SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 03.07.2026
Kabul | Accepted: 05.09.2026
doi 10.15337/suhfd.1985995

SUÇUN AYDINLATILMASINDA KİŞİSEL VERİLERİN YAPAY ZEKÂ DESTEKLİ SİSTEMLERDE KULLANILMASI: TAHMİNE DAYALI ÖNLEYİCİ KOLLUK (PREDICTIVE POLICING) FAALİYETLERİ HANGİ ANDAN İTİBAREN CEZA SORUŞTURMASI KAPSAMINDA DEĞERLENDİRİLMELİDİR?

Dr. Öğr. Üyesi Hasan ÇATAKLI*

Öz

Temel hak ve özgürlüklere ilişkin güvencelerin, ceza muhakemesinde soruşturmanın başlangıcından itibaren etkili olması sağlanmalıdır. Bu açıdan başlangıç şüphesi, sadece savcıya soruşturma başlatma yükümlülüğü getiren bir şüphe derecesi değildir. Başlangıç şüphesi aynı zamanda, bireyleri keyfi ceza soruşturmalarına karşı koruyan bir "koruyucu duvar" işlevi görmekte ve başta hukuk devleti ve ölçülülük ilkeleri olmak üzere, soruşturmanın başlatılabilmesi için anayasal anayasal güvencelerin bir gereği olarak ortaya çıkmaktadır- Fakat yapay zeka destekli sistemlerin önleyici kolluk faaliyetleri kapsamında kullanımıyla birlikte, güvenlik endişelerinin özgürlük karşısında giderek daha fazla tercih edilmesi, istihbari faaliyetler, önleyici kolluk faaliyetleri ve ceza soruşturması arasındaki sınırları belirsizleştirmektedir. Bu nedenle, suçun önlenmesinde kullanılan yeni teknolojilerin ortaya çıkardığı riskler karşısında

* Dr. Öğr. Üyesi, Süleyman Demirel Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Ana Bilim Dalı, Isparta, Türkiye | Asst. Prof. Dr., Süleyman Demirel University, Faculty of Law, Department of Criminal Law, Isparta, Türkiye.
hasancatakli@sdu.edu.tr • ORCİD 0000-0002-5631-3343.

Atıf Şekli | **Cite As**: **ÇATAKLI,** Hasan, "Suçun Aydınlatılmasında Kişisel Verilerin Yapay Zekâ Destekli Sistemlerde Kullanılması: Tahmine Dayalı Önleyici Kolluk (Predictive Policing) Faaliyetleri Hangi Andan İtibaren Ceza Soruşturması Kapsamında Değerlendirilmelidir?", SÜHFD, C. 34, S. 3, 2026, s. 1755-1825.

İntihal | **Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. | This article has been scanned via a plagiarism software and reviewed by at least two referees.

temel hak ve özgürlüklerin etkili bir şekilde korunabilmesi için, ceza muhakemesi güvencelerinin uygulanmaya başlayacağı eşik yeniden belirlenmelidir. Söz konusu eşiğin belirlenmesi, tahmine dayalı önleyici kolluk faaliyetleri kapsamında elde edilen kişisel verilerin başlangıç şüphesinin varlığının tespiti bakımından ne anlama geldiğinin belirlenmesini de gerekli kılmaktadır. Bu kapsamda gündem gelen bir diğer husus ise önleyici kolluk faaliyetleri kapsamında elde edilen verilerin ceza soruşturmasında kullanılabilmesini hukuki açıdan mümkün kılacak koşulların tespiti edilmesidir. Başlangıç şüphesinin önleyici kolluk faaliyetleri ile ceza soruşturması aşaması arasındaki sınırı belirleyen fonksiyonu bu çerçevede gündeme gelen hukuki tartışmalarda belirleyici bir rol oynamasına yol açmaktadır.

Anahtar Kelimeler

• Başlangıç Şüphesi • Öngörüye Dayalı Kolluk • Kişisel Veri • Bilişimsel Kaderini Tayin Hakkı • AB Yapay Zekâ Düzenlemesi

AN ISSUE FURTHER COMPLICATED BY THE USE OF PERSONAL DATA IN AI-POWERED PROGRAMS FOR CRIME CLEARANCE: AT WHAT POINT CAN PREDICTIVE POLICING ACTIVITIES BE CONSIDERED WITHIN THE SCOPE OF A CRIMINAL INVESTIGATION?

Abstract

A criminal procedure that embodies the requisite safeguards for fundamental rights and freedoms must be ensured from the very outset—namely, from the inception of the investigation. From this perspective, the threshold of initial suspicion is not merely a factual trigger imposing a duty on the prosecutor to initiate an investigation; rather, it functions as a 'protective shield' for individuals against prospective judicial proceedings, serving as a legal guarantee necessitated by the constitutional principle of proportionality. Nonetheless, the integration of artificial intelligence-driven systems into preventive policing has increasingly prioritized security over liberty, rendering the already thin line between intelligence, preventive policing, and criminal procedure virtually transparent. Consequently, in order to secure the necessary guarantees for fundamental rights and freedoms against these new technological tools of crime prevention, this boundary may need to be recalibrated and reconstructed further forward to effectively address these emerging challenges.

Key Words

• Initial Suspicion • Predictive Policing • Right to Informational Self-Determination • Personal Data • EU Artificial Intelligence Act

Extended Summary

Although the development of artificial intelligence-supported software enables highly positive advancements in many fields such as healthcare, infrastructure, communication, and research, its use for criminal purposes also poses a very serious risk to the protection of legal interests (Rechtsgüter), which constitute the fundamental basis of legitimacy for criminal law norms. This contemporary dimension of utilizing technology with criminal motivation elevates will manipulation through deception—specifically in the context of fraud targeting property assets—to a level that is extremely difficult to detect (Deepfake). The proceeds of crime are converted into cryptocurrencies and subsequently transferred across hundreds of different accounts, making tracking and seizure highly challenging. This method itself directly interferes with personality rights by relying on the unauthorized acquisition, processing, and use of personal data in the digital world. Confronting crimes committed through the use of artificial intelligence makes it a necessity to employ AI for intervention before the crime occurs, as well as for tracking and investigation after the crime is committed. In this context, the use of AI-supported programs that process personal data for preventive policing (Risk Assessment & Analysis / Profiling Tools & Systems) and, to a certain extent, in criminal procedure is becoming increasingly common, including in Continental Europe. This brings the issue of the balance between freedom and security in crime investigation to a new dimension. Indeed, this tension stems from the inevitable divergence between the liberal constitutional doctrine of fundamental rights and freedoms (Grundrechtslehre) and the structurally conservative, cautious, and preventive nature of the conception of protecting legal interests (Rechtsgutlehre/Rechtsgüterschutz), which serves as the justification for the legitimacy of criminal law norms.

The tension arising between the concepts and doctrines of these two fields of law—which intersect in areas such as preventive policing and protective measures in criminal procedure and are established in line with their diverging objectives—also highlights the necessity of producing a coherent legal stance. To express this "tension" specifically in terms of the subject matter, it manifests itself in the struggle to strike a balance between the prevention of crime, the clarification of crimes, and victims' rights on one side, and the right to protection of personal data as the digital counterpart of the right to shape one's personality based on decisions made of one's own free will on the other.

At this point, taking into account the technical dimension of predictive policing, digital personality, and personal data (or highly sensitive personal data), it is necessary to adapt existing concepts or develop new ones to integrate them into the current Law of Criminal Procedure within valid principles. This integration also entails new legislative regulations. The integration of AI-supported programs into the Criminal Justice System brings about the question: Will these

regulations be based on data protection law (Datenschutzrecht), or will they center on the protection of fundamental rights (Grundrechtsschutz) or product safety (Produktsicherheit)?

Another issue raised by this subject is the distinction between intelligence and preventive policing, as well as between preventive policing and judicial policing. Within the scope of this distinction, one of the first questions we encounter is: At what point should the outputs obtained from preventive policing activities carried out using AI be accepted as having transformed into a simple/initial suspicion (the starting point of criminal proceedings) indicating that a crime has been committed? Prior to the emergence of initial suspicion, law enforcement activities that interfere with fundamental rights and freedoms are subject to more flexible conditions than the protective measures in criminal procedure, with the aim of providing "effective intervention" capabilities . The answer to this question is crucial, as the activation of criminal procedure and the acquisition of the status of "suspect" trigger the safeguards regarding individual liberties (the rights of the suspect). Another question is: If there are not yet sufficient concrete grounds to accept initial suspicion, but there is a situation that needs to be investigated to determine whether initial suspicion exists, to what extent and in what manner will it be legally possible to utilize AI-supported programs and systems? This study aims to evaluate this issue within the scope permitted by a research article.

GİRİŞ

Gelişen ve kullanım alanları son derece yaygınlaşan bilişim teknolojisinin bir sonucu olarak, bireyin kişiliğinin siber uzaydaki bir yansıması niteliğinde olan dijital ikizinden bahsetmek mümkündür. Bu yansıma, elektronik ticaret platformlarının, arama motorlarının, seyahat asistanlarının, elektronik haberleşme araçlarının, sosyal medya platformlarının, akıllı ev eşyalarının, elektronik devlet sisteminin ve benzeri uygulama ve nesnelerin kullanılması sonucunda sanal dünyada veri olarak bıraktığımız izlerin bütününden oluşmaktadır.

Google, Microsoft ve X gibi şirketler tarafından sunulan yapay zekâ destekli dil işleme modellerinden yararlanan ve hayatımızın neredeyse bütün alanlarına temas eden entegre sistem ve uygulamaların kullanımıyla dijital dünyadaki varlığımızın kişiliğimizin bir parçası haline geldiğini söylemek mümkündür. Özel hayat alanı artık kişiliğin veriye dayalı bu yeni boyutuna da uzanmaktadır. Bu alanın hukuken korunması gerekliliği, anayasal bir temel hak olan kişi özgürlüğünün ve bireyin kişiliğini kendi kararları doğrultusunda geliştirme hakkının

(Selbstbestimmungsrecht) yeni bir boyutu olarak "bilişimsel kendi kaderini tayin hakkı" (**informationalle Selbstbestimmungsrecht**)[1] olarak adlandırılmaktadır. Söz konusu hak, bireylerin hayatlarının kişisel boyutunun ne zaman, ne şekilde ve ne ölçüde aşikâr kılınacağına karar verme yetkisinin kural olarak bireylere ait olması şeklinde tanımlanmakta ve veri koruma bakımından bir temel hak olarak kabul edilmektedir. Kişi özgürlüğünün bilişimsel alandaki tezahürü olan "bilişimsel kaderini tayin hakkı", kişisel verilerin ancak kanunla belirlenen şartlar çerçevesinde ve veri sahibinin bilgilendirilerek alınmış rızasına dayalı olarak işlenebilmesini gerektirmektedir.[2]

Yapay zekâ destekli yazılımların gelişimi, sağlık, altyapı, iletişim ve araştırma gibi birçok alanda son derece olumlu gelişmeleri imkân sağlamakla birlikte, bu yazılımların suç işlemek amacıyla kullanılması, ceza normlarının meşruiyetinin temel dayanaklarından biri olan hukuki değerlerin korunması bakımından oldukça ciddi bir risk[3] ortaya çıkarmaktadır.

Teknolojinin suç işlemek amacıyla kullanımının günümüzde kazandığı bu yeni boyut, özellikle mal varlığı değerlerine karşı işlenen dolandırıcılık suçları bağlamında, hile yoluyla iradenin manipüle

---

1 **LI**, Rueisiang, Die Auswirkungen von Künstlicher Intelligenz auf die Strafverfolgung, Baden-Baden 2025, s. 92; **BANERT**, Christian, KI-gestütze Ermittlungen und der Kernbereich privater Lebensgestaltung, Baden-Baden 2025, s. 92; Alman Federal Anayasa Mahkemesi, bireyin kişiliğini özgürce inşa etmesi hakkını, verilerin işlenmesi, sınırsız biçimde kullanılması ve kaydedilmesine ilişkin modern yöntemler karşısında korunması bağlamında konumlandırmaktadır, BVerfGE 65, 1 (43)=NJW 1984, 419; BVerfGE 125, 260 (310)=NJW 2010, 833Ü; "*Kaydedilmiş veri yığınlarının, verilerin kişiyle ilişkilendirilebilir surette kullanıldığı otomatikleştirilmiş veri analizi veya değerlendirilmesi yoluyla işlenmesi, bilişimsel kendi kaderini tayin hakkına (Art. 2 Abs. 1 bağlamında Art. 1 GG) müdahale teşkil eder*.", BVerfGE, Urt. V. 16.2.2023- 1 BvR1547/19-1 BvR 2634/20.

2 **TINNEFELD**, Marie-Theres/ **BUCHNER** Benedikt/**PETRI** Thomas/**HOF** Hans-Joachim, Einführung in das Datenschutzrecht, 7. Baskı, Berlin 2020, s. 122.

