cyber Criminology, 1-17.

Lovet G, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges', *Virus Bulletin Conference* (2009) < https://www.virusbulletin.com/conference/vb2009/abstracts/fighting-cybercrime-technical-juridical-and-ethical-challenges/> 26.10.2024 tarihinde erişildi.

Manning C, 'Old Laws, New Crimes: Challenges of Prosecuting Cybercrime in Ireland' (2016) SSRN Electronic Journal.

McGuire M ve Dowling S, 'Cyber Crime: A Review of the Evidence Research Report 75' (2013) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf> 13.10.2024 tarihinde erişildi.

Mckoy C, 'Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level' (Doktora, Walden University 2021) <https://scholarworks.waldenu.edu/dissertations/11204> 13.10.2024 tarihinde erişildi.

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

Nowacki J ve Willits D, 'An Organizational Approach to Understanding Police Response to Cybercrime' (2020) Vol. 43 No. 1, Policing: An International Journal, 63-76.

Önok M, 'Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği' (2013) Cilt: 19 Sayı: 2, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 1229-1270.

Özen M ve Özocak G, 'Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Ar Ama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)' (2015) 1 Ankara Barosu Dergisi 41.

Payne BK, 'Defining Cybercrime' Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde (Springer International Publishing 2020).

Phillips K ve diğerleri, 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' (2022) 2(2), Forensic Sciences, 379-398.

Sandilaç N, 'Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya' (2022) 4 Bilişim Hukuku Dergisi 81.

Senjo SR, 'An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data' (2004), 17, Security Journal, 55-71.

SİBERAY, 'Siberay Sözlük' (*Siber Suçlarla Mücadele Daire Başkanlığı*) <https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf> 26.10.2024 tarihinde erişildi.

Sofaer AD ve Goodman SE, 'Cyber Crime and Security The Transnational Dimension', *Hoover Institution's National Security Forum Series* içinde (Hoover Institution Press 2001).

Staniforth A, 'Police Investigation Processes: Practical Tools and Techniques for Tackling Cyber Crimes', *Cyber Crime and Cyber Terrorism Investigator's Handbook* içinde (Elsevier Inc 2014).

Taşçı U ve Can A, 'Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014' (2015) 25(2), Fırat Üniversitesi Sosyal Bilimler Dergisi, 229-248.

Topçuoğlu P, 'Türk Ceza Kanunu Kapsamında Bilişim Sistemine Girme Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2022).

Tropina T, 'Cyber-Policing: The Role of the Police in Fighting Cybercrime', *European Police Science and Research Bulletin – Police Science and Police Practice in Europe, Special Conference Edition* (2017) <https://www.cepol.europa.eu/sites/default/files/Special%20Conference%20Edition%20Nr.%202.pdf> 13.10.2024 tarihinde erişildi.

TÜİK, 'Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2024' <https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2024-53492> 25.11.2024 tarihinde erişildi.

Turhan O, 'Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)' (Planlama Uzmanlığı Tezi, TC Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı 2006).

Ulaştırma ve Altyapı Bakanlığı, 'Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020–2023' (2020) <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf> 17.10.2024 tarihinde erişildi.

Van Nguyen T, Truong TV ve Lai CK, 'Legal Challenges to Combating Cybercrime: An Approach from Vietnam' (2022) 77, Crime, Law and Social Change, 231-252.

Viano EC, *Cybercrime, Organized Crime, and Societal Responses* (Springer International Publishing 2017).

Wall DS, 'Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing' R Brownsword, E Scotford and K Yeung (eds), *The Oxford Handbook on the Law and Regulation of Technology* içinde (Oxford University Press 2017).

Willits D ve Nowacki J, 'The Use of Specialized Cybercrime Policing Units: An Organizational Analysis' (2016), 29(2), Criminal Justice Studies, 105–124.

Yağcı B, 'Bilgi ve İletişim Teknolojilerinin Gelişmesiyle Değişen Siber Suç Tanımı ve Yaklaşımlar' (2023), 1(1) (Eylül 2023), Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi), 147-182.

Yazıcı N, 'Türk Ceza Hukukunda Bilişim Suçları (TCK. M. 243-244 ve 245)' (Yayımlanmamış Yüksek Lisans, Fatih Sultan Mehmet Vakıf Üniversitesi 2021).