CEZA MUHAKEMESİ HUKUKU ÖZELİNDE YARGIDA DİJİTALLEŞME

Candide ŞENTÜRK*

ÖZ

21'inci yüzyılın getirdiği devinimlere ve çağın gereklerine uyum sağlamak oldukça önemlidir. Çağın değişmesi ve özellikle bilişim teknolojileri alanında baş döndürücü gelişmeler, kaçınılmaz olarak hukuk dünyasında da çeşitli değişimlere yol açmaktadır. Karşılaştırmalı hukuk sistemlerine bakıldığında, yargıda dijitalleşmenin sıklıkla dile getirildiği ve alt yapı çalışmalarının hızla sürdürüldüğü görülmektedir.

2020 yılında beklenmedik şekilde COVID-19 pandemisinin dünya ve ülke genelinde giderek yayılması, eğitimden sağlığa kadar her alanda dijitalleşmenin ne kadar önemli bir gereksinim olduğunu gözler önüne sermiştir. Aynı durum, yargı hizmetleri açısından da söz konusu olup, ertelenmek zorunda kalınan duruşmalar, bitmek bilmeyen yargılama süreçleri ve insan sağlığının tehlikede olması itibariyle iş gücünün sayısının azalması yargıda dijitalleşme gereksinimini vazgeçilmez hale getirmiştir. Bu durumda gerek soruşturma gerekse kovuşturma evresinde birçok işlemin online yapılmasına olanak sağlanması gerekmektedir. Bu bağlamda online uygulamaları bir süre önce hayata geçirmiş olan ülkelerin kanunlarındaki düzenlemeler ve deneyimleri göz önünde bulundurularak Türk hukukunda ceza muhakemesinin dijitalleşmesi üzerine düşünülmesi gerekmektedir.

Anahtar Kelimeler: *Soruşturma, Kovuşturma, Dijitalleşme, Yargıda Dijitalizasyon, Online Duruşma*

DIGITALIZATION OF THE JUDICIARY IN CRIMINAL PROCEDURE LAW

Abstract

It is very important to adapt to the movements brought by the 21st century and meet the requirements of the era. Due to the change of age and the incredible speed of technological developments, various changes must also occur in the legal world. Looking at comparative legal systems, it is seen that digitalization in the judiciary is often expressed and infrastructure work is continuing rapidly.

* **Dr. Öğr. Üyesi**, Yaşar Üniv. Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku ABD/ İZMİR, **e-posta:** candide.senturk@yasar.edu.tr

ORCID : 000-0002-0227-1782

DOI : 10.34246/ahbvuhfd.933622

Yayın Kuruluna Ulaştığı Tarih : 13/01/2021

Yayınlanmasının Uygun Görüldüğü Tarih: 19/04/2021

The pandemic process, which began unexpectedly in 2020, has shown how important digitalization is. Due to the delayed hearings, endless judicial processes and the fact that human health is in danger, the decrease in the number of labor forces has once again underlined the need for digitalization in the judiciary. However, both the investigation and the prosecution phase of the online work should be provided. In this context, it is necessary to consider the regulations in the laws of the country that have implemented online applications some time ago and the applicability of these regulations in Turkish law.

Keywords: *Investigation, Prosecution, Digitalization, Digitalization in The Judiciary, Online Trial*

GİRİŞ

Ceza muhakemesi hukukunda dijitalleşme, dünyada ve Türkiye'de sıklıkla gündeme getirilen bir konu haline gelmiştir. Yargılama için yeni ve radikal bir değişiklik önerisi geldiğinde, durumu dışarıdan bir gözlemci olarak değerlendirme gereksinimi vardır. Yargılama faaliyetlerinin siber alana kayması, yeni ve farklı bir yasal yaklaşımı da gündeme getirmektedir. Özellikle 2019 yılının son aylarında Çin'de başlayıp giderek tüm dünyaya yayılan COVID-19 pandemisinin yarattığı olağanüstü durum nedeniyle yargılamaların yapılamaması ve ülkelerde yargı sürelerinin geçici süre durdurulması önemli zaman ve para kayıplarına sebebiyet vermiştir. İşte bu noktada yargının dijitalleşmesi üzerinde *yeniden* düşünmek ve değerlendirmelerde bulunmak zorunluluğu daha da güncellik kazanmıştır. Nitekim halihazırda tartışılan konulardan biri de önümüzdeki on yıllık süre içerisinde, karar verme yetkisinin makinalara aktarılmasının ve yargıda kısmen somutlaşmaya da başlayan yapay zekâ kullanımı ile doğrudan etkileşim kurma mekanizmasının geliştirilmesinin getirecekleridir.

Sanal ortamda var olan ya da uygulanan tehdit, yüze karşı doğrudan yapılan tehdit kadar güçlü olarak hissedilmediğinden, bireyler daha az önlem almakta ve öngöremedikleri tehditlere karşı daha rahat davranabilmektedirler. Özellikle çocuk pornografisi ve nefret suçlarına ilişkin sanal ortamda önemli riskler mevcuttur[1]. Söz konusu suçlar başta olmak üzere suçlulukla mücadele

[1] Susanne Beck, "Die Diffusion strafrechtlicher Verantwortlichkeit durch Digitalisierung und Lernende Systeme", Zeitschrift für Internationale Strafrechtsdogmatik, 15. Vol., 2/2020, s.41-51, s.43.

edebilmek için yargıda dijital deneyim adım adım yerleşmeye başlamıştır.

Yargıda başvurulacak dijital araçlar, zaman ilerledikçe ekonomi ve ticaret alanına da yansıyan etkiler gösterecektir. Günümüzde, elektronik ticaret alanında ortaya çıkan çoğu uyuşmazlıkta geleneksel hukuk kurallarına başvurulmasında bir sakınca görülmemektedir. Buna karşılık hukukun diğer alanlarında dijital bir yargılamanın nasıl yapılabileceği çeşitli tartışmaları da beraberinde getirmektedir. İnternetin yapısı, belirli web sitelerinin ve sitelere ait kimi bilgilerin kaynağını gizleme olanağı sağlar. Bu da doğal olarak suçun işlendiği yerin ve failin tespitini oldukça zorlaştırır. Mahkemelerin, eylemin nerede işlendiğini, suç siber uzayda işlense dahi, tespit etmesi gerekmektedir[2]. Ceza muhakemesi hukuku, bilimsel ve teknolojik gelişmeler karşısında ister istemez birtakım değişikliklere uğramak ve teknolojik gelişmeler karşısında kendisini yenilemek zorunda olan bir alandır. İşte bu çerçevede biz de çalışmamızda, ceza muhakemesi hukuku bakımından dijitalleşme gereklilikleri ve karşılaştırmalı hukuk alanındaki örneklemin Türk hukukunda uygulanabilirliği üzerinde duracağız.

I. Yargıda Dijitalleşme Beklentileri

Yargıda dijitalleşme çerçevesinde, 2030 yılına kadar, yapay zekâların yargı mekanizması içerisinde aktif kullanımını için adım atılması hedeflenmektedir[3]. Özellikle yapay zekânın verdiği kararların, insanoğlunun verdiği kararlarla karşılaştırıldığında daha az hata payı içereceği düşünülmektedir. Ancak dijitalleşme için, yargıda atılması gereken pek çok adım bulunmaktadır. Yasalaşma süreci belki de bu adımlardan sonuncusudur. Bireyin dijitalleşme bağlamındaki konumunun ne olacağı, fail ve mağdura etkileri, karar verme yetkisinin yapay zekâya aktarılması ve dijitalleşmenin toplumsal ve bireysel sonuçları dikkatlice irdelenmelidir.

Ceza muhakemesi hukukunun dijitalleşmesi, yürürlükte olan kanunların teknolojik ve bilimsel değişiklikler ışığında ortaya çıkan yeni yaşam gerçekliğine adapte edilmesi ile mümkün olacaktır[4]. Bu itibarla kanunlarımızda

---

2 Dow Jones v Gutnick davası, Avustralya'daki internet yargı yetkisindeki en önemli otoriteye ilişkin bir yargılamadır. Avustralya 2002 HCA 56; 2002 210 CLR 575. Macquarie Bank v Berg 1999 NSWSC 526; Alan Davidson, "Jurisdiction in Cyberspace", Social Media and Electronic Commerce Law, 2nd Edition, Publisher: Cambridge University Press, August 2018, s..327-349, s.329-330.

3 Beck, s.41.

4 Ringe/ Trute, Zentrum für Recht in der digitalen Transformation (ZeRdiT); Milan Kuhli/

çağın gerekliliklerine uygun birtakım değişikliklerin yapılması artık bir zarurettir. Dijitalleşmenin beraberinde getirdiği değişikliklerin aynı zamanda mevcut hukuk sistemlerinde hâkim olan temel hukuk ilkelerinde de birtakım değişikliğe yol açacağı ifade edilmektedir[5].

Amerika Birleşik Devletleri'nde bir süredir, suçluların tekrar suç işleme olasılıklarında yapay zekâ kullanılmaktadır[6]. Örneğin, birkaç yıl önce, Eric Loomis isimli hükümlü altı yıl hapis cezasına çarptırılmadan hemen önce deneme amaçlı kullanılan "*Compas*" algoritması ona çok yüksek bir mahkûmiyet riski atfetmiştir[7]. Ancak robot hakimlerin şu an için istenilen düzeyde olmadığı açıktır. Algoritmaların çeşitli kaynaklardan gelen büyük miktarda verileri işlemekle sınırlı bir rolü olduğu gözlenmektedir[8]. Dolayısıyla yargı mekanizmasında yapay zekânın doğrudan kullanılması için biraz daha zamana ihtiyaç bulunmaktadır.

Yapay zekâ kullanımının yargı açısından kazanımlarına olağanüstü bir potansiyel değeri atfedilmektedir. Avrupa Komisyonu tarafından kurulan *Yapay Zekâ Üzerine Üst Düzey Uzman Grubu*, bunu "bireylerin ve toplumun refahını ve ortak iyiliği artırmak için umut verici bir araç" olarak görmektedir[9]. Nitekim Grup Nisan 2019'da güvenilir bir yapay zekâ için gerekli etik kurallar yayınlayarak yapay zekâ sistemlerinin demokrasi, hukukun üstünlüğü ve bireyler açısından taşıdığı riskler minimize edilmeye çalışılmıştır[10].

Janique Brüning, "Einleitung zur ZIS-Sonderausgabe, Strafrecht und Digitalisierung in Wissenschaft und Praxis", Zeitschrift für Internationale Strafrechtsdogmatik, 2/2020, 15. Vol., s.39-41.

5 Beck, s.41.

6 https://www.propublica.org/article/machttp://www.zis-online.com/dat/artikel/2020_2_1342.pdfhine-bias-risk-assessments-in-criminal-sentencing (Erişim Tarihi:06.06.2020)

7 Smith, New York Times (22.6.2016), https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?module=inline (Erişim Tarihi: 21.06.2020); Lasse Quarck, "Zur Strafbarkeit von e-personen", ZIS, Vol.15, 2/2020, s.65-70, s.65.

8 Quarck, s.65.

9 Kai Cornelius, "Künstliche Intelligenz*",* Compliance und sanktionsrechtliche Verantwortlichkeit, Zeitschrift für Internationale Strafrechtsdogmatik, 15. Vol. 2/2020, s.51-65; s.51.

10 Hochrangige Expertengruppe für Künstliche Intelligenz (Fn. 3), S.5. Grubun getirdiği etik kurallar şöyledir: Yapay zekâ; a) yasal olmalı, yani yürürlükteki tüm yasa ve yönetmeliklere uymalıdır, b) etik ilke ve değerlere uygunluğu garanti etmelidir, yani etik olmalıdır ve c) hem teknik hem de sosyal açıdan sağlam olmalıdır.