3 Postmodern toplumda dijital riskler ve ceza hukukunun bu yeni riskler karşısındaki pozisyonu için bkz. **SÖZÜER**, Adem/**TURHAN**, Esma Nur: "Risk Toplumunda Ceza Hukukunun Rolü ve Fonksiyonu", Özgenç, İzzet (Editör), Risk Toplumunun Ceza Hukuku Alanında Ortaya Çıkardığı Sorunlar, Türkiye Bilimler Akademisi Yayınları, Ankara 2025, s. 22-25.

edilmesinin tespitini oldukça zor bir boyuta taşımaktadır.[4] Suçtan elde edilen gelirlerin kripto paraya dönüştürülmesi ve arkasından yüzlerce farklı hesaba aktarılması, bunların takip edilmesini ve bunlara el konulmasını oldukça zorlaştırmaktadır. Söz konusu yöntemler, sanal dünyadaki kişisel verilerin (banka hesap bilgileri, kimlik bilgileri vb.) rıza dışında elde edilmesine, işlenmesine ve kullanılmasına dayandığından, kişilik haklarına doğrudan müdahale teşkil etmektedir. Konunun bir boyutunu, yapay zekâ kullanılarak işlenen suçlarla mücadelede hem suç işlenmeden önce müdahale edilebilmesi hem de işlendikten sonra yürütülen soruşturmada yapay zekadan yararlanılmasının giderek bir zorunluluk olarak ortaya çıkması oluşturmaktadır. Bu bağlamda, kişisel verileri işleyen yapay zekâ destekli sistemlerin önleyici kolluk faaliyetlerinde, özellikle risk değerlendirme, analiz ve profilleme ve sistemleri (risk assesment and analysis/profiling tools and system) kapsamında ve belirli ölçüde ceza muhakemesinde kullanımı, Kıta Avrupası da dahil olmak üzere gün geçtikçe yaygınlaşmaktadır. Bu teknolojilerin kullanımı, suçların soruşturulması ve kovuşturulmasında özgürlük ile güvenlik arasındaki denge sorununu[5] yeni bir boyuta taşımaktadır. Aslında bu sorun, liberal anayasal temel hak ve özgürlükler doktrini (Grundrechtslehre) ile ceza normlarının meşruiyetini hukuki değerlerin korunmasına dayandıran ceza hukuku anlayışının (Rechtsgutslehre/Rechtsgüterschutz) yapısal olarak ihtiyatlı ve korumacı niteliği arasındaki farklılıktan kaynaklanmaktadır[6]. Bu iki hukuk dalının

---

4 **TURHAN**, Turhan, **KIRLIOĞLU**, Gamze/**BELCİ**, Ozancan, Türk Ceza Kanunu'na Göre Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık-Phishing Yöntemiyle Online Bankacılık Erişim Bilgilerinin Ele Geçirilmesi ve Bunların Kullanılmasının Ceza Hukuku Açısından Değerlendirilmesi, Semih Yumak (Editör), Türk-Alman-Gürcü Ceza Hukuku Kolokyumu, Legal Yayınları Temmuz 2025. s. 105 vd.

5 Özgürlük ve güvenlik dengesi sorunu hakkında ayrıntılı bilgi için bkz. **TURHAN**, Faruk/**AKSU**, Muharrem: "11 Eylül Sonrası ABD'de Özgürlük ve Güvenlik Dengesi Açısından Terörü Önleme Amaçlı Tedbirler / Özellikle PATRIOT Kanunu ile Getirilen Kısıtlamalar", Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, C. 1, S. 1, 2016, s. 52 v.d.

6 **STUCKENBERG**, Carl-Friedrich, The Constitutional Defenciencies of the German Rechtsgutlehre, Oñati Socio-Legal Series, v. 3, n. 1 (2013) s. 31, 34-36.

kesiştiği önleyici kolluk ve ceza muhakemesindeki koruma tedbirleri gibi alanlarda her bir hukuk alanının kendine özgü amaçları doğrultusunda teşkil edilmiş kavram ve öğretiler arasında ortaya çıkan gerilim, insicamlı bir hukuki yaklaşım geliştirilmesi gerekliliğini ortaya çıkarmaktadır. Söz konusu "gerilim", konu özelinde bir şekilde ifade etmek gerekirse; bir tarafta suçun önlenmesi, aydınlatılması ve mağdur haklarının korunması diğer tarafta ise kişinin özgür iradesi ile aldığı kararlar doğrultusunda kişiliğini şekillendirme hakkının dijital dünyadaki karşılığı olan kişisel verilerinin korunması hakkı arasında denge kurulması gereğinde kendisini göstermektedir.[7]

Bu noktada, tahmine/öngörüye dayalı kolluk (predictive policing), dijital kişilik, kişisel veriler ve yüksek özellikte kişisel veri alanlarının teknik özellikleri dikkate alınarak, mevcut kavramların bu gelişmelere uyarlanması veya yeni kavramların geliştirilmesi ve bunların geçerli prensipler dahilinde mevcut ceza muhakemesi hukukuna entegre edilmesi gerekmektedir. Bu entegrasyon, aynı zamanda yeni yasal düzenlemeler yapılmasının gereğini de ortaya koymaktadır. Yapay zekâ destekli sistemlerin ceza adaleti sistemine entegrasyonu için yapılacak düzenlemelerde veri koruma hukuku (Datenschutzrecht), temel hakların korunması (Grundrechtsschutz) ve ürün güvenliği (Produktsicherheit) arasında hangisinin merkeze alınacağı sorusu ortaya çıkmaktadır.[8]

Konunun gündeme getirdiği bir diğer mesele ise istihbarat- önleyici kolluk ve önleyici kolluk -adli kolluk ayrımlarıdır. Bu ayrımlar kapsamında karşımıza ilk çıkan sorulardan biri, yapay zekâ kullanılarak gerçekleştirilen önleyici kolluk faaliyetlerinden elde edilen çıktıların

---

7 **CONRAD**, Cathrina Pia, Ein Update für den Kernbereichsschutz, Berlin 2024, s. 48. Bu bağlamda yapılan yeni düzenlemeler ile kapsamı ve boyutları gitgide daha da somutlaşmaya başlayan kişisel verilerin korunması hakkının kişi özgürlüğü ve bunun bir parçası olarak özel hayatın gizliğinin teknolojik gelişmeler bağlamında değişen insan ilişkilerine ve toplumsal yaşam koşullarına uyarlanması olarak kabul etmekteyiz. Aksi görüş için bkz. **KIZILIRMAK**, Baran, Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi, KHASHFD Cilt: 7 Sayı: 2, Aralık 2019, s. 225, 258.

8 **GLESS**, Sabine/**ERIKSSON**, Salome, KI in der Strafrechtspflege: Einführung, in: Künstliche Intelligenz in der Strafrechtspflege, Gless, Sabine/Avedisian Dorotea (edt.), Basel 2026, s. 3, 42.

hangi andan itibaren ceza muhakemesinin başlangıcı olan bir suçun işlendiğine basit şüpheyi/başlangıç şüphesini oluşturduğunun kabul edileceğidir. Başlangıç şüphesinden önce gerçekleştirilen ve temel hak ve özgürlüklere müdahale teşkil eden kolluk faaliyetleri, "etkin müdahaleye" imkân sağlamak amacıyla koruma tedbirlerine kıyasla daha esnek şartlara tabi tutulmaktadır.[9] Bu sorunun cevabı, ceza muhakemesi hükümlerinin uygulanmaya başlanması, kişinin şüpheli sıfatını kazanması ve buna bağlı olarak şüpheli haklarına ilişkin güvencelerden yararlanması bakımından önem arz etmektedir.

Diğer bir soru ise başlangıç şüphesinin kabulü için henüz yeterli somut dayanak noktaları bulunmamakla birlikte, bu şüphenin mevcut olup olmadığının tespiti amacıyla araştırılması gereken bir durum söz konusu olduğunda, yapay zekâ destekli program ve sistemlerden hukuken ne ölçüde ve ne şekilde yararlanabileceğidir.[10] Çalışmada söz konusu sorunların, bir araştırma makalesinin kapsamının elverdiği ölçüde değerlendirmesi amaçlanmaktadır.

I. YARGI SİSTEMLERİNDE VE ÇEVRELERİNDE YAPAY ZEKÂ KULLANIMINA İLİŞKİN CEPEJ[11] AVRUPA ETİK ŞARTI

Yapay zekâ destekli programların ceza adaleti sistemlerinde giderek artan kullanımı karşısında, Avrupa Konseyi Avrupa Adaletin Etkinliği Komisyonu (CEPEJ) 4 Aralık 2018 tarihinde Yargı Sistemlerinde ve Çevrelerinde Yapay Zekâ Kullanımına İlişkin Avrupa Etik Şartı'nı[12] yayınladı. Etik Şart, yapay zekâ destekli sistemlerin ceza adaleti sistemi içindeki kullanımının temel hak ve özgürlüklere etkisini ele almaktadır.[13]

---

9 **ERDOĞAN**, Irmak, Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenilmesine Etkileri, Ankara 2022 s. 43.

10 **GLESS/ERIKSSON**, s. 43, 44.

11 Avrupa Adaletin Etkinliği Komisyonu (CEPEJ)

12 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

13 **LI**, s. 150.

Etik Şart bağlamında dile getirilen en önemli hususlardan biri, hukuki karar alma mekanizmalarında yapay zekâ sistemlerinin kullanılması durumunda, kişi özgürlüğü, özel hayat ve adil yargılanma gibi temel hak ve özgürlüklerin dikkate alınması ve bunlara saygı gösterilmesinin sağlanmasıdır (Principle of respect for fundamental rights) sağlanmasıdır. Bu bağlamda, yapay zekâ destekli sistemlerin sadece insan tarafından alınacak kararları destekleyici bir rolde kalması ve , asla bir insan tarafından verilmesi gereken kararda onu tamamen ikame eden bir fonksiyon icra etmemesi gerektiği vurgulanmaktadır.[14]

Yargı sistemi içerisinde yapay zekâ kullanımında özellikle hassas verilerin (etnik köken, dini inanç ve kanaatler, sendika üyeliği, genetik ve biyometrik özellikler, sağlık bilgileri, cinsel hayat ve cinsel tercih, siyasi görüş) işlenmesi durumunda bu bilgilere dayalı olarak gruplama ve sınıflama yoluyla birey ve gruplar arasında ayrımcılığa yol açacak (Principle of non-discrimination) veya mevcut ayrımcılığı derinleştirecek bir deterministik analize dayalı çıktılar üretilmesinin önüne geçecek önlemlerın alınmış olması gereği vurgulanmaktadır.[15] Kullanılan yapay zekâ modelinin ayrımcılığa yol açacak çıktılar ürettiğinin tespit edilmesi durumunda, özellikle sistemi kararlarını destekleyici mahiyette kullananların bu risk hususunda bilinçlendirilmesine dikkat çekilmektedir. Etik Şart'ta söz konusu ayrımcılık riskini etkisiz hale getirecek, bunun etkisizleştirilmesi mümkün değilse riski azami düzeyde sınırlandıracak önlemlerin alınması gerektiği belirtilmektedir.[16]

Yargı sisteminde kullanılacak yapay zekâ destekli sistemlerin makine öğrenmesine dayalı modellerinin geliştirilmesi aşaması, yargı

---

14 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, s. 7- 8. Yapay zekâ algoritmaları, etik olarak insani düşüncenin otonomisi temelinde insani değerlendirmeleri dikkate alacak şekilde yapılandırılmalı ve ahlaki kararların kullanıcı tarafından yapay zekâ sistemine bırakılamayacağı şekilde yapılandırılmalıdır, **LI**, s. 150.

15 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, s. 9.

16 **LI**, s. 151.

karar mekanizmalarında yer alan hâkim, savcı, avukat, hukukçu akademisyenler ve sosyoloji ve felsefe gibi bilim dallarında çalışan uzmanların etkileşime dayalı ortak katılımıyla gerçekleştirilmelidir. Yazılımın geliştirilmesinde kullanılacak yargı kararlarına dayalı verilerin, doğrulanarak ve değiştirilmeden sisteme girilmesi ve kullanılması gereklidir. Yapay zekâ yazılımının bütün geliştirilme süreci, yazılımın çıktı olarak vereceği kararın anlam ve içeriğinde değişikliğe neden olabilecek bir değişikliğin söz konusu olmadığının denetlenmesini mümkün kılacak şekilde tasarlanmalıdır. Söz konusu gereklilik, kalite ve güvenlik prensibi (Principle of quality and security) olarak adlandırılmıştır. [17]

Etik Şart' ta belirtilen dört numaralı ilke, şeffaflık, bağımsızlık ve tarafsızlık prensibidir. Yapay zekâ destekli bir sistemin hukuki sonuç doğuracak veya birey bakımından olumsuz, kısıtlayıcı etkileri olacak şekilde kullanılması durumunda, veri işleme metodunun erişilebilir, şeffaf ve anlaşılır olması ve dış değerlendirmeye imkân sağlaması gerekmektedir. Bu sayede veri işleme yönteminin denetlenebilmesi mümkün olacaktır. Yargı sisteminde kullanılacak yapay zekâ modelinin tasarım aşamasından itibaren, yazılım üzerindeki fikri ve sınai haklar ile şeffaf, tarafsız ve yargılamada öncelenen amaç ve menfaatlerin dikkate alınması arasında denge gözetilmesi gerekmektedir. Bu noktada özellikle şeffaflık ilkesinin, yapay zekâ sisteminin yazılımın geliştirilmesi aşamasında kullanılan veriler bakımından tam olarak uygulanabilir olmadığı görünmektedir. Fakat şeffaflık ilkesi, yazılımın kodları ve bunların belgelendirilmesini gündeme getirdiğinde, yapay zekâ yazılımlarının ve yapay zekâ destekli sistemlerin önemli bir kısmının aynı zamanda ticari ürün niteliğinde olduğu düşünüldüğünde, ticari sırların

---

17 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, s. 10.

korunması gündeme gelmektedir. Şeffaflık ilkesi bu noktada bir sınırla karşılaşmaktadır.[18]

Etik Şart kapsamında beşinci ilke olarak "kullanıcının kontrolünde olma" (Principle "under user control") ifade edilmektedir. Yapay zekâ destekli araç ve hizmetlerin kullanımının, kullanıcının otonomisini sınırlayıcı bir etki göstermemesi gerekmektedir. Söz konusu prensip uyarınca, ilk olarak hukuk profesyonelleri mahkeme kararlarını ve bir sonuca ulaşılmasında kullanılan verileri her zaman denetleyebilmeli; ayrıca her somut olayın özelliklerini dikkate alarak bunlarla mutlaka bağlı olmamalıdırlar. Hâkimin, nasıl işlediğini, nasıl bağıntı kurduğunu, hangi verileri ne tür bir yöntemle işleyerek çıktı ürettiğini bilmediği bir sistemden çıkan sonuçları dikkate alarak karar vermesi durumunda, delillere doğrudan temas ederek vasıtasız bir şekilde kanaat oluşturduğunun kabulü mümkün olmayacaktır[19]. Bu durumda, AİHS m. 6 bağlamında adil yargılanma hakkı kapsamında değerlendirilen delillerin doğrudan doğruyalığı ilkesine[20] uygun olarak mahkeme huzurunda hukuki meselelerin duruşmalı olarak, görülmesinden bahsetmek mümkün görünmemektedir.[21] Prensibin ikinci bir boyutu ise AİHS m. 6'da düzenlenen adil yargılanma hakkı bağlamında mahkemeye

---

18 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, s. 11.

19 Maddi anlamda doğrudan doğruyalık ilkesi, hâkimin imkanlar dahilinde azami şekilde olay ile doğrudan bağlantı kurabilmesini mümkün kılan delillere dayalı kanaat oluşturmasını gerektirmektedir. Şekli anlamda doğrudan doğruyalık ilkesi ise, araya bir vasıta girmeksizin, hâkimin doğrudan kanaate ulaşmasını gerekli kılar, **ŞAHİN**, Cumhur/**GÖKTÜRK**, Neslihan, Ceza Muhakemesi Hukuku, 15. Baskı, Ankara 2024, s. 480, 481.

20 Söz konusu ilke AHİS m. 6/3-d bağlamında maddi anlamda doğrudan doğruyalık ilkesinin bir gereğidir, 479, 483; **ÜNVER**, Yener/**HAKERİ**, Hakan, Ceza Muhakemesi Hukuku, Ankara 2020, 17. Baskı, Ankara 2020 s. 93.

21 EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, s. 12; Yapay zekâ modelinin geliştirilmesinde kullanılan veriler ile yazılımın çalışma prensiplerinin fikri mülkiyet gerekçesiyle paylaşılmamasının savunma hakkını kısıtlayarak adil yargılanma hakkının ihlaline yol açabileceği yönünde bkz., **ERDOĞAN**, s. 52.

erişim hakkının bir yansımasını teşkil etmesidir. Davanın tarafları, gerek yargılama öncesi gerekse yargılama süreci içerisinde herhangi bir aşamada alınan bir kararda, yapay zekâ veya yapay zekâ kullanılarak işlenmiş bir verinin kullanıp kullanılmadığı, ne ölçüde kullanıldığı ve kullanımın alınan karara etkisi hususunda açık ve anlaşılır bir biçimde bilgilendirilmeli ve buna itiraz etme hakkına sahip olmalıdırlar. Yine ilke kapsamında belirtilen hususlar yerine getirilmediği takdirde, alınan kararlarda dayanak oluşturan delillerin veya bu delillerin elde edilmesi şeklini veya delile ulaşılmasına ilişkin süreçleri bilmeyen sanık veya şüphelinin, delilleri etkili bir şekilde delilleri tartışma ve bunlara itiraz etme imkanına sahip olduğundan bahsedilemeyecektir. Bu durumda, delillerin tartışılmış[22] olması gereği yerine getirilmemiş olacak ve çelişmeli yargılama ilkesinin[23] ihlali gündeme gelecektir.[24]

Etik Şart'ta yer alan prensipler ceza adaleti sistemi içerisinde kullanılacak yapay zekâ programlarının geliştirilmesi aşmasından itibaren yargı ve çevrelerinde kullanılmasına kadar uzanan gerekliliklere dikkat çekmektedir. Etik Sart'ın ülkemiz hukuku açısından doğrudan bir bağlayıcılığı yoktur. Fakat Etik Şart'ta dikkat çekilen prensipler hem Anayasa hem de tarafı olduğumuz AİHS'te yer alan adil yargılanma, silahların eşitliği, mahkemeye erişim hakkı, etkin savunma hakkı ve delillerin doğrudanlığı gibi temel haklar ve bunları hayata geçiren prensiplerin yargı ve çevresinde yapay zekâ destekli sistemlerin kullanılması durumuna uyarlanması anlamına gelmektedir. Söz konusu prensiplerin ihlali, yapılacak yargılamada alınan kararın veya verilen hükmün Anayasa ve AİHS'ye aykırı hale gelmesine yol açabilecektir. Bu sebeple, yapay zekâ destekli profilleme ve dijital araçların ceza adaleti sistemi içerisinde kullanılmaya başlamasıyla birlikte Etik Şart'ta ifade

---

22 **ŞAHİN/GÖKTÜRK**, s. 532.

23 **ÜNVER/HAKERİ**, s. 587.

24 Şekli anlamda doğrudan doğruyalık ilkesi ayrıntılı bir sözlü duruşmaya imkân verilmesi anlamına gelmektedir. Hüküm bakımından önem taşıyan bütün hususlar ve araştırma sonuçları mahkeme huzurunda savunmanın kendisi bakımından önem arz eden hususlara ilişkin görüş belirtebileceği şekilde duruşmaya getirilmelidir, **ŞAHİN/GÖKTÜRK,** s. 480, 481.

edilen ilkelerin, bir yargılama kapsamında verilecek kararlarla uygulamada somutlaştırılmayı beklediği söylenebilecektir.

II. CEZA MUHAKEMESİNDE BAŞLANGIÇ ŞÜPHESİ VE ALGORİTMİK OLARAK OLUŞTURULAN "ŞÜPHE"

A. Başlangıç (Basit) Şüphesinin Ceza Muhakemesi Bakımından Anlamı

Modern ceza muhakemesi hukukunun amacı hukuk devletine uygun araç ve yöntemlerle suç şüphesinin tavzih edilmesi, bir diğer ifade ile şüphenin yenilmesi gerekmektedir. Ceza muhakemesinin konusunun somutlaştırılması ve sınırlandırılması, şüphelinin haklarıyla birlikte muhakemenin bir öznesi olarak temayüz edebilmesinin şartı olarak kabul edilmektedir. Şüpheli ancak somut ve sınırları belirli olan bir suç şüphesi isnadının varlığı durumunda alacağı profesyonel hukuki yardımla kendisini etkin bir biçimde savunabilecektir. Suç tipinde yer alan tanıma uygun bir fiilin işlendiği izlenimini veren (CMK m. 160/1) somut ve ispatlanabilir bir olguya dayalı olarak beliren basit şüphe (başlangıç şüphesi) ile başlayan ceza muhakemesi, hem kovuşturma aşamasına geçme veya sanık hakkında mahkûmiyet kararı verilebilmesi hem de kanunda öngörülen koruma tedbirlerine başvurulabilmesi için farklı şüphe derecelerini aramaktadır.[25] Basit şüphe veya başlangıç şüphesinin yoğunluğu savcı tarafından iddianamenin düzenlenebilmesi için aranan "yeterli şüpheye" (CMK m. 170/2), temel haklara önemli müdahale teşkil eden bazı koruma tedbirlerine başvurulabilmesi için aranan "kuvvetli şüpheye" (CMK m. 100/1, m. 133/1) ve de doğal olarak mahkumiyet hükmü için gerekli suç teşkil eden "yüklenen suçu işlediğinin sabit olması, bir diğer ifadeyle fiilin sanık tarafından işlendiği hususunun aksini kabulü mümkün kılan makul bir şüphe kalmadığı suçun sanık tarafından işlendiğinin sübut bulması (CMK m. 223/5) durumuna nazaran daha azdır.[26] Fakat bu durum ceza soruşturmasının başlaması

---

[25] **WOHLERS**, Wolfgang, Das an einen tatbezogenen Anfangsverdacht gekoppelte Strafverfahren, AJP 2020, s. 1311, 1312.

[26] **ZAFER**, Hamide/**YAVUZ**, Yağız, Ceza Muhakemesinde Suç Şüphesi ve Dereceleri, MÜHF-HAD (Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi) Cilt: 30 Sayı: 2, Aralık 2024, s. 462, 466; **PETERS**, Sebastian, § 152, in: Münchener

için gereken başlangıç şüphesinin sadece bir söylenti, kriminal tecrübeye dayalı soyut bir çıkarım veya belirsiz genel bir düşünceden ibaret olduğu anlamına gelmeyecektir. Başlangıç şüphesinin varlığı kanunda suç olarak tanımlanan bir davranışın gerçekleştirildiğini düşündüren somut dayanak noktalarının ampirik bir dal olan kriminalistik perspektiften değerlendirildiğinde ceza hukuku bakımından soruşturulması/kovuşturulması mümkün ve yaptırım uygulanabilir bir suça işaret etmesine bağlıdır. Başlangıç şüphesi bu mahiyeti ile sadece savcı bakımından soruşturma başlatma gerekliliği ortaya koyan bir olgu değil, aynı zamanda adli makamların soruşturma başlatabilmesi için gerekli görülen belirli bir yoğunluktaki şüpheye[27] delalet etmektedir. Diğer bir ifade ile adli makamlar ancak "başlangıç şüphesi" düzeyine erişmiş bir şüphe yoğunluğu durumunda soruşturma başlatabilirler[28]. Aksi bir kabul daha ceza muhakemesinin başlangıcında masumiyet karinesi ile çelişik bir yaklaşıma tekabül edecektir. Yine soruşturmanın başlatılması için yeterli şüphe yoğunluğunun bulunup bulunmadığını değerlendirecek olan Cumhuriyet savcısının CMK m. 160/2'de belirtilen görevlerinden biri olan "şüphelinin haklarını korumak" yükümlülüğü de bu kabulü desteklemektedir. Bu sebeple başlangıç şüphesi, soruşturmanın başlatılabilmesi için gerekli asgari eşiği belirleyerek bireylerin kendilerine yönelik olarak başlatılması muhtemel adli süreçler karşısında "koruyucu duvar" işlevi görmektedir. Ayrıca soruşturmanın başlatılması için aranan belirli bir şüphe seviyesi olarak, anayasal ölçülülük prensibinden kaynaklanan bir gereklilik olduğu da ifade edilmelidir.[29] Bu bağlamda Türk ceza hukuku literatüründe söz konusu yoğunluktaki şüpheyi ifade etmek için yaygın şekilde kullanılan "basit

---

Kommentar zur Strafprozessordnung, Schneider, Hartmut (edt.), Band 2, 2. Baskı, München 2024, § 152 Kn. 36 (MüKoStPO-**PETERS**)

27 **WOHLERS**, s. 1316; **ÖZBEK**, Veli Özer/**DOĞAN**, Koray/ **BACAKSIZ**, Pınar, Ceza Muhakemesi Hukuku, 18. Baskı, Ankara 2025, s. 163; **RICKER** s. 43, 44; **HOVEN**, Elissa, Die Grenzen des Anfangsverdachts - Gedanken zum Fall Edathy, NStZ 2014, s. 362.

28 **WOHLERS**, s. 1313; **HOVEN**, s. 362.

29 **RICKER**, s. 62.

şüphe"[30] kavramı yerine, aynı zamanda adli makamların soruşturma başlatabilme yetkisinin doğması için bir gerekliliğe de işaret eden bu durumu daha iyi vurguladığı için "başlangıç şüphesi" (**Anfangsverdacht**) kavramını daha isabetli bulmaktayız.[31]

Başlangıç şüphesi, soruşturmanın başlatılabilmesi (ifade alma CMK m. 2/1-g, sorgu CMK n. 2/1-h vb..) için gerekli asgari şüphe eşiğini oluşturmaktadır. Bununla birlikte, soruşturma kapsamında başvurulabilecek koruma tedbirleri bakımından başlangıç şüphesinin varlığı tek başına yeterli olmayıp, ayrıca kanunda her bir tedbir için ayrıca öngörülen koşulların ve şüphe derecelerinin de gerçekleşmesi gerekmektedir. Nitekim gözaltına alma (CMK m. 91/2), zorla getirme (CMK m. 146/1), arama (CMK m. 116/1), bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma (CMK m. 134), katalog suçlara ilişkin olarak iletişimin dinlemesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi (CMK m. 135/1 ve 8), teknik araçlarla izleme (CMK m. 140/1) birbirinden farklı kanuni koşullara bağlanmıştır.

Temel hak ve özgürlüklere önemli müdahale teşkil eden koruma tedbirlerine başvurulması mevcut bir şüpheliyi gerektirmektedir ki bu da en azından bir başlangıç şüphesinin varlığını zorunlu kılmaktadır. Burada önemle vurgulanması gereken husus, varlığı için önceden belirli bir suç şüphesinin bulunması gereken koruma tedbirlerine, başlangıç şüphesini elde etmek için başvurulmasının mümkün olmadığıdır.[32] Bu bağlamda yapay zeka hususiyetine sahip program ve sistemler çok büyük veri yığınlarında çok kısa sürede işlem yaparak çıktılar ortaya koyabilmekte, bu çıktılar daha sonraki değerlendirme ve karar süreçlerinde veri olarak kullanılabilmekte ve yeni çıktıların üretilmesine dayanak teşkil edebilmektedir.[33]

---

30 **ZAFER/YAVUZ**, s. 466.