Dijitalleşme ve otomasyonun ceza hukukunda yol açacağı gelişmeler konusunda beklenti, önce fail ve daha sonra mağdur bakımından gelişmelerin olması yönündedir. Şüpheli ya da şüphelilerin öncelikle ele geçirilmesi, işlenmesi muhtemel suçları azaltacak ve buna paralel olarak doğacak zararları minimize edecektir. Örneğin kimlik avı ya da hack gibi bilişim sistemlerine sızma, genellikle mağdura küçük zararlar vermekle beraber, failler bu eylemlerini kalabalık kişi gruplarına karşı işlediğinde çok büyük gelirler elde edebilmektedir.

Özel ve olağanüstü durumlarda ceza muhakemesi hukukunda dijitalleşmenin öncelikle hayata geçirilmesi gerektiği kabul edilmektedir[11]. Örneğin İsviçre hukukunda özellikli durumlara özgü dijitalleşmenin önü açılmaya çalışılmaktadır[12]. Tabi bu noktada klasik ceza muhakemesi evrelerine özgü ilkelerin bulunduğu göz ardı edilmemelidir. Halka açıklık ilkesinin dijitalleşme ile gerçekleşip gerçekleşemeyeceği tartışılmakta ve dijitalleşme ile halka açıklığın daha geniş kitlelere yönelik gerçekleştirilebileceği kanaati bulunmaktadır[13]. Dijital medya araçları (podcast ya da web TV gibi) ile müzakerelerin ve yargılama prosedürlerinin daha geniş kitlelere ulaşacağı bir gerçektir[14]. Böylelikle, mahkeme salonlarına ulaşmak için harcanan zaman ve emek daha verimli başka bir hizmet için kullanılabilecek ve masraflarda ciddi bir azalma söz konusu olabilecektir. Ayrıca dijitalleşme ile yargılama süreleri kısalabilecek ve AİHS m. 6 gereği makul sürede yargılanma hakkı tesisinde hükümetlerin eli kuvvetlenecektir. Yargılamada bir aksaklık, hata söz konusu ise yüksek yargılama mercileri söz konusu eksiklik ve aksaklıkları, sistemde kayıtlı bulunan celseleri izleyerek de net bir şekilde görebilecek ve çözüm çok daha hızlı geliştirilebilecektir. Ancak, müzakerelerin ya da kararların

[11] Andreas Lienhard/Daniel Kettiger, "Justiz in Krisenzeiten-Digitalisierung fördern", NZZ Nr. 84 09.04.2020, S.8. (www.swisslex.ch/de/doc/essay Erişim tarihi:03.05.2020).

[12] Benjamin Schindler, (Verfahrens und Gerichtsorganisationsrecht/Justizöffentlichkeit im digitalen Zeitalter), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, s.741-757, s.742.

[13] Schindler, s.743. ZPO ve BGG gereği mahkeme kararlarının erişilebilir olması kantonlarda bir zorunluluktur ve halka açıklık ile şeffaflığı sağlamaktadır. (Daniel Hürlimann, Publikation von Urtelien durch Gerichte, in: sui-generis, 2014, s.30 (dn.35)). Beat Brandli, "III. Kommunikation im Recht/Einsatz von Informations und Kommunikationstechnologie im schweizerischen Zivilprozess", Kommunikation in Wirtschaft, Recht und Gesellschaft, Stampfli Verlag, 2010, s.239-260, s.242 vd.

[14] İsviçre'de 21 Haziran 2013 tarihinde Federal Yüksek Mahkemede görülen Motion Schmid davasında kararın canlı yayında halka duyurulması ilk kez gündeme gelmiştir. (Schindler, s.750).

canlı yayın akışı ile paylaşılacak olması yargı mensuplarının baskı altına girmelerine sebebiyet verebilecektir.

Yargıda dijitalleşmenin birtakım avantajları olduğu gibi dezavantajları da bulunmaktadır. Muhakeme hukukunda geleneksel olarak halk, sözlü yargılamayı izlemek suretiyle duruşmaları takip edebilmektedir. Dijitalleşme, kara Avrupası hukuk sistemini benimseyen ülkelerde daha ziyade tebligat, sesli-görüntülü iletişim araçları aracılığı ile bilgilendirme aşamasında söz konusudur[15]. İsviçre örneğine bakacak olursak, elektronik ortamda adli işlem yapma, 2000'li yılların başından itibaren gündeme getirilmiş (kısmen de hayata geçirilmiş) olup 2013 yılından itibaren ERV (Eigenmittelverordnung[16]) uygulamasıyla avukatlar, yargılama makamları, noterler arasında elektronik adli iletişim ağı oluşturulmuştur[17]. Almanya'da da ulusal yargı iletişim ağı ile adli iş ve işlemlerin dijital ortamda yapılması sağlanmakla birlikte, yine de dijitalleşmenin tam anlamıyla gerçekleştiğinden söz edilememektedir. Diğer bir deyişle dijitalleşme istenen seviyeye ulaşmamıştır.

Yargıda dijitalleşmenin en çok da organize suçlulukla mücadele alanında kazanım sağlayacağı düşünülmektedir. Organize suçlarla mücadele edebilmek için soruşturma işlemlerinin sanal ortamda daha etkin yapılması gerekmektedir. Organize suçlulukta, failler bilgisayar teknolojisini etkin biçimde kullanmakta ve devletin gözetiminden kaçınmak için siber alanda deep web ya da dark web[18] de denilen internetin en derin seviyesinde suç işlemeye devam etmektedir. Benzer şekilde, örgütlü suçlulukta örgüt üyelerinin kendi aralarında uçtan uca şifreli telefon uygulamaları kullanmaları, soruşturma makamlarının işini oldukça zorlaştırmaktadır. Bu itibarla, pratikte uzaktan erişim yoluyla, şüphelilerin kişisel bilgisayarlarına ulaşmak ve delil toplamak için artan bir istek vardır[19].

---

15 Schindler, s.749-750.

16 Eigenmittel und Risikoverteilung der Banken und Wertpapierhauser, D:01.06.2012, Inkraft:01.01.2013.

17 Brandli, s.243.

18 Derin ağ ya da derin web arama motorlarının içeriğini kaydedemediği verilerin bulunduğu binlerce linkten oluşan bir sistem olarak tanımlanmaktadır. https://tr.wikipedia.org/wiki/Derin_Ağ (Erişim Tarihi:14.05.2020).

19 Ernst Platz, "Rechtliche Zulassigkeit von "Remote Forensic Software" in der Schweiz-Inwieweit existiert in der Schweiz eine rechtliche Grundlage für den Einsatz von "Remote Forensic Software" durch die Ermittlungsbehörden?"", sic, 2008, s.838-844.

II. Sayısal Delil ve Suç Soruşturmalarına Etkisi

A. Sayısal Delil

Sayısal delil, bir veridir. Öğretide yapılmış olan en detaylı tanıma bakacak olursak, *Değirmenci* sayısal delili şu şekilde tanımlamıştır: "*Sayısal delil, ceza muhakemesinde maddi olayı kısmen veya tamamen açığa çıkaracak nitelikte, bilişim sisteminde saklanan ve ortaya çıkarılması hukuki ve teknik süreçlerin sonucu olan veridir*"[20]. Sayısal delile dikkat çekici özelliği veren hususun, verinin saklandığı ya da depolandığı yerin olduğu noktasında bir şüphe bulunmamaktadır. Sayısal delil, bilişim sistemleri aracılığıyla oluşturulan ya da bilişim sistemlerinde depolanan veri olduğundan, elde edilmesinde klasik yöntemlerin kullanılması her zaman sonuç vermeyecektir. Klasik olay yeri soruşturmalarında fiziksel delillerin toplanması ile; sayısal suç soruşturmalarında ise sayısal delilin toplanması ile olay soruşturmacıların gözünde tekrar canlandırılmaya çalışılmaktadır. Bu bağlamda kısaca sayısal delilin elde edilme yöntemleri ve bu yöntemlerin soruşturmalara etkisi üzerinde duracağız.

B. Sayısal Delilin Suç Soruşturmalarına Etkisi

Sayısal delil, sabit disklerde, belleklerde, mobil telefonlarda, bilgisayar ve bilgisayar işlevi gören cihazlarda, bilgisayar ağlarında, sistem günlüklerinde, elektronik postalarda ve veri tabanlarında bulunabilmektedir. Sayısal delilin elde edilmesinde ulusal ve uluslararası bağlamda önerilen pek çok metodoloji mevcuttur[21]. Ülkemizde konuyla bağlantılı ilk düzenleme, 5320 sayılı Ceza Muhakemesi Kanunu'nun Yürürlük ve Uygulama Şekli Hakkında Kanun ile yürürlükten kaldırılan 4422 sayılı Çıkar Amaçlı Suç Örgütleri ile Mücadele Kanunu'nun 4'üncü maddesidir. Bilgisayar verilerini incelemeye olanak veren düzenlemenin geliştirilmiş hali, 5271 sayılı Ceza Muhakemesi Kanunu'nun 134 ve 135'inci maddesinde düzenlenmiş bulunmaktadır. Bilişim sistemlerinde 134'üncü madde hükmü aracılığı ile veri arama; 135'inci madde hükmü ile akış halinde bulunan verinin elde edilmesi mümkün hale getirilmiş bulunmaktadır. Ancak uygulamada sayısal delil elde etme konusunda yayınlanmış yol gösterici bir kılavuz bulunmadığından adli bilişim bilirkişiliği yapan kurum ve kuruluşlar tarafından olaya göre değişen metodolojilerin kullanıldığı görülmektedir.

---

[20] Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin, Ankara 2014, s.31.

[21] Konuyla ilgili detaylı bilgi için bkz. Değirmenci, s. 161-191.

Gelişen teknolojiye bağlı olarak zaman zaman kullanılan yöntemlerde değişiklik olmaktadır. Nitekim teknolojinin gelişmesi ile bilişim suç faillerinin de kullandığı yöntemler değişmektedir. Bu itibarla sayısal delil elde edilirken delillerin tamamının kaybolmadan ya da deforme olmadan elde edilmesinin yanında güvenliğinin sağlanması hususunda azami özen gösterilmesi gerekmektedir. Sayısal delilin elde edilmesinin önüne geçmek amacıyla kullanılan zararlı yazılımlar aracılığıyla suça ilişkin delillerin geriye dönük olarak tüm izleri silinebilmektedir. Bu itibarla sayısal delilin elde edilmesi ceza hukukunun genel ve özel önleme amacının yerine getirilmesi bakımından elzemdir.

Sayısal delillerin elde edilmesinin icrasında kullanılan çevrimiçi arama ya da uzaktan arama (remote search), kolluk kuvvetlerine ağa bağlı bilgisayarın sabit diskinde arama olanağı sunmasının yanında elektronik posta ve ağ trafiğinin izlenmesine de imkân sağlamaktadır. Uzaktan arama yönteminde gerçek zamanlı denetim yapılabildiğinden kamera aktif hale getirilebilmekte, mikrofon ile ortam dinlemesi gerçekleştirilebilmektedir[22]. Söz konusu yöntemin yasal zemini gerek uluslararası gerekse ulusal platformda bulunmamakla beraber, çoğu zaman konut araması ile iletişimin denetlenmesi tedbirlerine ilişkin normatif düzenlemeler kıyas yoluyla uygulama alanı bulmaktadır. İletişimin denetlenmesi tedbiri ile büyük ölçüde benzerlik göstermekle beraber, bu yöntemde gerçek zamanlı veri akışı olmasa da denetim ve arama yapılabilmektedir. Oysa iletişimin denetlenmesinde, iletişim olmadığında denetim de mümkün olmamaktadır. Bu itibarla *remote search* yöntemi, bilişim suçları ile mücadele bakımından etkin bir soruşturma yöntemi olarak karşımıza çıkmaktadır.