31 **ÖZBEK/DOĞAN/BACAKSIZ**, s. 162.

32 **RICKER**, s. 54, 55; HK-StPO-**GERCKE**, § 94 Kn. 31; **HOVEN**, s. 362.

33 **ERDOĞAN**, s. 187, 188.

Genel önleyici amaçla kullanılan yapay zekâ özelliğine sahip program ve sistemlerin (profilleme teknolojileri, risk analiz programları, fiziki kimlik tespiti yapan yapay zeka destekli sistemeler) işledikleri verilere ve bu verilere dayalı olarak yaptıkları çıkarımlara (profilleme, sosyal medya üzerinden hesapların takibi ve bu mecralarda paylaşılan kişisel verilerin paylaşım amacı dışında kullanımı) henüz başlangıç şüphesinin dahi bulunmadığı bir aşamada CMK kapsamında başvurulabilmesi imkanı, mühim bir hukuki riski beraberinde getirmektedir. Söz konusu risk, somut delillere dayalı yeterli suç şüphesinin ya da kuvvetli suç şüphesinin varlığına bağlanmış koruma tedbirlerine denk ölçüde temel haklara müdahale teşkil eden işlemlerin gerçekleştirilmesidir. Özellikle bu sistemlerin henüz başlangıç şüphesinin dahi bulunmadığı bir aşamada kullanılması suretiyle kişisel verilerin birleştirilmesi, dijital veri örüntülerinin tespit edilmesi, profilleme yapılması ve bireyler hakkında risk ve şüphe tespitlerinde bulunulması, bireylerin kişisel özgürlük alanına, dijital kaderini tayin hakkı bağlamında (digitales Selbstbestimmungsrecht), orantısız bir müdahale anlamına gelecektir.[34]

Soruşturmanın başlamasının somut olgulara dayalı ve belirli bir suçun işlendiği izlenimini veren başlangıç şüphesinin varlığına bağlı olması kuralı bağlamında konuya ilişkin önem arz eden hukuki sorulardan biri yapay zekâ destekli sistemlerle veri madenciliği yöntemleri kullanılarak üretilen risk veya "şüphe" göstergelerinin başlangıç şüphesine olgusal olarak dayanak oluşturup oluşturmayacağıdır. Somutlaştırmak gerekirse Gelir İdaresi Başkanlığının, finans kurumlarının, ya da kolluk birimlerinin veri tabanlarındaki büyük verilerin risk değerlendirme veya tahmin algoritmalarıyla analizi sağlanarak "olağan dışı" veya "şüpheli" olarak kategorize edilen örüntülerin (özellikle kara para aklama, terörizmin finansmanı, kaçakçılık suçlarında yararlanıldığı görülmektedir) başlangıç

---

[34] **AKBULUT**, Berrin: "Soruşturma Yapılmasına Yer Olmadığı Kararı (CMK m. 158/6)", Ceza Hukuku ve Kriminoloji Dergisi, C. 10, S. 1, 2022, s. 158, 159.

şüphesinin dayanağını oluşturup oluşturmayacağı sorusu gündeme gelecektir.

Söz konusu algoritmaların isabetli sonuçlara ulaşmasının teknik olarak mümkün olup olmadığı sorusunun yanında ayrıca bu sistemlerin ve ürettikleri çıktıların yargıda karar mekanizmalarında kullanılmasına hukuken izin verilip verilemeyeceğinin değerlendirilmesi önem arz etmektedir.[35] Söz konusu yöntemlerin yargı ve çevresinde kullanılmaya başladığı andan itibaren hukuki açıdan cevaz verilebilmesi için sadece yapay zeka destekli programın verileri nasıl işlediği ve nasıl sonuç çıkardığı sorusunda önce, Avrupa Etik Şartında da belirtiği gibi, hangi verilerin, hangi soru setleri kullanılarak nasıl geliştirildiği, bu verilerin nasıl seçildiği soruları da kritik öneme haizdir. Yine yapay zekâ programlarının önleyici kolluk faaliyetleri ve diğer idari denetim faaliyetlerinde (yüz tanıma programlarının emniyet güçleri tarafından kullanımı, gümrüklerde yapılan araç aramalarının risk analiz programlarının çıktılarının da dikkate alınması, vergi kaybını önlemek amacıyla finansal verilerin analizinde risk analiz programlara başvurulması) kullanılması henüz başlangıç şüphesinin söz konusu olmadığı bir zaman diliminde kişisel verilerin kapsamlı bir şekilde işlenmesi nedeniyle, ölçüsüz bir temel hak müdahalesi anlamına da gelebilecektir. Söz konusu meseleleri değerlendirmeden önce başlangıç şüphesinin nasıl tespit edileceğine ilişkin normatif ölçütlerin ele alınmasının faydalı olacağına inanıyoruz.

B. Başlangıç Şüphesinin Tespiti ve CMK m. 158/6 Bağlamında Soruşturma Yapılmasına Yer Olmadığı Kararı

Yargıtaya göre bir suçun işlendiği izlenimi veren halin kolluk ve savcılık tarafından öğrenilmesiyle soruşturmanın başladığı kabul edilmektedir.[36] CMK m. 160/1'de ifade edilen "suçun işlendiği izlenimini veren bir hal" diğer bir ifade ile başlangıç şüphesinin olup olmadığı, Cumhuriyet savcısı tarafından değerlendirilmelidir. Gerekli şüphe

---

35 **WOHLERS**, s. 1314, 1315.

36 **ÜNVER/HAKERİ**, s. 505; 5 CD, 23.09.2010,949/6831; "Soruşturma evresi suç şüphesinin öğrenilmesi anından" başlayacak şekilde düzenlenmiştir, **ŞAHİN/GÖKTÜRK,** s. 32.

yoğunluğunu sahip olmayan bir ihbar veya şikâyet üzerine ceza soruşturmasının başlatılması hukuka aykırı olacaktır. Adli makamların haberdar olduğu bir olgunun başlangıç şüphesi oluşturup oluşturmadığının değerlendirildiği bu ön aşama, Alman ceza hukuku literatüründe "ön soruşturma"[37] (**Vorermittlung**) olarak adlandırılmaktadır. Bu aşamada başlangıç şüphesi oluşturacak ölçüde bir halin var olmaması sebebiyle, ön soruşturmanın ilgilisi hakkında "ceza kovuşturma organları tarafından soruşturma başlatma iradesi" henüz ortaya konulmuş olmayacağı için, bu kimse kendisine suçlama yöneltilmiş kimse (**Beschuldigter**)[38] olarak değerlendirilemeyecek ve bu sebeple başlangıç şüphesinin varlığına bağlı olarak temel hak ve özgürlüklere müdahale teşkil eden tedbirlere hükmedilemeyecek ve yine başlangıç şüphesinin varlığına bağlı kılınmış soruşturma usulleri kullanılamayacaktır.[39]

694 sayılı KHK'nın 145. maddesiyle CMK m. 158'e eklenen ve daha sonra 7078 sayılı Kanun'un 140 maddesiyle kanunlaştırılan 6. fıkrada "*İhbar ve şikâyet konusu fiilin suç oluşturmadığının herhangi bir araştırma yapılmasını gerektirmeksizin açıkça anlaşılması veya ihbar ve şikâyetin soyut ve genel nitelikte olması durumunda soruşturma yapılmasına yer olmadığına karar verilir*" hükmüne yer verilmiştir. Düzenlemenin gerekçesinde yeni fıkrayla "suç oluşturmayan veya soyut ve genel nitelikteki ihbar ve şikayetler için soruşturma öncesi bir değerlendirme mekanizması" oluşturulduğu ifade edilerek, bu tür ihbar veya şikâyetler üzerine derhal soruşturmaya başlanmasının "hem usul ekonomisi hem de "lekelenmeme hakkı" ile bağdaşmayacağı belirtilmiş ve soruşturma

---

37 **ZAFER/YAĞIZ**, s. 470.

38 Kişinin Alman Ceza Muhakemesi Hukuku bakımından sadece "Verdächtiger" olarak değerlendirilebilecektir. Alman ve Türk Ceza Muhakemesi Hukukları bakımından şüpheli, kendisine suçlama yönetilen kimse ve sanık kavramları arasındaki farklılıklar için bkz. **TURHAN** Faruk, Tanıklara Yemin verilmesine ilişkin Ceza Muhakemesi Kanunu Hükümlerinin Eleştirel Bir Değerlendirilmesi, HBV-HFD Ekim 2020 C. 24 Sayı 4, s. 371, 372.

39 **GERCKE**, Björn,§ 152, in: Heidelberger Kommentar zur Strafprozessordnung, Gercke, Björn/Julius, Karl-Peter/Temming, Dieter/Zöller, Mark A. (edt.), 5. Baskı, Heidelberg 2012, § 152 Kn. 5 (HK-StPO-GERCKE)

evresinin öncesinde soruşturmanın gerekli olup olmadığına ilişkin bir ön değerlendirme aşaması getirilmiştir.[40] Alman Ceza Muhakemesi Kanunu (ACMK) § 152'de açıkça bir ön soruşturma aşaması düzenlenmemiş olmakla birlikte, savcılığın soruşturma başlatması için aranan "yeterli somut dayanaklar" (zureichende tatsächliche Anhaltspunkte) ifadesinin bir gereği olarak uygulamada kabul edilen ön soruşturma (Vorermittlung) aşamasının, CMK m. 158/6 ile Türk ceza muhakemesi bakımından yasal bir dayanağa kavuşturulduğu söylenebilir.[41]

Bu bağlamda başlangıç şüphesinin varlığının tespitinde dikkate alınacak normatif ölçütlerin belirlenmesi önem kazanmaktadır. Almanya'daki uygulamada soruşturmanın başlatılması için gerekli başlangıç şüphesinin varlığının değerlendirildiği ön aşamada (Vorermittlungen), herhangi bir form ya da ya da Alman Ceza Muhakemesi Kanunu'nda açıkça düzenleyen yasal bir dayanağı olmasa da, soruşturma makamları tarafından bilgi edinme amacıyla kişilere soruların yöneltilmesi (informatorischen Befragung) suretiyle ihtimal dahilinde olan başlangıç şüphesinin varlığını ortaya koyacak somut olguların varlığının tespitine çalışılmaktadır.[42]

Başlangıç şüphesi kavram olarak tek başına yeterince somut olmaması sebebiyle somutlaştırılması için ilave normatif kriterlere ihtiyaç duyan bir kavramdır. Kavramın somutlaştırılması ihtiyacı uygulama

---

40 **ÖZBEK/DOĞAN/BACAKSIZ**, s. 164; **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 158.

41 Ayrıca Millî İstihbarat Teşkilâtı Kanunu m. 26: isimsiz, imzasız, adressiz yahut takma adla yapıldığı anlaşılan ya da belli bir olayı ve nedeni içermeyen, delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetler, Cumhuriyet savcılarınca işleme konulmaz" diyerek yine ön soruşturma aşamasına dayanak teşkil eden bir başka düzenleme olarak kabul edilebilecektir, **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 164.

42 HK-StPO-**GERCKE**, § 152 Kn. 5. Bu noktada sadece özel hukuk davası olarak hali hazırda görülen bir uyuşmazlıkta ödemeyi geciktirmek veya vakit kazanmak bir durumun abartılması suretiyle ceza yargılamasının sadece araçsallaştırıldığı bir şikâyet veya ihbarın gündem geldiği durumlarda başlangıç şüphesi önce bu ön aşama söz konusu olmaktadır, MükoStPO-**PETERS**, § 152 Kn. 38. Türk ceza hukuku bakımından bu süreç bilgi toplama süreci olarak adlandırılmaktadır, **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 159.

bakımından adli mercilere kararlarında bir takdir alanı vermektedir. Fakat bu takdir alanının kötüye kullanılması AİHS m. 6/1 bağlamında adil yargılanma hakkının ihlali teşkil edebilecektir.[43] Bu sebeple CMK m. 158/6'da düzenlenen ön soruşturma aşamasında başlangıç şüphesinin Cumhuriyet savcısının serbest takdirine bırakılmış bir karar olarak değil, bilakis somut olaya uygulaması gereken bir hukuki ölçüt olarak kabulü gereklidir.[44] Başlangıç şüphesinin var olduğuna ilişkin savcılık tarafından verilmiş kararın hâkim tarafından denetlenebilir bir karar olması gereği karşısında başka türlü bir yorum mümkün gözükmemektedir. Başlangıç şüphesi, bir tahmini aşan, somut olguların mantıklı ve tutarlı bir şekilde yorumu sonucu varılmış bir çıkarımdır. Bu sebeple söz konusu çıkarımın, çıkarımı yapan mercinin dışında da kriminalistik perspektiften makul ve savunabilir somut olgulara dayanması gerekmektedir. Kısaca ifade etmek gerekirse, başlangıç şüphesinin varlığının denetimi, bu değerlendirmenin savunulabilir olup olmadığına ilişkindir ve hukuk devleti ilkesi gereği sınırları keyfilik yasağı tarafından belirlenmektedir.[45] Her ne kadar CMK m. 173 sadece soruşturma yer olmadığı kararına karşı bir itiraz yolu öngörülmüşse de olası bir itiraz durumunda m. 173/2' de itiraz dilekçesinde soruşturmanın açılmasını gerektirebilecek olaylar ve delillerin belirtilmesi gereği vurgulanmıştır. İtirazı değerlendirecek sulh ceza hakimliği soruşturma açılması için gerekli başlangıç şüphesinin var olup olmadığını denetleyecektir.[46] Ayrıca lekelenmeme hakkı bakımından soruşturma açılması kararlarına karşı bir itiraz yolu düzenlenmesinin gerekli olduğunu düşünmekteyiz.[47]

---

43 "Başlangıç şüphesi bulunmamasına, genel ve soyut şüphe olmasına rağmen soruşturmanın başladığının kabul edilmesi ve koruma tedbirlerine başvurulması da keyfilik niteliği taşıyacak ve hukuka aykırılık oluşturacaktır.", **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 159.