III. Yargıda Dijitalleşme Örnekleri

Sayısal (dijital) delillerin dijital izlemede edenilen online araştırmalar yoluyla araştırılması da yargının dijitalleşmesi başlığı altında değerlendirilmektedir[23]. Benzer şekilde, yapay zekânın karar verme mekanizmasında kullanılması

[22] Kees Hudig, "State Trojans:Germany Exports 'Spyware with a Badge'", Statewatch, Vol.21, No:4, 2012, s.1-3; Hans Kudlich, "Ceza Kovuşturmasında Federal Truva Atları-Dijital Çağda Özel Yaşam Alanının Korunması", Çeviren: Rabia Ünlü, Alman-Türk Karşılaştırmalı Ceza Hukuku, C.I, Yayına Hazırlayan: Prof. Dr. Dr. Eric Hilgendorf-Prof. Dr. Yener Ünver, İstanbul 2010, s.220 vd.

[23] Delia Magherescu, "Using New Means of Technology during the Penal Proceedings in Romania", Revista Brasıleıra De Dıreıto Processual Penal Vol:5, Issue:3, s.1189-1217, 2019, s.1191 vd.

da yargının dijitalleşmesi seçeneklerinden biri olarak karşımıza çıkmaktadır. Ceza sorumluluğunun tespitinde, sensörler yardımıyla ağ üzerinden bilgi alan ve aldığı bilgileri değerlendiren yapay zekâ makineler özel bir rol oynamaktadır. Ne var ki, makinelerin hangi durumlarda hangi kararları vereceğini önceden tahmin etmek veya kararların neye dayandığını geriye dönük olarak belirlemek mümkün olamamaktadır[24]. Dijitalleşmenin gerçek zamandaki tezahürü olarak karşımıza online (çevrimiçi) ya da uzaktan arama çıkmaktadır. Globalleşen dünyada bilişim teknolojilerinin gelişmesine paralel olarak bilişim suçları ile mücadele yöntemleri sürekli değişmektedir. Bilişim suçları ile mücadelede etkin bir yöntem olarak online arama pek çok ülkede kullanılmaya başlanmıştır. Yukarıda ifade edildiği üzere kimi ülkelerde yasal zemini olmamakla beraber söz konusu arama, iletişimin denetlenmesi tedbiri kıyasen uygulanmak suretiyle pratikte hayata geçirilmektedir. Bu bağlamda dijitalleşme örneklerine İtalya, Almanya, İsviçre, Amerika ve İngiltere uygulamaları nezdinde bakılacaktır.

A. **İtalya Örneği**

Birkaç yıl öncesine kadar düşünülemeyen dijitalleşme örnekleri ülkelerde sıklıkla gündeme gelmeye başlamıştır. Örneğin İtalyan Yargıtay'ı 2016 yılında, casus yazılımların bazı suç örgütlerinin çökertilmesi amacıyla kullanımının hukuka uygun olduğuna karar vermiştir[25]. Böylelikle İtalya'da casus yazılımlar (örneğin *Trojan Horse* olarak anılan Truva atları), organize suçlarla ilgili ceza soruşturmaları yürütülürken müdahaleci bir soruşturma tekniği olarak kullanılabilir hale gelmiştir. Yasal değişiklik ise söz konusu karardan birkaç yıl sonra yapılmıştır. Casus yazılım kullanımına, iletişimin kesilmesi ve çevrimiçi arama yapılması amacıyla başvurulmasına olanak tanınmaktadır. Bu tür bir dijital soruşturmanın, ne pahasına olursa olsun maddi gerçeğe ulaşmak amacıyla yapılacak hukuka aykırı soruşturma işlemlerini kapsamadığını belirtmek gerekir. Ocak 2019 tarihinde kabul edilen kanun değişikliği ile yolsuzluk dosyalarına özgü olarak örgüt üyeleri arası iletişimi kesmek amacıyla casus yazılımların kullanımı serbest kılınmıştır[26].

---

[24] Yapay zekânın kararlarını belirleme sıralamasına ilişkin detaylar için bkz. **Beck**, s.44 vd.

[25] Michele Caianiello, "Criminal Process faced with the Challenges of Scientific and Technological Development", European Journal of Crime, Criminal Law and Criminal Justice, I:27, s.267-291, 2019, s.274.

[26] İtalyan Ceza Muhakemesi Kanunu m.266-267

Bu noktada, ceza muhakemesinde maddi gerçeğe ulaşmak için her yöntemin hukuka uygun olmadığını belirtmek gerekir. Nitekim öğretide, İtalyan Yargıtay'ının kararından sonra yapılan kanun değişikliklerine ilişkin, durumun bıçak sırtında yürümekten farkı olmadığı söylenmiştir. Yerinde olarak, kolluk kuvvetleri ile savcılık makamının böylesine geniş bir araştırma yetkisinin olması sakıncalı bulunmuştur[27]. Her ne kadar casus yazılımların kullanımı, örgütün iletişimini kesmek ya da durdurmak amacıyla kullanılacak olsa da aynı zamanda sabit diski kopyalamak gibi veri elde etmek amacıyla kişilerin bilgi sistemlerine sızmanın mümkün olması ceza muhakemesinin esasları ile kimi temel hak ve özgürlükler bakımından oldukça düşündürücüdür. Zaman içerisinde, ceza muhakemesinde dijital soruşturma, delil araştırma iş ve işlemleri ile ilgili yöntemlerin genişlemesi, temel haklar bakımından düşündürücü olacağı gibi, vatandaşların adalete olan inançlarının zayıflamasına da neden olabilecektir.

Temel hakların ihlal edildiği bir dava örneği İtalya'da görülmüştür. Sınır Tanımayan Güvenlik isimli kâr amacı gütmeyen bir araştırma şirketi, *Exodus* isimli bir casus yazılımın, androidlere yönelik kötü amaçlı bir yazılım olduğunu tespit emiş ve 2016 yılından 2019 yılının başlarına kadar çok sayıda veri toplayarak Google Play Store'da gizlenen bir uygulama olduğunu belirlemiştir[28]. Nisan 2019'da aynı yazılımın IOS kullanıcılarına yönelik bir sürümü daha tespit edilince, Napoli Savcılığı olaya ilişkin soruşturma başlatmıştır. Yapılan araştırmada, *Exodus* yazılımının yerel savcılık büroları tarafından da kullanıldığı ortaya çıkmıştır; ancak halen hangi büroların kaç olayda bu yazılımı kullandığı açıklanmamıştır. İşte böyle bir durumun ortaya çıkması adalete duyulan güvenin sarsılmasına sebebiyet vermektedir. Nitekim soruşturmanın tamamlanmasından sonra resmi makamlar tarafından yapılan açıklamada, hakkında herhangi bir soruşturma olmayan 1000'in üzerinde kişinin bilgisinin Exodus aracılığıyla ele geçirildiği ifade edilmiştir[29].

Bu tür davalardan çıkarılabilecek pek çok önemli çıkarım bulunmaktadır. Devletin, vatandaşlarının temel hak ve özgürlüklerini korumak ve gözetmek en önemli yükümlülüklerdendir. Benzer ihlallerin önlenmesi için gerekli tedbirlerin alınması gerekmektedir. Bunun için sınırsız hareket kabiliyeti veren teknolojik gelişmelerin kullanımı konusunda sıkı bir denetim

[27] Caianiello, s.274.

[28] https://securitywithoutborders.org/blog/2019/03/29/exodus.html (Erişim Tarihi: 08.05.2020)

[29] Caianiello, s.275.

yapılmalıdır. Aksi takdirde sınırsız güç kullanımı önemli hak ihlallerine sebebiyet verebilecek ve AİHM nezdinde verilecek ihlal kararları kaçınılmaz olacaktır. *Exodus* davasından sonra, casus yazılımların potansiyel olarak bireylerin özel hayatları açısından tehlike içeren yegâne teknoloji olmadığı da ifade edilmektedir[30]. Telefon verilerinin toplanması, dijital çağın önemli gelişmelerinden biri olarak kabul edilir. Modern ceza muhakemesi hukukunda telefon iletişim verilerinin elde edilmesi birtakım sıkı kurallara bağlanmıştır. Bu kuralların belki de en önemlisi hâkim/savcılık yazılı emrinin bulunması zorunluluğudur. Ancak İtalyan Ceza Muhakemesi Kanunu'nda savcılığın iletişim verilerinin denetimi ile ilgili sıkı kurallar getirilmediği, bu söz konusu kapsamlı yetkinin soruşturma makamlarına sınırsız yetki ve erişim olanağı vermesinin tehlike oluşturduğu haklı olarak ifade edilmektedir[31].

Avrupa Adalet Divanı, telefon verileri toplama işlemleri için kolluk makamlarına emrin yetkili makam olarak hâkim tarafından verilmesi gerektiğini, bunun temel hakların ihlalini önlemek için bir güvence olduğunu ifade etmiştir[32]. Nitekim benzer bir durum GPS takibi bakımından da söz konusu olup, savcılık tarafından somut olaya özgü yazılı ya da sözlü bir emir verilmesine gerek bulunmaksızın polis kontrolünde denetim yapılması bir zafiyet olarak görülmektedir[33].

B. **Almanya Örneği**

Alman Federal Anayasa Mahkemesi'nin (Bundesverfassungsgericht) 2008 tarihli bir kararında bilgi teknoloji sistemlerine gizlice sızmanın ancak bir yargı kararı ile mümkün olacağına işaret edilmiş ve özel hayatın mutlak dokunulmaz olan çekirdek alanının korunmasının zorunluluğuna dikkat çekilmiştir[34]. Kararda, internet aracılığıyla gizli soruşturmanın anayasa aykırılığı ifade edilmemiştir; bunun yerine anayasada yer alan hakların korunması bakımından online aramanın ya da federal Truva atı kullanımının sınır ve kapsamının belirlenmesi gerekliliği üzerinde durmuştur. Benzer bir

---

30 Caianiello, s.276.

31 Caianiello, s.277.

32 Caianiello M., "Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase", Oxford Handbook Online Criminology, Oxford Press, Editors: D.K. Brown-J.I. Turner- B. Weisser, 2019, s.1-27.

33 Caianiello, s.277.

34 27.02.2008 T. BvR 370/07 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvro37oo7en.html

yaklaşım Adalet Divanı'nın İrlanda Dijital Haklar, *Seitlinger ve Diğerleri* davasında da sergilenmiştir[35]. Divan, ülkelerdeki yasal sistemlerin, AB Temel Haklar Şartı'nda yazılı ilkelere uygun olması şartıyla soruşturma işlemleri yapılırken telefondan veri toplama işlemlerinde kişisel veri koruma sınırlarının sıkı bir şekilde belirlenmesi gerektiğini ifade etmiştir.

Nordrhein-Westfalen eyaleti, Anayasanın Korunması Kanun'unda (Verfassungsschutzgesetz) 20 Aralık 2006 yılında değişiklik yapmak yoluyla online arama konusunda açık bir düzenleme getirmiştir. Söz konusu normatif düzenleme ile internet üzerinden gizli soruşturma yapılması mümkün kılınmıştır. Almanya'da 17 Ağustos 2017 tarihli Ceza Muhakemesinin Etkili ve Pratiğe Uygun Olarak Düzenlenmesi Hakkında Kanun ("Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens") ile çevrimiçi (online) araştırmalar, gizli soruşturma önlemi olarak hayata geçirilmiştir. Ancak halihazırda kovuşturma evresi için bir yetkilendirme söz konusu değildir. Sisteme gizlice yüklenen bir izleme yazılım programı olarak "*program kontrollü gizli araştırmacı*" aracılığı ile yapılan[36] online araştırmalar, Ceza Muhakemesi Kanunu'nda soruşturma evresinde temel haklara ciddi müdahale olarak kabul edilmektedir[37].