44 HK-StPO-**GERCKE**, § 152 Kn. 11; BGHSt 15, 158; MükoStPO-**PETERS**, § 152 Kn. 37.

45 **HOVEN**, s. 363.

46 **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 190.

47 Hali hazırda CMK m. 173'te düzenlenen SYOK kararına karşı itiraz durumunda hakkında SYOK kararı verilen kişiye yargısal yoldan bildirim yapılmamasının kişisel verilerin korunması ilkesine, çekişmeli yargılama ilkesine, silahların eşitliği ve adil yargılanma hakkına aykırılık teşkil ettiği belirtilmektedir, **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 191, 192.

Bununla birlikte yeni düzenlemenin bir sonucu olarak adli makamların iletilen suça ilişkin haberin başlangıç şüphesi yoğunluğuna ulaşmadığı fakat "ihbar ve şikâyet konusu fiilin suç oluşturmadığının bir araştırma yapılmasını gerektirmeksizin açıkça" anlaşılmıyorsa durumun açıklığa kavuşturulması için bir araştırma yapma ihtiyacı söz konusu olabilecektir. Bu soruşturmanın ön aşamasında özellikle savcılığın yapabileceği işlemlerin, bu noktada başlangıç şüphesinin varlığına bağlı koruma tedbirleri veya soruşturma usullerine başvurulamayacağı aşikâr olmakla birlikte,[48] (bilgi edinme vs.) kanunda düzenlenmesi gerektiğini düşünmekteyiz.

Başlangıç şüphesinin varlığının üç unsura bağlı olduğu kabul edilmektedir. İlk olarak bir suçun işlendiği ihtimaline delalet eden somut emarelerin bulunması gerekmektedir. Sonrasında bu somut emareler kriminalistik biliminin tecrübeleri doğrultusunda yorumlandığında, bir suç tipinin unsurlarının gerçekleşmiş olmasının ihtimal dahlinde görünmesi gerekmektedir. Son olarak ise, değerlendirmeye konu hal bir bütün olarak ele alındığında, kovuşturulabilir bir suçun işlendiği ihtimalinin bulunduğu neticesine ulaşılması gerekmektedir.[49]

1. Bir Suçun İşlendiğine Delalet Eden Somut Emareler

Adli makamlar, suç oluşturması muhtemel bir fiile bizzat tanıklık etmek suretiyle bir suçun işlendiği izlenimin veren bir hali öğrenmiş olabilecekleri gibi, basın ve diğer iletişim araçları, ihbar veya şikâyet yoluyla da böyle bir durumdan haberdar olabilirler. Fakat adli makamların bir suçun işlendiğinden haberdar olmalarının genel olarak ihbar veya şikâyet yoluyla gerçekleştiği görülmektedir. Bu durumda özellikle ihbar veya şikâyetin varlığı, tek başına ve her durumda suçun işlendiği izlenimini veren bir halin bulunduğunu göstermez. İhbar veya şikâyet, konu edindiği olaya ilişkin olarak ihbar edenin veya şikâyetçinin iddiasını içermektedir. Bu itibarla şikâyet veya ihbar sahibinin kim olduğu, güvenilir olup olmadığı önem arz etmektedir. Bu noktada

---

48 HK-StPO-**GERCKE**, § 152 Kn. 5; **AKBULUT**, Soruşturma Yapılmasına Yer Olmadığı Kararı, s. 160.

49 **WOHLERS**, s. 1316.

anonim ihbarların ayrıca değerlendirilmesi gerekmektedir. CMK m. 158/6 "soyut ve genel nitelikteki" ihbar ve şikayetlerin tek başlarına başlangıç şüphesi için yeterli olmadığını doğrudan düzenleme altına almaktadır. Yine bu bağlamda değinilmesi gereken bir diğer düzenleme 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun'un 4. maddesidir. Memur ve diğer kamu görevlileri hakkında yapılacak ihbar ve şikayetlerin Cumhuriyet başsavcıları ve izin vermeye yetkili merciler tarafından işleme konulabilmesi için gerekli şartlar 4483 sayılı kanunun 4. Maddesinde, ihbar ve şikayetlerin soyut ve genel nitelikte olmaması, kişi ve olayların belirtilmesi, konu edindiği iddiaların ciddi bulgu ve belgelere dayanması ve ihbar ve şikâyet sahibinin doğru adı, soyadı, imzası ve iş veya ikamet adresini içermesi bir zorunluluk olarak belirtilmiştir. Yine aynı maddenin 4. fıkrasında ad, soyadı, imza, ikamet adresi veya işyeri adresi gerçeğe uygun olamayan, fakat konu edindiği iddiaları "sıhhati şüpheye mahal vermeyecek belgelerle ortaya" koyan ihbar ve şikayetlerin dikkate alınması gerektiğini belirtmektedir. İhbar ve şikayetlerin dikkate alınabilmesi için aranan bu şartların sadece memurlar ve diğer kamu görevlileri bakımından değil, diğer kişiler bakımından aramamasının isabetli olacağı yerinde olarak belirtilmektedir.[50] Aslında başlangıç şüphesi yoğunluğuna ulaşan bir şüphenin varlığı bağlamında bir suç tipinin unsurlarını gerçekleştiren bir fiilin işlendiğine işaret eden[51] somut delilleri bulunmasını gerektirmesi sebebiyle, 4483 sayılı Kanun m. 4'te belirtilen ihbar ve şikayetlerin işleme konulabilmesi için taşıması gerekli hususiyetlerin bütün kişiler bakımından başlangıç şüphesinin varlığını kabulünde de geçerli olduğu yönündeki görüşe biz de katılmaktayız.

İhbarın veya şikâyetin içeriğinin akla ve mantığa uygun olması ciddiye alınabilmesi bakımından gerekli bir ön şarttır. Belirli bir kişinin kişilik özelliklerine dayanan çıkarımlar üzerinden varılan suç şüphesi başlangıç şüphesinin varlığı için yeterli değildir. Ceza muhakemesi, tehlike esasına dayalı ve suçun önlenmesini temel alan bir hukuki süreç

---

50 **ÖZTÜRK**, Bahri vd.., Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 17. Baskı, Ankara 2023, s. 603.

51 **RICKER,** s. 71.

değildir. Ceza muhakemesi, somut olgulara dayanan ve suç teşkil eden bir fiilin işlendiğine ilişkin şüpheyi aydınlatarak, maddi gerçeği ortaya koymayı amaç edinir. Esas hareket noktası bir fiildir. Bu sebeple somut olgulara dayanarak zaman, mekân ve bir insan tarafından gerçekleştirilen bir suç tipine uygun bir fiilin işlendiği ihtimalinin ortaya koyulması gerekmektedir.[52] Sırf teorik olarak mümkün bir ihtimal, belirsiz olan dayanak noktaları dayalı çıkarım ve hukuki tecrübeden yoksun bir bakış açısıyla yapılan tahminler başlangıç şüphesinin varlığı için yeterli olmayacaktır.[53]

Ceza muhakemesi, somut bir fiile dayanan şüpheyi aydınlatmayı amaç edinir. Önleyici amaçla yapılan kontroller, emniyet güçlerinin saha tecrübeleri doğrultusunda özellikle kriminal açıdan belirli kategorilere dahil edilen gruplar ve bu grupların yaşadığı bölgeler alınarak gerçekleştirildiğinde, büyük ölçüde kişilerin karakter özelikleri dikkate alınmış olmaktadır. Geçmiş davranışlar ve karakter özellikleri gibi parametreler üzerinden temellendirilen bir yaklaşım, tehlike ve tehlikelilik odaklı önleyici kolluk faaliyetleri bakımından dikkate alınabilecekse de bu perspektifin suç soruşturmasının başlatılması için yeterli kabul edilmesi, fail ceza hukuku anlayışına evrilme tehlikesini doğuracaktır. Fiil ceza hukuku anlayışı içerisinde tamamen kişilik özelliklerini esas alınarak oluşturulan bir şüphe, suç soruşturmasının başlatılabilmesi için gerekli olan başlangıç şüphesinin varlığının gerekçelendirilmesi bakımından yeterli kabul edilemez.[54]

Somut olgulara dayanan ve kriminalistik açıdan mantıksal bir tutarlık içerisinde bir suç tipinin unsurlarının gerçekleşmiş olabileceğine işaret eden bir durumun kabulü için, sadece teorik bir ihtimale işaret ve kriminalistik belirsizliğe neden olan olgular yeterli kabul edilemeyecektir. Tanığın, yapacağı açıklamaları ileride kendisi veya aile bireyleri aleyhine sonuç doğurabileceği gerekçesiyle bilgi vermekten kaçınması veya DNA analizi için örnek vermemesi tek başına suç

---

52 **WOHLERS**, s. 1317.

53 **RICKER**, s. 75-76.

54 **WOHLERS**, s. 1317.

işlendiğine işaret etmeyen belirişiz ihtimaller ortaya koyan olgulara örnek olarak gösterilebilir.[55]

Bir davranış, kendisi suç oluşturmasa bile, başkaca olgularla birlikte değerlendirildiğinde, bir suçun işlendiğine ilişkin şüpheyi destekleyici bir mahiyette dikkate alınabilir. Fakat bu davranış, tek başına başlangıç şüphesinin varlığını kabul etmek için yeterli olmayacaktır. Bu durumda, suç teşkil etmeyen bir fiil, ancak diğer somut olgular ve emarelerle bir bütün olarak değerlendirildiğinde, kriminalistik açıdan cezalandırılabilir bir fiilin işlenmiş olabileceğine işaret etmesi halinde, başlangıç şüphesinin varlığı bakımından rol oynayabilir. Bu bakımdan, uyuşturucu madde üretiminde kullanılabilecek araç ve gereçlerin satın alınması, olağan dışı şekilde artan elektrik tüketimi ve tek başına satın alınması suç teşkil etmeyen, fakat birtakım kimyasal işlemlerden geçirildiğinde uyuşturucu madde üretiminde kullanılabilecek kimyasalların satın alınması, suç teşkil etmeyen fiiller olmakla birlikte, bir bütün olarak değerlendirildiğinde, suç teşkil eden uyuşturucu madde üretimi bakımından başlangıç şüphesinin varlığının kabulü için yeterli kabul edilebilir.[56]

Alman literatür ve uygulamasında oldukça tartışılan, Alman Federal Meclis Milletvekili Sebastian Edathy olayı,[57] başlangıç şüphesinin nahoş olsa bile suç teşkil etmeyen bir davranışın, kriminalistik tecrübe ışığında başlangıç şüphesinin varlığına delalet edip edemeyeceğinin değerlendirilmesi bakımından somut bir örnek teşkil etmektedir. Çocuklara ilişkin pornografik içerikli materyal satışı yapan bir satıcıdan 9- 14 yaş arası çıplak çocukların resimlerinin satın alınması, "çıplak çocuk resimleri satın alınması eylemi gerçekleştiren kişiler tecrübeler ışığında yasa dışı pornografik içeriklerle de ilgilenmektedir" bağıntısını yapılarak bildirimde bulunması sonucu Edathy hakkında yasa dışı çocuk pornografisine ilişkin materyalleri bulundurabileceğine ilişkin somut bir emare kabul edilmiştir. Bu "somut emare" başlangıç şüphesi olarak

---

55 MükoStPO-**PETERS**, § 152 Kn. 39; **WOHLERS**, s. 1317.

56 MükoStPO-**PETERS**, § 152 Kn. 39a.

57 **HOVEN**, s. 361.

yeterli kabul edilmiş ve hakkında soruşturma başlatılmıştır.[58] Bu durumda söz konusu ihtimali gerekçelendirme şekli savunulabilir bir temele dayanmakta mıdır sorusu başlangıç şüphesinin varlığının hukuki denetimi bakımında önem arz etmektedir.

Söz konusu olayda savcılığın başlangıç şüphesinin var olduğu sonucuna varırken yaptığı gerekçelendirme şeklinin dayandığı argümantasyon yapısı "kişi suç teşkil etmeyen, fakat ahlaki açıdan kabul edilmez görünen, 9-14 yaş arası çocukların fotoğraflarını edinmiştir. Öyleyse söz konusu kişi muhtemelen suç teşkil eden çocuk pornografisi materyalini de edinmiştir" şeklinde görünmektedir.[59] Suç teşkil etmeyen bir davranıştan, başkaca olguların varlığını aramadan suç teşkil eden bir davranışın gerçekleşmiş olması ihtimalinin bulunduğu sonucuna varmıştır. Böyle bir sonuca varmak için düşünülebilecek bir ihtimal şüphelinin karakter özelliğine dayanabilir. Hoven'ın değerlendirmelerini dikkate aldığımızda bu argümantasyonun şu şekilde yapıldığı düşünülebilir: "Kişi çocukların çıplak fotoğraflarını edinmiştir. Çocukların çıplak fotoğrafları pedofililer edinmektedir. O zaman bu kişi bir pedofilidir. Pedofililer aynı zamanda çocuklara ilişkin pornografik içeriğe sahip materyal de edinirler. O zaman bu kişide muhtemelen benzer materyaller olabilir" şeklinde yapılanmış olacaktır ki, bu somut bir olguya dayanan değil kişinin belirli bir profile kategorize edilmiş karakter özelliği üzerinden yapılan ve bu sebeple soruşturma başlatmak için savunulamaz görünen bir gerekçelendirme teşkil etmektedir.[60]

Somut olay bakımından kişi hakkında bir ceza soruşturması başlatmadan önce, kişinin ortaya çıkan bu eğilim de dikkate alınarak bir suç işlenmiş olabileceği ihtimalini destekleyebilecek başkaca somut dayanak noktalarının bulunup bulunmadığına ilişkin genel bir araştırma yapılması gerekecektir.[61] Ortadaki somut olgu, Alman Ceza Kanunu'na göre suç teşkil etmeyen bir davranıştır. Çocukların yer aldığı pornografik içerik bulundurmaya yönelik başlangıç şüphesinin varlığı için yeterli

58 **HOVEN**, s. 362.