C. **İsviçre Örneği**

İsviçre'de soruşturma makamları, bilişim teknolojileri aracılığıyla suç faaliyetlerini ortaya çıkarmak adına çeşitli araçlar kullanmaktadırlar[38]. En sık kullanılan yöntem, doğrudan bilgisayar kasalarına el konulması suretiyle disklerde araştırma yapmaktır. Diğer bir seçenek ise, veri trafiğinde fark edilmeden gizlice telefon ya da bilgisayar bağlantılarının izlenmesidir. Çağın suçla mücadele gereksinimleri için dijital araştırma faaliyetlerinin yasal zemine oturtulması gerekmektedir. Nitekim İsviçre'de Telekomünikasyon Trafiğinin İzlenmesi Hakkında Federal Yasa (BÜPF)[39] ile gizli takibin yasal dayanağı oluşturulmuştur. Yakın bir zamanda, VoıP yazılımı olan Skype gibi

---

35 EU Court of Justice, 08.04.2014 T. C.No: C-293/12 and C-594/12

36 Michael Soine, "Die Strafprozessuale Online-Durchsuchung", Neue Zeitschrift für Strafrecht (NStZ) 2018, s.497; Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Massnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen JR 9, 2018, s.16.

37 Soine, s.497.

38 Platz, s.838.

39 Bundesgesetz vom 18 Marz 2016 betreffend die Überwachung des Post und Fernmeldeverkehrs (BÜPF)

telekomünikasyon hizmetlerindeki uçtan uca şifrelemenin kolluk ve savcılık makamı için kaldırılması talep edilmiştir[40]. Böylelikle klasik telekomünikasyon araçları dışında internet hizmet sağlayıcısı aracılığıyla sunulan hizmetler de online araştırmanın bir parçası haline getirilmek istenmektedir.

D. **Amerika Örneği**

Amerika Federal Yüksek Mahkemesi, Haklar Bildirgesi'nde yer alan ilkeleri, çağın gerekliliklerini dikkate alarak, dijital devrimin getirdiği zorluklara uyarlamıştır[41]. Mahkeme ilk kez *US v. Jones* Kararında[42] *GPS* takip cihazının takılması için Anayasa'nın IV. Değişikliğinin güvencelerini uygulama kararı almıştır. Sonrasında *Carpenter* kararında[43], hükümetin bireylerin verilerini toplamasına ilişkin geçmişe dönük olarak IV. Değişikliğin koruma alanını genişletmiştir[44].

Dijital çağdan önce ceza muhakemesinde delil araştırma faaliyetleri daha ziyade şüpheliyi takip etmekten ibaretti. Ancak dijital araçlardan yararlanmadan araştırma faaliyetlerini yürütmek, doğrudan şüpheliyi sürekli kolluk kuvvetleri aracılığı ile takip etmek hem oldukça masraflı ve hem de oldukça zordu. Bu sebeple, nadiren gerçekleştirilmekte ve toplumun bireyin uzun süreli takip edilmemesi gerektiği beklentisine de uygun davranılmaktaydı[45]. GPS bilgisinin uzun süreli kayıtları time stamp denilen şekilde, verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği bilgisi ile bunların gerçekleşme zamanlarını elektronik ortamda depolar. Mobil telefonun yerinin tespitinin yapılmasıyla telefon kullanıcısının ayak bileği monitörü takmış gibi gözetlendiği ve polisin başka türlü edinemediği tüm bilgilere erişimin bu yolla sağlandığı belirtilmiştir. Mahkeme, söz konusu uzun süreli kayıtlar yoluyla, vatandaşların ailevi, politik, dini bilgilerinin ele geçirileceğini ve bu kayıtların özel hayatın çekirdek kısmına zarar vereceğini

---

[40] Platz, s.840; Beranok Zanon, Reschtsfragen zu VoIP im Hochschulumfeld, SWITCH Journal, 2006, s.26.

[41] https://www.supremecourt.gov/search.aspx?Search=+Jones++565+U.S.+400+2012&type=Site (Erişim Tarihi:11.05.2020)

[42] Karar tarihi:23 Ocak 2012 https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf (Erişim Tarihi:20.12.2020).

[43] Karar tarihi: 22 Haziran 2018 https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (Erişim Tarihi:20.12.2020)

[44] Konum bilgilerinin edinilmesi, *Carpenter* şirketinin kablosuz ağ çalışmalarının bir ürünüdür.

[45] Carpenter v. United States, 585 US. (2018) https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/18-8666.html (Erişim Tarihi:11.05.2020).

ifade etmiştir. Benzer bir yaklaşım, cep telefonlarına uzaktan erişmek yoluyla fotoğraf, video kayıtlarından ya da yazışmalardan, hedef kişinin nerede olduğunu tespit ederek tutuklamaların yapılmasında yaşanmaktadır[46]. Söz konusu kararlar, geleneksel ceza muhakemesi ilkelerini ve usul kurallarını, bilimsel ve teknolojik gelişmelere adapte ederek başta adil yargılanma olmak üzere silahların eşitliği gibi ceza muhakemesinin esaslarını korumayı başarmıştır. Bu açıdan söz konusu kararlar, dijital çağ bakımından devrim niteliğinde kabul edilmektedir[47].

Avrupa Birliği'ne üye ülkelerde verilen kararlar, ABD Federal Mahkeme tarafından verilen kararlarla paralellik arz etmekte olup; dijital yargısal işlemler aracılığı ile delil elde edilirken, bireylerin mahremiyetinin ve hukukun üstünlüğünün korunması unutulmamalıdır. Savunma makamına, soruşturma makamları tarafından uygulanan dijital delil elde edilmesine yönelik müdahaleci soruşturma işlemleri ve koruma tedbirlerine ilişkin savunma yapmasına imkân tanınması oldukça önemlidir[48].

Adaletin gelecekteki gelişme potansiyeline bakarsak, dijital bir devrimin gerçekleşeceği beklenmektedir. Önümüzdeki yıllarda, önleyici ve geleneksel ceza adaleti arasındaki sınırların bulanıklaştırılmasıyla da yargı makamı yerine geçmek üzere yapay zekânın aşamalı kullanımının devreye gireceği kabul edilmektedir[49]. Nörobilim aracılığıyla ceza adaletinin yönetiminde yenilikçi bir yaklaşım izlenebileceğine inanılmaktadır. Örneğin şüpheli ya da sanığın tehlikelilik durumunu değerlendirmede yapay zekâdan yararlanabilecektir, benzer şekilde delilin niteliğinin ortaya konulmasında insan faktörü olmadan nörobilim aracılığıyla yargılama makamının iş yükü azaltılabilecektir. Konuya ilişkin olarak İtalya'da, deneme amacıyla tanık, mağdur ve sanığın güvenilirliğini test etmek için yapay zekânın deneme amaçlı kullanılabileceğinden söz edilmektedir[50]. 2011 yılında görülen bir davada, yargılamanın sonunda mağdurun ve sanığın güvenilirliğini test etmek

---

46 Riley v. California, 573, U.S. (2014) https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf (Erişim Tarihi: 11.05.2020).

47 Caianiello, s.280.

48 G.Malgieri /P.De Hert , "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges", The Cambridge Handbook of Surveillance Law (Editors: D.C. Gray-S. Henderson), New York 2017, s.509-523.

49 Caianiello, s.281.

50 Caianiello, s.281.

için nörobilimsel deneye katılmaları karara bağlanmıştır. Hem sanık hem de mağdur IAT, TARA testine tabi tutulmuştur. Yapay zekânın kullanıldığı IAT-TARA test sonucu doktorlar, mağdurun ifadesinin güvenilir olduğunu ve sanığın mahkûm edilmesi gerektiğini test sonuçları ile ortaya koymuştur[51].

E. **İngiltere Örneği**

İngiltere'de bir ceza muhakemesi kanunu bulunmamaktadır; muhakemeye ilişkin kurallar Police and Criminal Evidence Act[52] ile benzer bazı diğer kanunlar ve temyiz mahkemesinin içtihatlarından oluşmaktadır. Nitekim İngiltere'de de online aramanın temelini oluşturabilecek bir kanuni düzenleme olmadığı gibi, uzaktan erişim sağlayan yazılımların kolluk kuvvetlerince kullanılabileceğine ilişkin verilmiş içtihadi bir karar da bulunmamaktadır. Ancak kolluk kuvvetlerinin bir hâkim kararı olmaksızın bilişim suçları faillerinin bilgisayarlarına uzaktan erişim imkânı sağlayan İç İşleri Bakanlığı planının olduğu ifade edilmektedir[53].

III. Dijitalleşmede Olanaklar ve Sınırlar

Adli yazılım olarak işlev gören yapay zekanın uzaktan kullanılması için birtakım sınırlamalar söz konusudur. Her şeyden önce bunun için açık bir yasal düzenleme mevcut olmalıdır. Şüphelinin özel hayatının dokunulmazlığı, haberleşme özgürlüğü ile ilgili dijital işlem ile elde edilecek yarar arasında bir oran bulunmalıdır[54]. Uygulamada, soruşturma makamlarının -dijitalleşme aracılığıyla- sahip oldukları daha fazla verinin doğru bir şekilde kullanılması, iki ucu keskin bıçak üzerinde yürümeye benzetilmektedir. Bu noktada, kanunilik ilkesi ve orantılılık ilkesi dikkate alınarak düzenleme yapılmalıdır.

Kanunilik ilkesi mümkün olduğunca kapsamlı ve belirli bir değerlendirme yapılmasını gerektirirken; orantılılık ilkesi mümkün olduğunca ölçülü bir müdahale için düzenleme getirilmesini şart kılar. Federal Anayasa Mahkemesi, 2005 yılında verdiği bir kararda: "*veri taşıyıcılarını ve bunlarla ilgili verileri ararken, güvence altına alırken ve ele geçirirken, arama*

[51] 19.07.2011 T., Supreme Court of Cassation http://www.cortedicassazione.it/corte-di-cassazione/it/homepage.page;jsessionid=24B0D25B5E47D28E1E9683F04B746DD9.jvm1

[52] 1984 tarihli kanun metni için bkz. https://www.legislation.gov.uk/ukpga/1984/60/contents (Erişim Tarihi:18.04.2021).

[53] Değirmenci, s.232.

[54] Platz, s.841; Schneider, s.81.

kararına esas olayla bağlantısı olmayan bilgilere erişimden kaçınılmalıdır"[55] demiştir. Anayasa ile güvence altına alınmış hak ve özgürlüklerin korunması için soruşturma makamlarının sınırsız bir şekilde hareket serbestisine sahip olduğu düşünülmemelidir. Kanuni sınırlar dahilinde, ilgili temel hakkın sınırlandırılmasına yönelik koşullara uyularak gerekli araştırma ve soruşturma işlemleri yürütülmelidir.

Devletin uzaktan erişim ile örneğin şüphelinin bilgisayarında arama yapmasının bilgisayarda yer alan verilerin bütünlüğünü bozacağı ifade edilmektedir[56]. Soruşturma makamlarının, uzaktan erişim yoluyla kişisel verileri de ele geçirebileceği göz önüne alındığında, Kişisel Verilerin Korunması Kanunu'nun uygulama alanına da müdahale gündeme gelebilir. Big data çağında gizlilik oldukça önemli bir konudur. Üçüncü kişiler tarafından depolama alanlarında, bilgisayarlarda, akıllı cihazlarda saklanan kişisel verilere soruşturma makamlarının gelişi güzel ve sınırsız biçimde erişimi üzerine dikkatlice düşünülmelidir. Nitekim günlük yaşamda sıklıkla, mobil telefonlarla iletişimde olduğu gibi veri akış yoluyla iletişim kurulmaktadır. Özel servis sağlayıcıları tarafından depolanan pek çok kişisel veri mevcuttur. Örneğin akıllı ev sistemlerinde kişinin sesi, davranış modelleri, göz retinası kayıtlı olup, bu verilerin, soruşturma makamları tarafından tıpkı bir teknik araçlarla izleme koruma tedbirinde olduğu gibi bunların suçun aydınlatılması amacıyla toplanmak istenmesi, bu verilere erişimin yasallığı üzerine tartışmaları da gündeme getirmektedir[57]. Özellikle, özel veri depolayan kurumların soruşturma makamları ile iş birliğine girmesinin mümkün olduğu; bu durumun bireysel kullanıcılarla karşılaştırıldığında temel hak ve özgürlükleri daha fazla kısıtlayıcı bir korelasyon içinde olduğu ifade edilmektedir[58]. Nitekim Almanya'da, elkoyma işleminin konusunu oluşturan big dataların Alman CMK § 95 uyarınca bunları özel olarak depolayan şirketlerin eşyayı teslim etme mecburiyeti kapsamında soruşturma makamlarına verileceği belirtilmektedir. Söz konusu hükmü tamamlayıcı nitelikte olan bir diğer hüküm olarak Alman

---

[55] BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02.

[56] Kişinin bilgisayarının dokunulmazlığı, yetkili kişinin verilerini siber uzayda bozulmadan tutmasına ve yetkisiz erişimin olmamasına olanak tanır. J. Rehberg/ N. Schmid, Strafrecht III, 8. Aufl., Zürich 2003, s.150-151; P. Weissenberger, Basler Kommentar, Strafrecht II, 2. Aufl., Basel 2007, StGB 143, N.3.

[57] Ralf Peter Anders, "Die Privatsphäre im Zeitalter von Big Data Zum staatsanwaltschaftlichen Zugriff auf personenbezogene Daten in Speichern privater Dritter", ZİS 15. Vol., 2/2020, s.70-79, s. 70.

[58] Anders, s.70.

CMK § 161 (araştırmalar ve gizli soruşturmalardan elde edilen verilerin kullanılması) gösterilmektedir. Bu maddeye göre maddi gerçeğe ulaşmak için, Savcılık makamı tüm kamu kurumlarından bilgi isteyebilir ve her türlü araştırmayı kendisi yapabilir; polis böyle bir durumda savcılığın tüm emir ve isteklerini yerine getirmeye mecbur olup, tüm makamlardan bilgi istemeye yetkilidir. Bu hükümler çerçevesinde soruşturma makamlarının bu tür verileri edebilecekleri ve bunun yasal olduğu kabul edilmektedir.

Federal Anayasa Mahkemesi'nin kredi kartı verilerinin soruşturma makamları tarafından elde edilmesine yönelik verdiği karar bu noktada oldukça önemlidir[59]. Çocuk pornografisi içeriğine sahip web sitesine erişim için, 79,99 ABD dolarının kredi kartı ile ödenmesi zorunluluğu bulunmaktaydı. Savcılık makamı, bu web sitesinin müşterilerini tespit edebilmek amacıyla Almanya'daki Mastercard ve Visa şirketlerine Filipin'e para transferi yapan hesapların tamamını istemiştir. Her iki şirket de savcılığın talep ettiği bilgileri iletmişlerdir. Veri aktarımının süjesi haline gelen kredi kartı sahipleri anayasa şikayetinde bulunmuşlardır. Ancak Federal Anayasa Mahkemesi, burada bir ihlalin söz konusu olmadığına, savcılık makamının Alman CMK 161'inci maddedeki[60] yetkisini kullandığına, araç ile amaç arasında bir oran bulunduğuna; bu sebeplerle şikayetlerin kabul edilmez olduğuna karar vermiştir[61].

---

[59] BVerfGE NJW 2009, 1405-1408. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/02/rk20090217_2bvr137207.html (Erişim Tarihi:29.06.2020)

[60] Savcının Genel Soruşturma Yetkileri- 1) 160 (1) ila (3) maddelerinde belirtilen amaçlar doğrultusunda, savcılık, diğer kanuni hükümler hariç olmak üzere, tüm makamlardan bilgi istemeye ve her türlü soruşturmayı kendi başına yapmaya veya bunları polis teşkilatı yetkilileri ve memurlarına yaptırmaya yetkilidir. Polis teşkilatı yetkilileri ve görevlileri savcılığın talep veya emrine uymakla yükümlüdür ve bu durumda tüm mercilerden bilgi istemeye yetkilidir.

(2) Kişisel verilerin silinmesi bu Yasada açıkça emredildiği için, Federal Veri Koruma Yasası'nın 58 (3) Bölümü geçerli değildir.

(3) Bu Kanuna göre bir tedbire ancak bazı cezai suçlardan şüphelenilmesi halinde izin veriliyorsa, diğer kanunlara göre karşılık gelen bir tedbire dayanılarak elde edilen kişisel veriler, tedbirden etkilenen kişilerin rızası olmaksızın ancak ceza yargılamalarında delil amacıyla kullanılabilir, durumu açıklığa kavuşturmak için bu Kanuna göre böyle bir tedbirin emredilmesi gerekirdi. Bölüm 100e paragraf 6 numara 3 etkilenmeden kalır.

(4) Polis kanunu temelinde kapalı soruşturmalar sırasında kendini koruma amaçlı teknik araçların kullanımından apartman dairesinde veya apartman dairesinden elde edilen kişisel veriler, ancak orantılılık ilkesine (Temel Kanunun 13 (5) .Maddesi) uygun olarak delil amacıyla kullanılabilir. Düzenleyen makamın bulunduğu bölgedeki yerel mahkeme (Bölüm 162, Paragraf 1) tedbirin yasallığını tesis etmiştir; Yakın bir tehlike durumunda, yargı kararı derhal verilmelidir.

[61] Mahkeme, içtihatlar çerçevesinde fiziki varlığı olan eşyanın teslim edilmesine ilişkin

Özellikle örgütlü suçlulukla mücadele bakımından kamu yararının ön planda tutulması gerektiği, bu sebeple maddi gerçeğe ulaşmak amacıyla verilere yönelik bu tür müdahalelerin söz konusu olacağını söylemek gerekir. Benzer bakış açısı, şüphelinin özel hayatının korunması bakımından da geçerlidir. Uzaktan erişim ile bilgisayara entegre olan mikrofon ve kameranın izlenmesi, ilgilinin özel hayatının dokunulmazlığının ihlal edilmesine yol açacaktır. Bu itibarla ülkemizde, yapay zekâ olan adli yazılımları uzaktan kullanarak gizli erişimin sağlanması için muhakkak kanunilik ilkesine uygun olacak içerikte bir normatif düzenleme olması gerekir. Nitekim, karşılaştırmalı hukuk sistemlerine baktığımızda, gizli soruşturma işlemleri ve koruma tedbirleri için muhakkak özel bir yetkilendirmenin bulunduğu kanuni bir yetkilendirmenin olması gerektiği, özel hayatın dokunulmazlığına ancak bu şekilde riayet edileceği ifade edilmektedir[62].

Çevrimiçi (online) aramalara yoğun biçimde başvurulması, bilişim teknolojisi sistemlerini izleme veya araştırma olanaklarından yararlanılması, tedbirden etkilenen kişi sayısını artmasına yol açar. Bilgi teknolojilerine dayalı cihazlar, metin mesajı, görüntü ve ses dosyaları şeklinde hassas kişisel verileri içerir. Potansiyel olarak bu kadar kapsamlı verilere devlet organlarının erişim sağlaması, kaçınılmaz olarak toplanan verilerin, davranış profili ve iletişim profile oluşturmaya kadar varan risklere neden olur[63].

Alman ceza muhakemesi hukukunda, 24 Ağustos 2017'den itibaren Alman CMK §100b'de yapılan değişiklikle çevrimiçi aramalar için yasal bir dayanak oluşturulmuştur[64]. Alman CMK §100b I, kolluk kuvvetlerine, bilgi teknolojisi sisteminde teknik araçlara müdahale etme ve ondan veri toplama yetkisi verir. "*Bilgi Teknolojisi Sistemi*" terimi gelişmeye açıktır ve belirli işletim sistemlerini, giriş yollarını, programlamayı veya özel teknik özellikleri tanımlamadan gelecekteki cihaz ve program türleri de dahil olmak üzere

kuralların fiziki varlığı bulunmayan nesneler için de kullanılabileceğini ifade etmektedir. Ancak verilerin ayıklanmasına özellikle dikkat edilmesini, verilerin *tamamı* yerine, savcılığın ihtiyacı olan verilerin ayıklanarak bir kopyasının alınması gerektiğini ifade etmiştir. Kriterlerin belirlenmesinde ise Siber Suç Sözleşmesinin ilgili hükümleri dikkate alınmaktadır. (BVerfG NStZ-RR 2003, 176; BVerfG NJW 2009, 2431; Michael Greven: in Hannich Rolf , Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 94, no.4).

62 Anders, s.71.

63 BVerfGE 120, 274 no. 232; 141, 220 no. 238.

64 Art. 3 des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017

hepsini kapsar[65].

Çevrimiçi (online) arama, Alman CMK § 110 (3)'e göre[66] klasik bilgisayarlarda arama ve kaynak iletişimin denetlenmesi olarak ikiye ayrılır. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesinde, çevrimiçi (online) arama ile teknik olarak benzer özellikler taşısa da cihazın daha kapsamlı bir şekilde araştırılmasına izin veren çevrimiçi aramanın aksine, soruşturma organlarının erişim yetkisi esas itibariyle sadece iletişim ile sınırlıdır[67]. Telekomünikasyon araçlarında, iletişim verileri şifrelenmeden önce veya şifresi çözüldükten sonra kaydedilebilir[68]. Nitekim iletişim sürecinde kaydedilemeyen hiçbir veri kullanılamaz (Alman CMK §100a (5)1 no. 1b). Çevrimiçi aramada ise, bir bilgisayar sisteminde daha kapsamlı ve özel bir araştırma söz konusu olup, bu yolla sadece iletişim verileri değil, sohbetler, yüklenen fotoğraflar, yazılı notlar ve web sitesi geçmişleri gibi tüm depolanmış veriler görüntülenebilir. Böylece izlenen kişinin çevrimiçi davranışlarının kapsamlı bir profili ortaya çıkarılabilir[69]. Hükümdeki, "*ilgili kişinin bilgisi olmadan bile*" ifadesi, çevrimiçi aramanın prensipte gizlice gerçekleştiğini açıkça ortaya koymaktadır. Bununla birlikte, izlenen kişinin bunu öğrenmesi, elde edilmiş olan delillerin geçerliliğini etkilemez[70]. Şüphelinin hakkında çevrimiçi arama yapıldığını öğrenmesi ve rıza göstermesi, bundan etkilenebilecek diğer kişilerin temel haklarına müdahale yetkisi olarak değerlendirilemeyeceği gibi; mahkeme kararı, şüphelinin tedbir hakkında bilgi sahibi olması ve rıza göstermesi halinde de bir zorunluluktur[71].