59 **HOVEN**, s. 361,362.

60 **HOVEN**, s. 365, 366.

61 **HOVEN**, s. 366.

değildir.[62] Değerlendirmeye konu olgu, tek başına dikkate alındığında sadece kişinin eğilimlerine dayalı bir tehlikelilik değerlendirmesine imkân vermektedir.

Başlangıç şüphesinin varlığı kabul edilmese dahi, yapay zekâ destekli programların önleyici kolluk faaliyetleri kapsamında yürütülen araştırmalarda kullanıldıklarında, dijital ortamda belirli ölçüde otonom[63] bir şekilde verileri kısa sürede işleyerek çeşitli çıktılar üretebilmektedirler. Çıktıları doğrultusunda, belirli kişi veya kişilere ilişkin değerlendirme arz eden çıktılar ortaya koyabilmektedirler. Bu çıktılar belirli kişi veya kişilere yönelik somutlaşmış suç şüphelerine işaret edebilmektedir. Bu durumda, yapay zekâ destekli sistemlerin somut olarak belirli birey veya bireylere yöneldiği andan itibaren, güvenceli bir sistem oluşturmak için, soruşturma öncesi savcının değerlendirmesinde bir adli süreç kabul edilmesi gerekli görünmektedir. Savcıların onayıyla ve kontrolünde devam eden bilgi edinme, somut bir suç şüphesinin varlığını destekleyen başkaca emarelerin olup olmadığı ve bu bağlamda başlangıç şüphesi düzeyine varan bir şüphe derecesinin mevcut olup olmadığına yönelen araştırma süreci, hukuki güvencelerin sağlanması bakımından elzem gözükmektedir. Bu sebeple, önleyici kolluk faaliyetleri kapsamında kullanılmak amacıyla geliştirilen yapay zekâ destekli programlar, bunlar aracılığı ile gerçekleştirilen analizler sonucunda elde edilen çıktılar somut bir kişiye işaret ettiği andan itibaren veri işleme faaliyetlerine devam edilebilmesini savcının onayına bağlayacak şekilde tasarlanmalıdır. CMK m. 158/6'da SYOK kararı verilmesini gerektiren hallere ilişkin düzenlemeden hareketle, soruşturma öncesinde bir ön değerlendirme aşamasının varlığı kabul edilebilir. Bununla birlikte bu ön aşamanın yapay zekâ teknolojilerinin

---

62 **WOHLERS**, s. 1319; MükoStPO-**PETERS**, § 152 Kn. 39b.

63 **ERCAN**, Cannur: "Robotların Fiillerinden Doğan Hukuki Sorumluluk: Sözleşme Dışı Sorumluluk Hallerinde Çözüm Önerileri", Türkiye Adalet Akademisi Dergisi, Sayı: 19, 2019, s. 20; **CİĞER**, Selim, Yeni Tip Gemilerin İşleyiş Esasları Bakımından Otonomi Kavramı ve IMO'nun Otonom Gemi Kategorileri Üzerine Düşünceler, İstanbul Hukuk Mecmuası, Cilt: 82, Sayı: 4, 2024, s. 1142; **ÇELİK**, Dursun, Tam Otomatikleştirilmiş İdari İşlemler, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 28, Sayı: 4, Ekim 2024, s. 422.

yargı ve çevresinde kullanılması ile ortaya çıkan soruları, başlangıç şüphesi öncesi veri işlemeye dayalı dijital işlem ve araştırmaları da kapsayacak düzenlemeler de içerek şekilde yeniden düzenlenmesi gerektiği kanaatindeyiz.

2. Somut Dayanak Noktalarının Kriminalistik Tecrübe Işığında Yorumu

Tek bir delile dayalı somut olgu, bir suç tipinin unsurlarının gerçekleşmiş olabileceği sonucuna ulaşmak için yeterli olabilir. Fakat emareler, genel olarak tek başlarına başlangıç şüphesinin varlığını ortaya koymaya yetecek ölçüde delalet gücüne sahip değillerdir.[64] Bir örnekle açıklamak gerekirse evinden değerli bir eşyasının çalındığını bildirmek için gelen kişinin "eve geldiğinde çalışma odasındaki kasasının açık ve içindeki ziynet eşyasının kayıp olduğunu" belirten beyanı hırsızlık suçunun işlendiğine ilişkin başlangıç şüphesinin varlığını kabul etmek için tek başına yeterli olmayabilir. Hırsızın eve hangi yoldan girmiş olabileceği, evin pencere veya kilitlerinde bir zorlama olup olmadığı, komşulardan etrafta şüpheli birini gören olup olmadığı, varsa kamera kayıtları gibi diğer hususların da sorgulanması gerekir. Bu noktada yapılacak kriminalistik değerlendirme elbette istatistiki verilere dayalı tecrübelere dayanacaktır. Dolayısıyla pozitif bilimlerin sıkça başvurduğu tümevarım yöntemi[65] kullanarak yapılan ve bu sebeple de yanlışlanma riski yüksek bir çıkarımdır. Tek tek somut olgulardan yola çıkılarak bir suçun işlenmiş olabileceği sonucuna ulaşılmaktadır. Başlangıç şüphesinin varlığı bakımından değerlendirilen somut olguların zorunlu olarak tek bir sonucu desteklemesi gerekmemektedir. Önemli olan, somut olayda olgu veya olgulardan, kriminalistik tecrübe ışığında bir suç tipinin unsurlarının gerçekleşmiş olabileceği yönünde yapılan çıkarımın mantıksal açıdan tutarlı olmasıdır. Diğer bir ifadeyle, çıkarımın makul

---

64 **WOHLERS**, s. 1317.

65 Bu yöntem hakkında bkz. **SEROZAN**, Rona, Hukukta Yöntem-Mantık, 3. Bası, İstanbul 2024, s. 37.

üçüncü kişiler tarafından anlaşılabilir, gerekçeleri bakımından doğrulanabilir ve bu suretle denetlenebilir olması gerekir.[66]

Kriminalistik verilerin ortaya koyduğu belirleyici istatistiki korelatif ilişkiler, somut olguların değerlendirilmesinde elbette dikkate alınabilir; fakat istatistiksel verilerin, somut olgulardan hareketle başlangıç şüphesinin varlığını kabul etmek bakımından yegâne dayanak olarak kullanılması durumunda, yürütülen araştırma "*balık yakalamak için rastgele bir olta atmak*" (*fishing expedition*)[67] eyleminden farklı görünmeyecektir. Vergi kaçırma bakımından (Steuerhinterziehung) bir örnek vermek gerekirse, vergi kaçırmak maksadıyla veya finansal kaynağın menşeini gizlemek amacıyla bazı kişilerin finansal işlemleri, nakit veya kıymetli evrak teslimi suretiyle banka gişeleri, finans kuruluşları, para transfer ofisleri veya serbest depolar üzerinden gerçekleştirdikleri bilinmektedir. Fakat bu istatistiki veri, tek başına, söz konusu işlem nedeniyle vergi kaçakçılığı suçunun işlenmiş olabileceği yönünde başlangıç şüphesinin varlığı için yeterli olmayacaktır.[68] Kişinin ancak "tezgah üstü" (Tafelgeschäfte**)** olarak adlandırılan işlemlere, gizleyici veya örtülü yöntemler çerçevesinde başvurduğuna ilişkin somut emarelerin bulunduğu ortaya konulabiliyorsa, bu emareler vergi kaçakçılığı suçunun işlenmiş olabileceğine ilişkin başlangıç şüphesinin kabulü için yeterli bir dayanak oluşturabilecektir.[69] Bu noktada önemli olan, istatistiksel verilere dayalı kriminalistik tecrübenin ortaya koyduğu bir davranış biçimi ile bir suçun işlenmesi arasındaki ilişkinin başkaca somut olgularla desteklenmesidir. Yine bir örnekle somutlaştırmak gerekirse, otomatik bilgi değişiminin kabulünden önce İsviçre bankalarının, yabancı banka müşterilerinin mal varlıklarını saklamaları ve kendi ülkesinde vergilendirmeden kaçmaları için cazip finans kuruluşları olduğu bilinmektedir. Ancak bir İsviçre bankasında hesap sahibi olmak, vergi kaçırma fiili bakımından başlangıç şüphesi için yeterli

---

66 **WOHLERS**, s. 1317, 1318.

67 **WOHLERS**, s. 1318.

68 **HOVEN**, s. 361.

69 BGH 15.6.2001- VII B 11/00, NJW 2001, 2997; BVerfG 11.3.2002-2 BvR 972/00, NJW 2002, 1940.

kabul edilemeyecektir. Kişinin bir İsviçre bankasında hesap sahibi olmasının yanında, para transferlerinde karmaşık işlem zincirleri kullanma, küçük parçalar halinde büyük işlemler gerçekleştirme (Smurfing) veya paravan hesaplar kullanma gibi maskeleme işlemlerine de başvuruyorsa, bu durumda başlangıç şüphesinin varlığı kabul edilebilecektir.[70]

3. Kovuşturulması Mümkün Suç

Ceza muhakemesi, mevcut somut dayanak noktalarının kriminalistik tecrübe ışığında değerlendirilmesi sonucu, somut veya somutlaştırılabilir bir suçun işlenmiş olabileceğine ilişkin şüphenin yenilmesini hedeflemektedir. Ceza muhakemesinin amacı, önce başlangıç şüphesinin varlığını ortaya koyan somut dayanak noktalarının tespiti; başlangıç şüphesinin varlığı durumunda soruşturma aşamasında kamu davası açılması için gerekli yeterli şüphenin bulunup bulunmadığının tespiti; yeterli şüphenin varlığı durumunda açılan kamu davasıyla birlikte sanığın kendisine atfedilen suçu işlediğinin hukuka uygun delillerle sabit olup olmadığının belirlenmesi suretiyle maddi gerçeği araştırmaktır.[71] Savcılığın başlangıç şüphesinin var olduğu yönünde değerlendirme yapmasıyla başlayacak olan soruşturma evresinin amacı, kamu davası açılabilmesi için "yeterli şüphenin" mevcut olup olmadığının tespitidir.[72] Adli makamlara gelen şikayet veya ihbara konu edilen olgu, herhangi bir suç tipinin unsurlarıyla uyuşmuyorsa, bu noktada kovuşturulması mümkün bir suç söz konusu olmadığı için kamu

---

70 **WOHLERS**, s. 1318; BVerfG 2 BvR 1372/07, 17.2.2009. Yine Almanya'da kişinin kendi isteğiyle para karşılığında cinsel ilişkide bulunması (Fuhuş/Prostitution) belirli yasal düzenlemeler kapsamında yasaldır. Bu şekilde maddi gelir elde etme ile vergi kaçırma (Steuerhinterziehung) suçunun işlenmesi arasında belirgin bir istatistiksel korelasyon bulunmaktadır. Fakat kişinin maddi gelir karşılığı cinsel ilişkide bulunması söz konusu suç bakımından tek başına başlangıç şüphesine ulaşmak için yeterli olmayacaktır, **HOVEN**, s. 367.

71 Bu bağlamda ceza muhakemesinin yegâne amacının maddi gerçeğin aydınlatılması olduğunun söylenemeyeceğini düşünmekteyiz. Aynı yönde, **YURTLU**, Fatih, Güncel Kararlar Işığında Önleme Araması Neticesinde Elde Edilen Delillerin Hukuka Uygunluğu Üzerine Bir Değerlendirme, AndHD 11 (1), Ocak 2025, s. 289, 290.

72 **ÖZBEK/DOĞAN/BACAKSIZ**, s. 174.

davasının açılması için yeterli şüphenin bulunup bulunmadığını araştırmak anlamsız olacak; başlangıç şüphesinin varlığından bahsetmek etmek mümkün olamayacaktır.[73]

Bu noktada ifade etmek gerekir ki, suç tipinin objektif unsurlarının gerçekleşmiş olabileceğine ilişkin somut dayanak noktaları mevcutsa, sadece failin bilinmemesi, subjektif unsurun gerçekleşmemiş olması ihtimali, hukuka uygunluk sebebinin veya kusurluluğu ortadan kaldıran nedenlerin somut olayda bulunması ihtimali, başlangıç şüphesinin varlığını kabule engel teşkil etmeyecektir.[74] Yine muhakeme şartlarının eksikliği, başlangıç şüphesinin varlığını kabule engel teşkil etmez. Bu durumda savcılık soruşturmayı başlatacaktır. Ancak savcılık, öncelikle muhakeme şartının eksikliğinin giderilmesine yönelik girişimlerde bulunmalıdır. Bir örnekle açıklamak gerekirse, soruşturulması ve kovuşturulması şikâyete bağlı bir suçun işlendiğine ilişkin somut dayanak noktalarının varlığı halinde savcılık soruşturmayı başlatacaktır. Fakat mağdurun şikâyet hakkını kullanıp kullanmayacağının belirlenmesi için kendisine bilgi verilecek; eğer şikâyet şartı gerçekleşmezse, soruşturma sona erdirilecektir.[75] Eğer şikâyet yapılmamış ve şikâyet süresi geçmişse, muhakeme engelinin mevcudiyeti açıkça ortaya çıkmış olacağı için soruşturma başlatılmamalıdır.[76]

C. Başlangıç Şüphesi Öncesi Önleyici Kolluk Faaliyetlerinde Yapay Zekâ Destekli Sistemlerin Kullanımı

1. Genel Bir Bakış

İdari kolluk faaliyetleri kural olarak bir suç şüphesinin henüz doğmadığı veya kanunun ifadesiyle "bir suçun işlendiği izlenimini veren hâlin yetkili makamlarca öğrenilmesinden" önceki evrede söz konusu olan ve kamu düzenini sağlamayı ve suçun vuku bulmasını önlemeyi amaçlayan kolluğa tanınmış önleyici yetkilerdir. Adli kolluk- idari kolluk ayrımı bakımından faaliyetin taşıdığı amaç belirleyici olmaktadır.