İsviçre ceza muhakemesi hukukunda dijitalleşmenin sınırlarıyla ilgili tartışmalardan birisi de, yapay zeka olan adli yazılımın teknik cihaz olarak değerlendirilip değerlendirilemeyeceğidir[72]. Teknik cihaz olarak

---

65 Jürgen-Peter Graf, BeckOK StPO, 28. Edition, § 100 b no. 7.

66 BGH, Beschluss vom 31. Januar 2007 - StB 18/06

67 Bernd Heinrich / Tobias Reinbacher, Online Durchsuchung, Oktober 2019.

68 https://www.jura.uni-wuerzburg.de/fileadmin/02150030/Strafprozessrecht/18a-quellentkue.pdf (Erişim Tarihi:18.05.2020).

69 https://www.lto.de/recht/hintergruende/h/bmjv-bmi-entwurf-ueberwachung-bfv-bnd-staatstrojaner -online-durchsuchung/ (Erişim Tarihi:18.05.2020).

70 Eschelbach , SSW-StPO, 3. Auflage, 2018, § 100 b no.1.

71 Sonie, s.498.

72 İsviçre'de 01.03.2018 yılında yürürlüğe giren Posta ve Telekomünikasyon Trafiğinin İzlenmesine Dair Federal Kanun (BÜPF) ve kanunun uygulanma alanını gösteren Yönetmelik (VÜPF) hükümleri uyarınca uzaktan erişim yoluyla iletişim takip edilebilmektedir.

değerlendirilirse telekomünikasyon yoluyla iletişimin denetlenmesi çerçevesinde soruşturma makamlarının gerekli çevrimiçi araştırma işlemlerini yapabileceği kabul edilmektedir[73]. Aksi takdirde kanuni bir dayanak bulunmadığından yapılan araştırmalar neticesi elde edilen deliller hukuka aykırı sayılacaktır. Bu bağlamda önemli sorunlardan biri de şudur: Şayet adli yazılım bir cihaz olarak takip amacıyla kullanılacaksa, özel hayatın dokunulmazlığı korumasında olan verileri hâkim dosyada nasıl değerlendirecektir? Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinde, iletişimin ve şüphelinin sistem üzerinden fiziksel takibi söz konusudur. Ancak uzaktan adli yazılım ile kişinin kamerasına erişilmekte, mikrofonu kontrol altına alınabilmekte ve anlık mesajlaşma içerikleri izlenebilmekte ve veri taşıyıcısına aktarılabilmektedir. Bu bakımdan adli yazılımın uzaktan kullanılmasının, gizli koruma tedbirlerinden olan telekomünikasyon yoluyla iletişimin denetlenmesi ile bir tutulması mümkün değildir.

IV. Dijitalleşmenin Soruşturma Sürecine Etkileri

Zamanın gerektirdiği hızlı teknik gelişmeler dikkate alındığında, ceza hukukunun söz konusu teknik gelişmelere ayak uydurup uyduramadığı incelenmelidir. Teknik ilerlemenin doğurduğu bilgisayar dolandırıcılığı ve veri hırsızlığı gibi suçlar[74] ile beyaz yaka suçları ceza muhakemesi hukukunu ister istemez dijitalleşmek zorunluluğu ile karşı karşıya bırakmaktadır[75].

Sanal ortamda işlenen suçlarda, faili tespit etmek ve onu cezalandırmak oldukça zordur. Örneğin DDos saldırılarında ya da Shitstormslarda mağdurun saldırıya uğradığından haberi bile olmayabilmektedir[76]. Kullanıcı olan mağdurlar çoğunlukla internet aracılığıyla ya da internette işlenen suçların azaldığı varsayımıyla hareket etmektedirler. Karşılaştırmalı hukuka bakıldığında, sanal ortamda işlenen suçlarla ilgili olarak daha çok fail odaklı bir yaklaşım sergilendiği görülmektedir[77]. Sanal ortamda failin davranışlarının izlenmesi için özellikle kolluk makamlarının dijital yolla içeriklere erişim

[73] Platz, s.843.

[74] Wolfgang Joecks / Klaus Miebach, Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 3. Aufl. 2019, §263a, no.11.

[75] Frederic Schneider, "Auswirkungen der Digitalisierung auf das Ermittlungsverfahren, Impulse aus der Strafverteidigungspraxis", Zeitschrift für Internationale Strafrechtsdogmatik, 2020/2, s.79.

[76] Beck, s.44.

[77] Beck, s.44.

olanağına sahip olması gerekmektedir. Dolayısıyla soruşturma makamlarının delil elde etmesi amacıyla gerekli dijital olanaklara sahip olması artık bir zaruret teşkil etmektedir.

Ceza muhakemesinde hızla dijitalleşen çağın gereksinimlerine yanıt vermek ve uygulamada karşılaşılan somut olaylara çözüm bulmak amacıyla birtakım değişiklikler yapılması zorunludur[78]. Teknik gelişime uyum sağlamayan ve nihayetinde maddi ceza hukuku ile ceza muhakemesi hukukunda gerekli değişimi yakalayamayan ülkeler yakın gelecekte önemli sorunlar yaşayacaktır. Bu nedenle, muhakemenin yaşam gerçekliğine sürekli uyarlanması artık bir gereksinim teşkil etmektedir.

Dijitalleşmenin soruşturmaya etkisini belirlemeye çalışırken soruşturmaya hâkim olan ilkeler göz ardı edilmemelidir. Öncelikle getirilen düzenlemenin mutlaka kanunilik ilkesine uygun olması gerekmektedir. Nitekim bu konuda kanuni düzenlemeye sahip Alman Ceza Muhakemesi Kanunu'nun ilgili maddesinin, kanunilik ilkesine uygun olarak düzenlendiği, bu itibarla temel hakların çekirdek alanına dokunulmadığı, özenli bir düzenleme getirildiği ifade edilmektedir[79]. CMK'da getirilmesi önerilen düzenlemenin de benzer şekilde, korunmak istenen temel hak ve özgürlükler ile orantılı, açık, belirli, muğlak ifadelere yer verilmeden, soruşturma makamlarına verilecek yetkinin sınırlarının ve kapsamının belirlendiği bir içeriğe sahip olması gerekmektedir.

Dijitalleşme ile karanlık bir alanın aydınlatılması, daha kısa sürede adli sonuçlar elde edilmesi gibi önemli hizmetlerde bulunulmaktadır. Bu nedenle ceza hukukunun işlevselliğini arttırmak adına dijitalleşmenin hızla hayata geçirilmesi gerekir. Daha fazla veri, sadece niteliksel olarak değil, aynı zamanda niceliksel olarak da "daha fazla gerçek" anlamına gelir[80].

Ceza muhakemesi, basit şüphe dediğimiz bir şüphe derecesi ile başlar ve savcılık makamının yaptığı araştırmalar neticesinde basit şüphenin yeterli şüphe derecesine ulaşması ile soruşturma evresi nihayete erer. Bir fiilin cezalandırılabilmesi için fail tarafından işlendiğini gösteren somut göstergeler olmalıdır. Dijital gelişimin bir sonucu olarak giderek daha fazla verinin var olması ve bu verilerin teknik gelişme açısından daha hızlı bir şekilde analiz

78 Schneider, s. 80.

79 Schneider, s.79; Knauer/ Kudlich/ Schneider, Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 152, no.1.

80 Schneider, s.80.

edilmesi, başlangıç şüphesinin giderek daha yoğun bir şüphe derecesine dönüşmesine yol açmaktadır.

Yargının dijitalleşmesi ile daha fazla veri daha hızlı elde edilerek daha süratli analiz edilebilir. Uygulamada, dijital alanda ortaya çıkan bu gelişmenin, soruşturmanın yürüyüşü üzerinde klasik soruşturma usullerine kıyasla iki kat etkisi bulunmaktadır. Böylelikle, başlangıç şüphesinden yeterli şüphe derecesine daha hızlı varılabilmektedir. Özellikle ticari ceza ve beyaz yaka suçları bakımından soruşturmanın dijitalleşmesinin, verilerin kaybolmadan hızlıca elde edilmesini sağladığı ve soruşturmanın tamamlanıp kovuşturma evresine süratle geçişin anahtarı olduğu ifade edilmektedir[81]. Özünde, dijitalleştirilmiş ya da sayısallaştırılmış ceza soruşturmalarının amacı, eylem ve fail ile ilgili soruşturmanın öznel düşüncelerden bağışık olarak maddi gerçeğe daha güvenilir biçimde ulaşmak için en nesnelleştirilmiş şekilde delilleri toplamaktır[82].

Önemli suçlar açısından elde edilen deneyimler, soruşturma makamları için bilgisayar sistemlerinin aranması ve elde edilen verilerin değerlendirilmesi olanağının daha yaygın kullanımını haklı çıkardığını göstermiştir. Dolayısıyla artan dijitalleşme, ceza muhakemesi kanunlarında yeni, kısıtlayıcı ve soruşturma makamlarına özgü yetki veren düzenlemelere duyulan ihtiyacı ortaya çıkarmıştır[83].

Alman kanun koyucu, arama yerlerinin veya sanal ortamda işlenen suçlar dışında saklanan verilerin sisteme işlenmesi için Ceza Muhakemesi Kanunu § 110 (3)'e karşılık gelen verilere erişim ile ilgili olarak defalarca düzenlemeler yapmış olsa da yurtdışında bulunan veriler için kanunda özel bir düzenleme bulunmamaktadır. Bununla birlikte, özellikle, dijitalleşmeden kaynaklanan "*daha fazla teknoloji ve daha fazla veri*" durumu ile nasıl başa çıkılacağı henüz kesin olarak açıklığa kavuşturulmamıştır. Dünyanın önde gelen internet operatörlerinden De-Cix'in, Almanya Federal İstihbarat Teşkilatının (BND) veri akışını kullanmasına karşı, 2017 yılında yürürlüğe giren ve yurtdışındaki yabancıların iletişim bilgilerinin izlenmesini düzenleyen BND yasasının anayasaya aykırı olduğu gerekçesiyle açtığı dava, Leipzig'de Federal İdare Mahkemesince reddedildi. Mahkeme, İçişleri Bakanlığının, BND'nin stratejik iletişimi izlemeye yardımcı olması amacıyla internet şebekelerine

81 Schneider, s.80.

82 Schneider, s.79.

83 Schneider, s.81.

ihtiyaç duyulabileceği kararını vermiştir[84]. İşte bu ve benzeri durumlarda açık bir yetkinin tanınmış olması ve yetkinin sınırlarının kanun koyucu tarafından belirlenmiş olması gerekmektedir.

V. Bir Dijitalleşme Örneği Olarak Online (Çevrimiçi) Duruşma

Ceza muhakemesinin bir diğer önemli evresi olan kovuşturma evresinde de dijitalleşmenin devamlılığını görmek gerekir. Yukarıda da ifade ettiğimiz gibi özellikle tüm Dünya ülkelerinin etkilendiği COVID-19 pandemi sürecinde hem toplum sağlığını korumak hem de yargının aksamadan ilerlemesini temin edebilmek adına online (çevrimiçi) duruşmaların hayata geçirilmesi büyük önem taşımaktadır.

HSK tarafından Mart ayından itibaren sıklıkla COVID-19 kapsamında tedbir alınmış ve alınan tedbirlerin süresinin uzatılmasına karar verilmiştir. HSK'nın verdiği kararlarda özellikle cezai işlerle ilgili suçlulukla mücadele kapsamında iş ve işlemlerin devam etmesi gerektiği ve rutin faaliyetlerin gecikmeksizin yerine getirilmesi kararı verilmiştir. Nitekim geciken adalet, adalet değildir. AİHS'nin 6'ıncı maddesi uyarınca adil bir yargılama tesis edebilmek için makul sürede yargılamaların bitirilmesi gerekmektedir.

Bu süreçte, acil ve tutuklu işler ile yürütmenin durdurulması istemlerinin yerine getirilmesi için yeteri kadar Cumhuriyet Savcısı ve hâkimin görevlendirilmesine, geri kalan hâkim ve savcının UYAP imkanlarından yararlanarak uzaktan çalışmalarının temin edilmesi sağlanmıştır. İşte tam olarak suç ve suçlulukla mücadelenin aksamaksızın sürdürülebilmesi bakımından müdafi ve vekilin online olarak duruşmalara katılmasının mümkün kılınması da büyük önem arz etmektedir. Böylelikle yargılamalar da aksamamış olacaktır.

26.03.2020 tarihinde yürürlüğe giren 7226 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un geçici 1'inci maddesi, durma süresince, ilk derece adli ve idari yargı mercileri ile bölge adliye ve bölge idare mahkemeleri bakımından duruşmaların ve müzakerelerin ertelenmesi de dahil olmak üzere alınması gereken diğer tüm tedbirler ile buna ilişkin usul ve esasların belirlenmesinde HSK'yı, Yargıtay ve Danıştay'daki işler bakımından ise Başkanlar Kurulu'nu yetkili kılmıştır. HSK, ilgili kanunun verdiği yetkiye dayanarak 30.03.2020 tarihinde aldığı kararları tüm teşkilata

[84] https://tr.sputniknews.com/avrupa/201806011033679849-bnd-internet-sebeke-almanya/ (Erişim Tarihi:08.07.2020)

duyurmuştur. CMK'ya göre tutukluluk değerlendirmesinin zorunlu olduğu durumlarda, tutuklu ve müdafinin SEGBİS uygulaması üzerinden dinlenilerek duruşmaların icrasına karar verilmiştir. Hukuk hakimlerinin bir kısmının da ceza mahkemesi hâkimi olarak nöbet listelerine yazılmasına karar verilmiştir.

Ancak pandemi karantinasının bitimi olan 1 Haziran 2020 itibariyle "yeni normalleşme" kapsamında çalışmalar başlatılmış ve duruşmalar kaldığı yerden devam etmiştir. Bu noktada pandeminin yayılma riski halihazırda devam etmekte ve duruşmaların online yapılmasının artık mümkün kılınması gerekmektedir. Nitekim pandeminin öngörülebilir olmayan bir süre daha devamı beklenmektedir. İşte bu noktada CMK'daki duruşma evresine ilişkin düzenlemelerin dijitalize edilmesine yönelik alternatiflerin geliştirilmesi gerekmektedir. Örneğin bu amaçla, 20 Eylül 2011 yılında yürürlüğe giren SEGBİS Yönetmeliği'nde değişiklik yapılması önemli bir adım olacaktır. Yönetmeliğin 12 ila 17'inci maddeleri arasında usul hükümlerine yer verilmiştir. Buna göre, soruşturma ya da kovuşturma evresinde talep eden makamın uygun bulması ile pek çok alternatif durumda SEGBİS ile uzaktan erişim ya da katılım mümkündür. Yönetmeliğin 21'inci maddesi uyarınca SEGBİS, CMK'nın uygulandığı durumlarda kullanılabilir ifadesine yer vererek, kıyasen hâkim ya da mahkemenin uygun bulduğu durumlarda kullanılabilmesinin önünü açmaktadır. Usul hükümlerine ekleme yapmak yada var olan hükümde değişiklik yapak suretiyle, özellikle duruşma evresine ilişkin bir düzenleme yapılması isabetli olacaktır.

Duruşmaların dijital ortamlarla yapılmasının sağlanması için ülkemizde adımlar atılmış olup pilot bölgelerde uygulamalar başlatılmıştır. Teknolojinin gelişmesi ve hayatımızın her alanına adapte olması ile Adalet Bakanlığı, "*Yargı Reformu Stratejisi*"[85] metninin "*Performans ve Verimliliğin Arttırılması*" başlıklı 4'üncü maddesinin "*Yargıda bilişim sistemleri geliştirilecektir*." hedefi doğrultusunda avukatların duruşmalara video konferans yöntemiyle katılmalarına imkân sağlayacak olan *e-duruşma* sisteminin pilot uygulama ile başlayacağını açıklamıştır. 15 Eylül 2020 tarihi itibariyle Ankara Batı Adliyesi 1. ve 2. Tüketici Mahkemesi ile 1. ve 2. İcra Hukuk Mahkemesi'nde e-duruşma pilot uygulaması başlamış olup bu uygulama ile bilişim sistemlerinin günümüz teknolojilerinin imkânları doğrultusunda kullanıcı dostu yöntemlerle hukuk sistemimize adapte edilmesi yönünde ilerlenmesi amaçlanmaktadır. Esasen duruşma salonlarında uzaktan teknoloji aracılığıyla katılımın varlığı, 20

[85] https://sgb.adalet.gov.tr/Resimler/SayfaDokuman/23122019162931YRS_TR.pdf (Erişim Tarihi: 18.10.2020).

Eylül 2011 tarih ve 28060 sayılı Resmî Gazete'de yayımlanan "*Ceza Muhakemesi'nde Ses ve Görüntülü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik*" (SEGBİS) ile başlamış ve şüpheli ya da sanığın sesli ve görüntülü iletişim kanalıyla yargılama sürecine katılmasıyla kendini göstermiştir[86]. Ancak müdafinin yargılama sürecine dijital kanallar yoluyla katılabileceği e-duruşma uygulaması bu yönüyle bir ilk olmaktadır. 4 Aralık'ta yapılan duyuruya göre, e-duruşma sistemi yaygınlaştırılmaya çalışılarak, 07.12.2020 tarihinden itibaren İzmir, Bursa, Aydın, Adana, Antalya, Balıkesir, Denizli, Diyarbakır, Erzurum, Eskişehir, Gaziantep, Hatay, Kahramanmaraş, Kayseri, Kocaeli, Konya, Malatya, Manisa, Mardin, Mersin, Muğla, Ordu, Sakarya, Samsun, Şanlıurfa, Tekirdağ, Trabzon ve Van Adliyelerinde Tüketici, İcra Hukuk ve Kadastro Mahkemelerinde e-duruşma sistemi kullanıma açılmıştır.

Bu bağlamda, online duruşmalarda müdafinin savunma makamı olarak üzerine düşen yükümlülük ve sahip olduğu yetkiler bakımından katılımın detaylarına ilişkin bir belirleme yapılmasına ihtiyaç bulunmaktadır. SEGBİS'in doğrudan doğruyalık ilkesini ihlal edip etmediğine ilişkin yapılan değerlendirmeler burada da gözden geçirilmelidir. Bu noktada, dikkat edilmesi gereken hususların ne olduğunun belirlenmesinde AİHM'nin *Marcello-İtalya* Kararı ile[87] Yargıtay 16. CD'nin 19.06.2015 tarih ve 2015/1076-1932 sayılı kararındaki[88] kriterler gözden uzak tutulmamalıdır. Genel kural, sanığın duruşmada hazır bulundurulması olmakla beraber, bu yükümlülük, ancak somut ciddi nedenlere dayalı olarak mahkeme kararı ile sınırlandırılabilir. Bahsi geçen kararlara göre, savunmanın yapıldığı, esasa ilişkin delillerin toplandığı oturumlara, sanığın SEGBİS yolu ile katılması açık kabulüne dayalı olmalıdır. Teknik bağlantının iyi olması ve talebi doğrultusunda sanığın yanında halihazırda müdafi bulunması olanağının sağlanması, soru sorma imkanının sağlanması, duruşmanın tamamında katılım koşulları

[86] Alman CMK (StPO) m.247a'da tanığın korunması maksadıyla video konferans yoluyla duruşmaya katılım düzenlenmiştir. Duruşma salonunda sesli görüntülü video konferans yönteminin kullanılması birtakım koşullara bağlanmıştır: Örneğin tanık ya da şüphelinin belirsiz bir süre mahkemenin bulunduğu yere getirilmelerinin mümkün olmaması ya da tanığın uzaklık sebebiyle duruşma salonunda bulunmasının onlardan beklenemeyecek olması gerekmektedir.

[87] AİHM Üçüncü Dairesi'nin 05.10.2006 Tarih ve 2004/45106 sayılı kararı. https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22marcello%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-77246%22]} (Erişim Tarihi:04.12.2020).

[88] Benzer yönde bkz. Yar. 16. CD, 19.06.2015 T., 2015/1078-1930; Yar. 16. CD, 19.06.2015 T., 2015/1083-1926.

gerçekleştiğinde, savunma hakkının kısıtlanmadığı kabul edilebilecektir.

Yargı reformu stratejisi kapsamında e-Duruşma uygulaması nasıl işleyecek sorusuna verilecek yanıtlar ise şöyle sıralanabilmektedir: e-Duruşma uygulamasının mevcut olduğu mahkemedeki duruşmaya e-duruşma yoluyla katılım sağlamak isteyen avukat, UYAP Avukat Portal üzerinden, ilgili duruşmadan 24 saat öncesine kadar uzaktan erişim ile duruşmaya katılma isteğinin gerekçeleriyle birlikte talepte bulunacaktır. Duruşmaya 24 saatten az bir süre kaldığında sunulan talepleri ise sistem kendiliğinden reddedecektir. Avukat tarafından gönderilen e-duruşma talebi, dosyaya bakmakla görevli hâkim tarafından değerlendirilecek ve hâkim tarafından talebin kabul edilmesi halinde avukat, UYAP Avukat Portal uygulaması üzerinden duruşmaya video konferans yoluyla katılım gösterebilecektir. Duruşmadan önce e-imza veya mobil imza ile kimlik doğrulaması yapılacak, avukatın bilgileri ve fotoğrafı Hâkim tarafından UYAP sistemi üzerinden teyit edildikten sonra duruşma başlayabilecektir. Duruşma başladığında UYAP Avukat Portal/ Celse uygulaması üzerinde "duruşmaya katıl" butonu aktif hale gelecek ve bu yöntemle duruşmaya dahil olunacaktır. 1136 sayılı Avukatlık Kanunu madde 49'da düzenlenen avukatların duruşmalara cübbe ile katılma zorunluluğuna e-duruşma uygulaması bir istisna getirmediğinden, video konferans yoluyla yapılan e-duruşmalara da cübbe ile katılım sağlanacaktır. Duruşmanın kesintisiz olarak devam etmesi için en az 8Mbit internet bağlantısı hızı olması ve internet bağlantısının kafe, restoran vb. ortak kullanıma açık bir bağlantı olmaması gerekmektedir. Duruşma sırasındaki görüntü ve ses aktarımının kalitesi kullanıcının sorumluluğunda olacaktır[89].

Online duruşma uygulamasının, pandemi sürecinde adliyelerde ve duruşma salonlarında kalabalıkların oluşmasının önlemesi, avukatların aynı güne verilen farklı şehirlerde birden fazla duruşmasının olması durumunda hepsine katılım sağlayabilecek olması, makul sürede yargılamanın bitirilebilecek olması gibi pek çok olumlu yönü bulunmaktadır. Ancak Bakanlık tarafından açıklandığı üzere, ortak kullanıma açık ağlardan erişimin sağlanması gibi bir durumda, güvenlik ve gizlilik ihlal edilmeye açık hale gelebilecektir.