---

73 **WOHLERS**, s. 1319.

74 **WOHLERS**, s. 1319.

75 **TURHAN**, Faruk, Ceza Muhakemesi Hukuku, Ankara 2006, s. 316.

76 **WOHLERS**, s. 1319, 1320.

Nitekim adli kolluk CMK m. 164/1' de, ilgili kanunlarla belirtilen soruşturma işlemlerini yapan güvenlik görevlileri olarak tanımlanmıştır. Yine PVSK m. 2/B'de polisin işlenmiş bir suç hakkında kanunlarda yazılı görevleri yerine getireceği, yine 3201 sayılı Emniyet Teşkilatı Kanunu m. 9/C'de adli polis tanımının "adli işlerle uğraşmak" kavramına dayandırılması ve 3201 sayılı Kanunu 12. maddesinde "adli işlere müteallik tahkikatın" "salahiyetli adli otoritelerin direktifleri" altında yerine getireceğini vurgulanması, amaçsal yaklaşımın belirleyici olduğunu ortaya koymaktadır. Soruşturma evresi CMK m. 2/e bağlamında "suç şüphesinin" kanuna göre yetkili mercilerce öğrenilmesi ile başlamaktadır. O halde, kolluk makamları ve personelinin faaliyetinin, işlendiği veya işlenmekte olduğu düşünülen belirli bir suçun soruşturulmasına yönelik olması halinde adli kolluk faaliyeti olarak kabul edilmesi doğru görünmektedir.[77]

Kolluk faaliyeti belirli ve somut bir suçun araştırılmasına yönelik değilse, genel olarak kamu düzeni korunması veya suçun işlenmesinin önlenmesi amacıyla gerçekleşiyorsa ortada önleyici (idari) kolluk faaliyetinin bulunduğunun kabulü gerekecektir.[78] Başlangıç şüphesinin var olup olmadığını takdir savcılık makamına ait olması sebebiyle, kolluk belirli bir suçun işlenmiş veya işlenmekte olabileceğine ilişkin bir hali öğrendiği andan itibaren derhal savcılığa durumu bildirmek zorundadır.[79] Kolluğun durumu savcılığa intikal ettirmeden önce, suç işlendiğine ilişkin şüphenin başlangıç şüphesi düzeyine ulaşıp ulaşmadığını araştırması gerektiğinin kabulü,[80] belirli bir suç işlendiğini düşündüren bir durumla karşılaşan kolluğun başlangıç şüphesinin varlığını ayrıca değerlendirebileceği sonucuna yol açacaktır. Oysaki bu değerlendirme savcının görevine girmektedir.

---

77 Benzer amaçsal bir sınırlama yaklaşımı savunmaktadır, **LI**, s. 51

78 Söz konusu yaklaşımın Fransa'da 1951 tarihli Baud ve Dame Noualek Kararlarında geliştirilen "belirli bir suçla ilgili olma" kriterine dayandığı yönünde, bkz. **GÖZLER**, Kemal, İdare Hukuku, Cilt II, 3. Baskı, Bursa 2019, s. 484- 489; Adli kolluğun görevi bir suçun işlenmesiyle başlar, **ÖZBEK/DOĞAN/BACAKSIZ**, s. 179, 180.

79 **TURHAN**, s. 94.

80 **YURTLU**, s. 299.

Önleyici kolluk faaliyetleri kapsamında karşılaşılan bir olgu üzerine kolluk faaliyeti, somut ve belirli bir suçun araştırmasına yöneldiği andan itibaren sürecin adli kolluk faaliyetine dönüştüğünün kabulü gerekecek ve kolluğun derhal savcılığa durumu intikal ettirmesi ve onun emir ve talimatları doğrultusunda hareket etmesi gerekmektedir. Aksi takdirde kolluk faaliyetleri kapsamında karşılaşılan durumlar belirli bir somut suçun işlendiğini düşündürdüğünde, kolluğun durumdan savcılığı haberdar etmeden önce başlangıç şüphesinin var olup olmadığını değerlendirmesi veya varlığını tespit için araştırma yapabileceği düşüncesi doğacaktır.

Uygulamada ortaya çıkan sorunlar başlangıç şüphesinin varlığının değerlendirilmesinin savcılığın görev ve yetkisinde olduğunu ortaya koyacak bir ön araştırma aşamasının somut bir kanuni düzenleme ile açıklığa kavuşturulması gereğine işaret etmektedir. Bununla birlikte kolluk faaliyetlerinin somut bir suça yöneldiği andan itibaren başlangıç şüphesinin varlığının kolluk tarafından ayrıca tespit edilmesi beklenmeksizin[81] adli bir sürece dönüşmesi gereğinin yeterince vurgulanması önem arz etmektedir.

Kolluk faaliyeti bakımından genel olarak belirleyici olan, faaliyetin somut ve belirli bir suça yönelip yönelmediği olacaktır (CMK m. 164/2, m. 161/2). Bu noktada CMUK m. 156/1'de kolluğun suçluları aramak ve işin aydınlatılması için gerekli acele tedbirleri alma yükümlülüğüne ilişkin düzenlemenin 5271 sayılı CMK'ya alınmadığını da belirtmek gerekmektedir.[82] Kolluk, kural olarak Cumhuriyet savcısının emir ve

---

81 Yine istihbarat faaliyeti, önleyici kolluk ve adli kolluk faaliyetinin uygulamada nasıl iç içe geçtiğini, çoktan belirli bir suça yönelmiş bir şüphenin varlığına rağmen önleyici kolluk faaliyeti kapsamında delil elde edilmeye çalışıldığına ilişkin bir "önleme aramasının" hukuka aykırı olduğunu yönünde, Yargıtay CGK. T. 14.02.2024, E. 2023/522, K. 2024/65.

82 Bu noktada 2007 PVSK'ya eklenen ek madde 6'nın 3. fıkrasında: "Edinilen bilgi veya alınan ihbar veya şikâyet üzerine veya kendiliğinden bir suçla" karşılaşması durumunda polisin "suçun delillerinin kaybolmaması ya da bozulmaması için derhal gerekli tedbirleri" alma yükümlülüğü getiren düzenleme bağlamında suç delillerinin kaybını ve bozulmasını engelleme noktasında göstereceği adli faaliyet bakımından Cumhuriyet savcısının ya da sulh ceza hakiminin emir ve talimatı olmadan harekete geçme yetkisinin bulunduğu ifade edilmelidir. Fakat bu, adli

talimatı olmadan, kural olarak dorudan doğruya suçu araştırma yetkisine sahip değildir.[83] Nitekim 680 sayılı KHK'nın 27. maddesiyle PVSK'ya eklenen ve 7072 sayılı Kanun m. 26 ile aynen kabul edilen 18. fıkra ile polis, "sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya" yetkili kılınmıştır. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları da polisin bu kapsamda talep ettiği bilgileri bildirmekle yükümlü kılınmıştır. Anayasa Mahkemesi, soruşturmayı yapacak yetkili başsavcılığın belirlenmesinin ve bu konudaki uyuşmazlıkların çözümünün yargı mercilerinin görevi olduğunu; soruşturma kapsamında gerekli bilgilerin Cumhuriyet savcısı tarafından istenebileceğini ve de yalnızca Cumhuriyet başsavcılığının belirlenmesi amacıyla kişisel verilere doğrudan erişim yetkisi tanınmasının demokratik toplum düzeninin gereklerine aykırı olduğunu belirterek düzenlemenin iptaline karar vermiştir.[84]

Yapılan faaliyetin belirli bir suça yönelmesi durumunda, mecburilik ilkesine dayalı olarak hukuk tarafından sıkı koşullara bağlı olarak belirlenen sınırlar dahilinde yürütülen ceza soruşturması kapsamında değerlendirilmesi yönündeki bizim de benimsediğimiz yaklaşımın[85] Avrupa Birliği Yapay Zekâ Düzenlemesi'nde (**EU Artifical Intelligence Act/AB YZD**) tanımların yer aldığı 3. maddenin 46 numaralı paragrafında yapılan ceza soruşturmasının tanımında[86] benimsendiğini

---

kolluk faaliyeti kapsamında suç aydınlatılmasında doğrudan doğruya yetkili olduğu anlamına gelmeyecektir. Düzenlemenin dolaylı olarak araştırma mecburiyeti getirdiği noktasında bkz. **ÖZBEK/DOĞAN/BACAKSIZ**, s. 186.

83 **TURHAN**, s. 93; Nitekim kolluk suçüstü hali ve gecikmesinde sakınca bulunan hallerde, Cumhuriyet savcısına erişilememesi veya olayın genişliği itibarı ile Cumhuriyet savcısının iş yükünü aşması durumunda sulh ceza hakimine de bütün soruşturma işlemlerini yapma yetkisi verilerek, kolluğun belirli bir suçun işlenmesi ihtimali ile ilgili suça ilişkin şüphenin aydınlatılmasında doğrudan doğruya araştırma yetkisine haiz olmadığı ortaya konulmaktadır, **ÖZBEK/DOĞAN/BACAKSIZ**, s. 185 186.

84 AYM, 19.2.2020, E. 2018/91, K.2010/10; **ŞAHİN/GÖKTÜRK**, s. 145, 146 (dipnot 169).

85 **LI**, s. 49, 50; **SCHULENBURG**, Johanna, Legalität- und Opportunitätsprinzip im Strafverfahren, in: JuS 2004, s. 765, 768, 769.

86 Metnin İngilizcesi: 'law enforcement' means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection

görmekteyiz. Düzenleme aslında adli ve idari kolluk faaliyetlerini de ihtiva eden İngilizcedeki "law enforcement" terimini kullanmıştır. Söz konusu terim hem kamu güvenliğini ve tehlikenin önlenmesi faaliyetlerini hem de bir suçun soruşturulması, kovuşturulması ve hükmedilen cezaların infazına ilişkin adli takibatı (Strafverfolgung) içermektedir. Kavram tanımlanırken öncelikli olarak yapılan faaliyetin konusu öncelenerek suça ilişkin olması dikkate alınarak tanımlanması sebebiyle kavramın adli takibat (**Strafverfolgung**) olarak kabulü isabetli görülmektedir. Yapılan faaliyetin belirli bir suçun soruşturulması, aydınlatılması veya kovuşturulmasına yönelik olması halinde, söz konusu faaliyetin adli kolluk faaliyeti ve ceza muhakemesinin bir parçası kabul edilmesi gerektiği görüşündeyiz.[87]

Adli kolluk ve idari kolluk teşkilatlarının birbirinden ayrılmamış olması sebebiyle, yapılan kolluk faaliyetinin niteliğinin değerlendirilmesi ancak somut olay özelinde yapılabilecek bir ayrım olarak gözükmektedir. Çalışma önleyici kolluk bağlamında kullanılan yapay zekâ destekli program ve sistemlerin kullanıldığı durumlarda başlangıç şüphesinin tespiti bağlamında ortaya çıkan problemlere odaklanmaktadır. Bu bağlamda çalışmanın devamında kullanılan teknolojiler ve bunların uygulandığı somut olaylar dikkate alınarak ayrım somutlaştırılacaktır.

2. Önleyici Kolluk Faaliyetlerinde Yapay Zekâ Kullanımına Genel Bir Bakış

Önleyici kolluk faaliyetlerinde yapay zekanın kullanımı farklı amaçlarla, farklı çıktılara ulaşmak için gerçekleşiyor olsa da bu

---

or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security, https://ai-act-law.eu/article/3/. ; metnin Almancası: "Strafverfolgung": Tätigkeiten, die von den Strafverfolgungsbehörden oder in deren Auftrag zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, durchgeführt werden", https://artificialintelligenceact.eu/de/article/3/ , https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/6_Definitionen/start.html.

87 **LI**, s. 52.

uygulamaların temelinde güvenlik güçlerinin tehlikenin ve suçların önlenmesine ilişkin görevleri kapsamında çok büyük veri yığınlarının analizi suretiyle bilgi ve bulgu edinilmesi yer almaktadır. Söz konusu yöntemler modern risk toplumunda, özelikle teknolojik gelişmelerle gündeme gelen yeni tehditlere ilişkin risklerin erken tespit edilmesi ve bunlara zamanda müdahale edilebilmesi için güvenlik güçlerine avantaj sağlayabilmektedir. Buna karşın söz konusu yöntemlerin kullanımı, temel hak ve özgürlüklere orantısız müdahale riskini de beraberinde getirmektedir.