İtalya'da uygulanan *Italian Trial Online* (TOL) ve Kanada'da uygulanan CIMS online duruşma örneklerine bakacak olursak; TOL örneğinde duruşma,

[89] https://bigm.adalet.gov.tr/Home/SayfaDetay/e-durusma-sistemi17062020040538 (Erişim Tarihi:04.12.2020).

duruşma salonu dışından katılan kişilerin de erişimine açıldığından kullanıcı kitlesinin genişliği sebebiyle sistemin dışarıdan satın alınması, dosya güvenliğinin sağlanamaması gibi aksaklıklarla karşılaşılmıştır[90]. Bu bağlamda, ülkemizde pilot uygulama olarak uygulanmaya başlayan *e-duruşma* şimdilik avukatlarla sınırlı bir şekilde başlamış olması itibariyle teknik aksaklığın daha az yaşanacağı umudunu barındırmaktadır. Ancak teknik alt yapının iyileştirilmesi böylelikle, avukatların duruşmalara katılma esnasında teknik problemlerle karşı karşıya kalmasının önüne geçmek gerekecektir.

Bu noktada, karşılaştırmalı hukuktaki online duruşma ya da online mahkeme uygulamalarına bakmak yol gösterici olacaktır. Online mahkemelerin ya da online duruşmaların, sınırlı ya da sıfır hukukî bilgiye sahip, yetersiz kaynaklar sebebiyle avukat yardımına erişemeyen taraflar için önemli bir çıkış noktası olacağı ifade edilmekle beraber, ilgililere yardımı olması amacıyla, dünyadaki online duruşma uygulamaları sıklıkla sadeleştirilmiş ve basitleştirilmiş ara yüz kullanmayı tercih etmektedirler[91]. Online duruşma uygulamaları, dijital ortamlarının yargının tarafsızlığı ve bağımsızlığı ile adil yargılanma hakkı gibi temel değerlerle çelişmemek adına, kendi kendisini temsil eden tarafın özerkliğini, dolayısıyla kendi kaderini tayin etme hakkını korumayı garanti etmektedir[92]. Dolayısı ile ceza muhakemesi hukukunda kovuşturma evresine hakim olan ilkelerin online duruşmalar için de korunması hedeflenmekte ve gerekmektedir.

Online duruşma/mahkeme uygulamaları için yapılan araştırmalar, dijital ara yüzlerin pek çok fonksiyonunu ön plana çıkarmıştır. İnsan-bilgisayar etkileşimini algılayan ve takip eden yapay zekâ kullanımı ile daha doğru bir ara yüz yaratma çalışmaları son on yıllık süreçte tüm hızıyla devam etmektedir[93]. Örneğin İngiltere ve Galler'de 1.2 milyon sterlin bütçe ayrılarak, online duruşmaların ortaya çıkardığı sorunlara çözüm bulmak ve işleyişi

---

90 Giampiero Lupo / Jane Bailey, "Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples*",* Laws (MDPI), Vol 3, Issue: 2, 2014, s. 353-387, s.386.

91 Sela Ayelet, "E-Nudging Justice: The Role of Digital Choice Architecture in Online Courts", Journal of Dispute Resolution, Vol. 2019, Issue 2, 2019, s.127-164, s.128.

92 Ayelet, s.129.

93 Ayelet, s.129; Anthony Jameson / Bettina Beredent/ Silvia Gabrielli / Federica Cena / Cristina Gena / Fabiana Vernero / Katharina Reinecke, Choice Architecture for Human-Computer Interaction, 7:1-2, Now- 2014, s.14-15.

kolaylaştırılmak için çalışıldığı bilinmektedir[94]. Teknolojinin kullanılması ile yargılama maliyetleri azaltılabilecek, prosedürler daha şeffaf ve kolaylıkla takibi mümkün olacaktır. Daha erişilebilir ve verimli bir yargılama süreci söz konusu olabilecektir[95]. Ancak yine de yargılama süreçlerinde tarafların haklarını ve önemli usul ilkelerini ihlal etme endişesi vardır. Özellikle savunma makamının etkinliği adına, müdafi ile sanığın online duruşmaya kesintisiz, tüm aşamalara hâkim olacak şekilde katılımının sağlanması, başkalarının duyamayacağı ortamda görüşmelerinin sağlanması ve etkin bir savunmanın önüne engel çıkarılmaması gerekmektedir.

Online duruşmalar bakımından bir diğer tehlike, siber uzayda sıklıkla karşılaşılan sistemin hacklenmesidir[96]. Bu itibarla bilgi güvenliğinin sağlanması bakımından kimlik doğrulaması sistemlerinin etkin bir şekilde e-duruşma platformunda kullanılması gerekmektedir.

SONUÇ

Bilgi teknolojileri sistemlerinin çoğu, insan hayatında önemli bir rol oynamaktadır. Bilgisayarlar, laptoplar, tabletler, akıllı telefonlar soruşturma makamları için oldukça kıymetli veri kaynaklarıdır. Bilişim teknolojileri cihazları, özellikle örgütlü suçlarda kriptolojik prosedürlerle tekrar tekrar kullanılmaktadır. Bu itibarla geleneksel soruşturma yöntemleri çağımızda ve ilerleyen zaman diliminde çoğunlukla başarısız olacaktır.

Toplumun artan dijitalleşmesinin doğal olarak ceza muhakemesi hukuku bakımından da durmadığı unutulmamalıdır. Soruşturma prosedürü kapsamındaki gerçek değişiklikler göz önüne alındığında ortaya çıkan sorular özellikle temel haklarla ilgilidir. Dijital soruşturma prosedürünün temel haklarla uyumlu tasarımı oldukça önemlidir. Bu itibarla gerek kanunilik gerekse ölçülülük ilkeleri ön plana alınmak suretiyle bir yol haritası çıkarılması gerekir.

Dijitalleşmenin ceza muhakemesi hukukundaki esaslı iki evre olan hem soruşturmayı hem de kovuşturmayı kapsaması gerekliliği de gözden uzak tutulmamalıdır. Bu açıdan, kanun koyucu tarafından getirilmesi önerilen dijitalizasyonu sağlamaya yönelik düzenlemeler bütüncül bir yaklaşıma

---

[94] Ayelet, s.130.

[95] Bu noktada, çevrimiçi iletişim süreçlerinin teknik manada kusursuza yakın işlemesi gerekliliği hususunda fikir birliği bulunmaktadır. (Ayelet, s.132).

[96] Ayelet, s.132.

sahip olmalıdır. Özellikle kovuşturma evresinin özü olarak kabul edilen duruşma devresinde, vasıtasızlık ilkesinin gereklilikleri dikkate alınarak, alt yapı yetersizliklerinin ya da eksikliklerinin süratle tamamlanarak, yargılama makamı, savunma makamı ve katılan taraf arasındaki dijital etkileşim kusursuz bir işleyişe kavuşturulmalıdır.

KAYNAKÇA

Anders R. P, "Die Privatsphäre im Zeitalter von Big Data Zum staatsanwaltschaftlichen Zugriff auf personenbezogene Daten in Speichern privater Dritter", ZİS 15. Vol., 2/2020, s.70-79.

Ayelet S, "E-Nudging Justice: The Role of Digital Choice Architecture in Online Courts", Journal of Dispute Resolution, Vol. 2019, Issue 2, 2019, s.127-164.

Beck S, "Die Diffusion strafrechtlicher Verantwortlichkeit durch Digitalisierung und Lernende Systeme", 15. Vol., 2/2020, s.41-51.

Brandli B, "III. Kommunikation im Recht/Einsatz von Informations und Kommunikationstechnologie im schweizerischen Zivilprozess", Kommunikation in Wirtschaft, Recht und Gesellschaft, Stampfli Verlag, 2010, s.239-260.

Caianiello M, "Criminal Process faced with the Challenges of Scientific and Technological Development", European Journal of Crime, Criminal Law and Criminal Justice, 27, 2019, s.267-291.

Caianiello M, "Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase", Oxford Handbook Online Criminology, Oxford Press, Editors: D.K. Brown-J.I. Turner- B. Weisser, 2019, s.1-27.

Cornelius K, "Künstliche Intelligenz", Compliance und sanktionsrechtliche Verantwortlichkeit, Zeitschrift für Internationale Strafrechtsdogmatik", 15. Vol. 2/2020, s.51-65.

Davidson A, "Jurisdiction in Cyberspace*",* Social Media and Electronic Commerce Law, 2nd Edition, Publisher: Cambridge University Press, August 2018, s.327-349.

Değirmenci O, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin, Ankara 2014.

Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Massnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen JR 2018.

Graf J-P, BeckOK StPO, 28. Edition.

Greven M: in Hannich Rolf, Karlsrucher Kommentar zur Strafprozessordnung, 8. Aufl. 2019.

Heinrich B/Reinbacher T, Online Durchsuchung, Oktober 2019.

Kees H, "State Trojans:Germany Exports 'Spyware with a Badge'", Statewatch, Vol.21, No:4, 2012.

Hürlimann D, Publikation von Urtelien durch Gerichte, in: sui-generis, 2014.

Jameson A/ Beredent B/ Gabrielli S/ Cena F/ Gena C/ Vernero F/ Reinecke K, Choice Architecture for Human-Computer Interaction, 7:1-2, Now, 2014.

Joecks W/Miebach K, Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 3. Aufl. 2019.

Knauer/ Kudlich/ Schneider, Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016.

Kudlich H, "Ceza Kovuşturmasında Federal Truva Atları-Dijital Çağda Özel Yaşam Alanının Korunması", Çeviren: Rabia Ünlü, Alman-Türk Karşılaştırmalı Ceza Hukuku, C.I, Yayına Hazırlayan: Prof. Dr. Dr. Eric Hilgendorf-Prof. Dr. Yener Ünver, İstanbul 2010.

Kuhli M/Brüning J, "Einleitung zur ZIS-Sonderausgabe, Strafrecht und Digitalisierung in Wissenschaft und Praxis", Zeitschrift für Internationale Strafrechtsdogmatik, 15. Vol., 2/2020, s.39-41.

Lienhard A/Kettiger D, "Justiz in Krisenzeiten-Digitalisierung fördern", NZZ Nr. 84 09.04.2020, S.8. (www.swisslex.ch/de/doc/essay).

Lupo G/ Bailey J, "Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples", Laws (MDPI), Vol 3, Iss 2, 2014, s. 353-387.

Magherescu D, "Using New Means of Technology during the Penal Proceedings in Romania", Revista Brasıleıra De Dıreıto Processual Penal Vol:5, Issue:3, s.1189-1217.

Malgieri G./De Hert P., "European Human Rights, Criminal Surveillance,

and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges", The Cambridge Handbook of Surveillance Law (Editors: D.C. Gray-S. Henderson), New York 2017, s.509-523.

Platz E, "Rechtliche Zulassigkeit von "Remote Forensic Software" in der Schweiz-Inwieweit existiert in der Schweiz eine rechtliche Grundlage für den Einsatz von "Remote Forensic Software" durch die Ermittlungsbehörden?"", sic, 2008, s.838-844.

Quarck L, "Zur Strafbarkeit von e-personen", ZİS, Vol.15, 2/2020, s.65-70.

Rehberg J./Schmid N., Strafrecht III, 8. Aufl., Zürich 2003.

Ringe/ Trute, Zentrum für Recht in der digitalen Transformation (ZeRdiT)

Schindler B, (Verfahrens und Gerichtsorganisationsrecht/Justizöffentlichkeit im digitalen Zeitalter), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, s.741-757.

Schneider F, "Auswirkungen der Digitalisierung auf das Ermittlungsverfahren, Impulse aus der Strafverteidigungspraxis", Zeitschrift für Internationale Strafrechtsdogmatik, 2020/2, s.79-83.

Soine M, "Die Strafprozessuale Online-Durchsuchung", Neue Zeitschrift für Strafrecht (NStZ) 2018.

Weissenberger P., Basler Kommentar, Strafrecht II, 2. Aufl., Basel 2007.

Zanon B, Reschtsfragen zu VoIP im Hochschulumfeld, SWITCH Journal, 2006.