İnsanların günlük yaşamının önemli bir bölümü yapay zekâ sistemleri tarafından işlenebilecek çok miktarda verinin üretildiği dijital ortamlarda gerçekleşmektedir. Vatandaşlar ticaret, alışveriş, finansal işlemler, sosyal iletişim, fikir ve görüş paylaşımlarını, sanatsal faaliyetlerini, hobilerini ve boş zaman aktivitelerini (oyun, medya içeriklerine ulaşım vb.) dijital ortamlarda gerçekleştirerek geride çok büyük miktarda dijital veri ve iz bırakmaktadır. Bu alanda saniyeler içerisinde çok büyük veri yığınlarını analiz ederek sonuçlara ulaşan yapay zekâ sistemleri, henüz başlangıç şüphesinin bile söz konusu olmadığı bir aşamada başta özel hayatın gizliliği ve kişisel verilerin korunması olmak üzere temel hak ve özgürlüklere yoğun ve orantısız müdahale riskini ortaya çıkarmaktadır. Söz konusu durumun ortaya çıkardığı bir diğer problem ise temel hak ve özgürlüklere müdahale edici nitelikteki PVSK m. 9 önleme araması ile PVSK ek madde 7 kapsamında belirtilen suçların işlenmesinin önlenmesi amacıyla hakim kararı veya gecikmesinde sakınca olan hallerde kanunda yetkili kılınan idari amirin yazılı emriyle yapılabilecek iletişimin ve internet veri trafiğinin denetlenmesine yetkilerin kullanılması suretiyle kolluk kuvvetlerinin çok kapsamlı ve bilgiye çok hızlı bir şekilde, erişim sağlayabilecek olmasıdır. Üstelik bu bilgilerin hatalı olma veya insan tarafından kavranması ve açıklanması güç korelasyonlara dayanma ihtimali de bulunmaktadır. Bu durumda demokratik hukuk devletinde hukuki güvenliğin sağlanması bakımından şeffaflık ve denetlenebilirliğin sağlanması için gerekli

istihbarat faaliyetleri ile önleyici kolluk faaliyetlerinin ayrılması prensibinin[88] aşındırılması riski oldukça yüksektir.

Ayrım prensibinin (**Trennungsgebot**) bilişimsel boyutu kendi kaderini tayin hakkı bağlamında istihbarat teşkilatları ve önleyici kolluk makamlarının sahip olduğu verilerin birbirinden ayrılması ve ağır saldırılara yönelik operasyonel görevlerin yerine getirilebilmesi amacıyla müdahale eşiğinin aşılması (**Eingriffsschwelle**) sebebiyle kabul edilen istisnalar dışında, söz konusu kurumlar arasında veri paylaşımının da engellenmesini gerektirmektedir.[89] Ayrım prensibini gerekçesiyle birlikte veciz bir şekilde ifade eden ve çokça atıf yapılan *Gusy*'in sözleriyle, "kim hızlı bir şekilde her şeyi bilebiliyorsa, her şeyi yapmaya yetkili olmamalıdır ve kim hızlı bir şekilde her şeyi yapabiliyorsa, her şeyi bilmeye yetkili olmamalıdır".[90]

Bu bağlamda KVKK kişisel verilerin işlenmesine ilişkin sınırlamaların belirli bir ölçüde veya tamamen uygulanmayacağı hallerin düzenlendiği KVVK m. 28'in /1 (ç) hükmünde kanun tamamen uygulanmayacağı haller içerisinde milli savunma, milli güvenlik, kamu güvenliği ve ekonomi güvenliğin sağlamasına yönelik önleyici, koruyucu ve istihbarı faaliyetler kapsamında kanun gereği yetkili kişi ve kurumlar tarafından işlenmesini saymıştır. Kanunda istihbarat faaliyetlerinin tanımının yer almaması, önleyici faaliyetler ile istihbarat faaliyetlerinin iç içe geçtiği düzenlemeler bulunması ve bu faaliyetler kapsamında elde edilen verilerin köklü amaç değişimine rağmen aynı veri tabanlarının kullanılması veya veri paylaşımının söz konusu olması sebebi kullanılmaya devam edilmesini gündeme getirecektir. Bu kapsamda kişisel verilerin elde edildiği amaca uygun olarak kullanımı, veri sahibine itiraz hakkı (insan tarafından değerlendirilmeyi talep etme hakkı) ve

---

88 **GRAULICH**, Kurt, Zum Trennungsgebot im Sicherheitsrecht, in: Digitalisierung, Globalisierung und Risikoprävention, Festschrift für Ulrich Sieber, ENGELHART, Marc/KUDLICH, Hans/VOGEL (edt.), Benjamin, 2. Baskı, Berlin 2022, s. 929, 944.

89 **GRAULICH**, s. 944, 945.

90 **GUSY**, Christoph, Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV), Vol. 77, No. 3 (1994), s. 242, 243.

suçla ilgisi olmayan bireylere ilişkin verileri ayrı değerlendiren güvencelerin sağlanması gibi hususlar kişilik hakkının bir uzantısı olan "bilişimsel kaderini tayin hakkının" bir gereğidir.

Kişisel verilerin suçun aydınlatılması ve önlenmesinde kullanımının, kişisel verilerin korunmasına ilişkin getirilen genel koruma rejimi dışında bırakılması, suçun aydınlatılması ve önlenmesi amacıyla yürütülen faaliyetlerin gereği gibi yapılabilmesi açısından gerekli görülebilir. Fakat bu, suçun aydınlatılması ve önlenmesi amacıyla kullanılacak kişisel verilerin bütün güvencelerden yoksun bırakılabileceği anlamına gelmemektedir. Bu noktada KVKK m. 28'de yer alan, kişisel veriler için öngörülen koruma rejiminin dışında tutulan hallerin belirsizliğe yol açmayacak şekilde yeniden ele alan ve bu bağlamda işlenen kişisel veriler bakımından, suçun aydınlatılması ve önlenmesi amacıyla yürütülen faaliyetlerin özelliklerini de dikkate alan, bu alana özgü bir koruma rejimi öngören yeni bir düzenlemeye ihtiyaç olduğu açıktır.[91] Aksi takdirde, ilgili veri işleme faaliyetlerine dayalı çıktıların dikkate alındığı karar süreçlerinde, delillerin elde edilmesi ve değerlendirilmesinde denetlenebilirlik, şeffaflık ve delillerin değerlendirilmesinde doğrudan doğruyalık gibi prensiplerin göz ardı edilmesinin adil yargılanma hakkının ihlaline yol açması muhtemel görünmektedir. Söz konusu düzenleme yapılırken, kişisel verilerin suçların önlenmesi ve adli amaçlarla yetkili makamlar tarafından işlenmesi durumunda, AB Genel Veri Koruma Tüzüğü[92]'nde öngörülen koruma rejiminin dışında, fakat ilgili faaliyetlerin sağlıklı bir şekilde

---

91 **ERDOĞAN**, s. 144, **KIZILIRMAK**, s. 257, 258.

92 Kişisel verilerin korunması gündeme geldiğinde AB bakımından temel metin olarak AB Genel Veri Koruma Tüzüğü (General Data Protection Regulation, GDPR) karşımıza çıkmaktadır. AB Genel Veri Koruma Tüzüğü kişisel verilerin korunmasına ilişkin genel nitelikte bir düzenleme olarak, kişisel verilerin işlenmesinin söz konusu olduğu özel ve kamusal bütün süreçlere ilişkin temel prensipleri, kişisel verileri işleyenlerin yükümlülüklerini ve kişisel veri sahiplerinin haklarını düzenlemektedir, **ERDOĞAN**, s. 85; **ERCAN**, Cannur, Dijital İçerik ve Dijital Hizmet Sözleşmeleri, Ankara 2024, s. 43.

gerçekleştirilmesine engel olmadan gerekli güvenceleri sağlamayı hedefleyen 2016/680 sayılı Direktif dikkate alınabilecektir.[93]

a. Önleyici Kolluk ve İstihbarat Faaliyetlerinden Elde Edilen Deliller Başlangıç Şüphesinin Tespitinde Kullanılabilir Mi?

İstihbarat faaliyetleri yürüten kurumların operasyonel kabiliyetleri ve müdahale yetkileri farklı amaçlara dayanmasına rağmen, adli makamların sahip olduğu yetkilere benzerlik gösterdiği gibi bunları da aşabilmektedir. Somut olgulara dayalı bir suç şüphesinin veya önleyici kolluk faaliyetleri kapsamında gündeme gelen somut bir güvenlik tehlikesinin dahi söz konusu olmadığı bir aşamada, Trojan programları kullanarak takip edilen kişinin dijital verilerine ulaşılması, iletişimin izlenmesi, teknik araçlarla izlenmesi ve stratejik nitelikteki kablo hatları ve yayın frekanslarının izlenmesi yoluyla veri ve sinyal trafiğinin kitlesel olarak izlenmesi gibi, muhataplarının kendilerini savunma imkanının bile bulunmadığı yöntemlere başvurulması söz konusu olmaktadır. Dolayısıyla bu yöntemlerle başlangıç şüphesinin öncesinde elde edilen verilerin, başlangıç şüphesine dayanak oluşturmak veya başlatılan ceza soruşturmasında kullanmak için ceza muhakemesi alanına aktarılması, başlangıç şüphesinin özgürlükleri koruyucu etkisini geçersiz kılma tehlikesini ortaya çıkarmaktadır.[94] Yapay zekâ destekli program ve sistemlerin kullanılması ve belli tehlike alanlarında kurumlar arası veri paylaşımı başlangıç şüphesinden bağımsız ceza soruşturması tehlikesini büyütmektedir. Bu durumda yeni gelişmeleri dikkate alarak ceza soruşturması kapmasında gündeme gelen hukuki güvencelere dayalı düzenleme ihtiyacı kendini göstermektedir.

Bu bağlamda PVSK Ek m. 7'de belirtildiği gibi "ülke seviyesinde ve sanal ortamda istihbarat" faaliyetinde bulunarak toplanan veriler ve ek m. 7/1'de belirtilen amaçlarla "telekomünikasyon yoluyla yapılan iletişim denetlenmesi", "internet bağlantı adresleri ile internet kaynakları arasındaki veri ve sinyal trafiğinin denetimi ve kaydı" veya suçların önlenmesi amacıyla istihbarat amacıyla "teknik araçlarla izleme" yoluyla

93 **KIZILIRMAK**, s. 247- 249.

94 **WOHLERS**, s. 1323, 1324.

elde edilen verilerin, sadece söz konusu işlemlerin hakim kararına veya kanunda öngörülen hallerde yetkili makamın yazılı emrine dayanması nedeniyle dayanması sebebiyle ceza muhakemesinin herhangi bir aşamasında kullanılması kabul edilmemelidir. Nitekim Yargıtay da istihbaratı amaçlı yapılan iletişimin tespit edilmesi, dinlenmesi ve sinyal bilgilerinin değerlendirilmesi yoluyla elde edilen bulguların ceza yargılamasında delil olarak kullanılamayacağına; fakat ceza soruşturmasının başlatılmasına dayanak teşkil edebileceğine karar vermiştir.[95]

Ülkemiz yargı pratiği de dikkate alınarak, söz konusu verilerin hangi şartlarda başlangıç şüphesinin varlığına hükmedilmesine dayanak olarak kullanabileceğinin, hangi durumda ceza muhakemesi kapsamında alınan kararlarda ve nihayet hükümde dayanak teşkil edebileceğinin yasal olarak düzenlenmesine ihtiyaç olduğunu düşünmekteyiz. Adli makamlar ile emniyet ve istihbarat birimleri arasındaki ortak veri kullanımı demokratik hukuk devletinde belirli sınırlar dahilinde kalmalıdır. Elbette ki aktüel bir terör tehdidinin söz konusu olduğu durumlarda, henüz suçun ön alanında bulunulmasına rağmen tehdidin engellenmesi için gerekli çıkarımları yapmaya yönelik önemli bilgilerin edinilmesi, ortak veri tabanını kullanılmasına duyulan ihtiyacı gerekçelendirebilecektir. Fakat bu şekilde emniyet ve istihbarat birimlerinin yürüttüğü hukuka uygun faaliyetler sonucunda elde edilen verilerin ve bu verilere dayalı çıkarımların, herhangi bir normatif ölçüte bağlı olmadan, çalışmanın konusu bakımından özelleştirdiğimizde başlangıç şüphesinin varlığını kabul etmek bakımından kullanımı, ancak şekle indirgenmiş bir hukuka uygunluk anlayışı içerisinde savunulabilecektir. Söz konusu veri paylaşımını ve elde edilen verilerin ceza yargılamasında sonraki kullanımına ilişkin normatif ölçütlerin ülkemizde yasal veya içtihadı olarak ortaya konulamamış olduğunu görmekteyiz.

Yargıtay CGK, MİT Kanunu m. 4/1-i kapsamında MİT'in, "*dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber*

---

95 CGK, 17.05.2011, 9/93-95 karar için bkz. **ÜNVER/HAKERİ**, s. 465.

güvenlik konularında" elde ettiği istihbaratı "gerekli kuruluşlara ulaştırmak" görevi çerçevesinde, faaliyetleri sırasında elde ettiği veya rastladığı "terör suçları, sınır aşan örgütlü suçlar veya siber suçlara konu" bilgi, belge, veri ve materyalleri adli makamlara bildirmesini, isabetsiz olarak, bu materyallerin "soruşturma veya kovuşturma evrelerinde delil olarak kullanılması için adli makamlarla yapılan bir paylaşım" olduğu .şeklinde değerlendirmektedir.[96]

Söz konusu düzenleme kapsamında MİT tarafından adli mercilere yapılacak bildirim, soruşturma öncesinde, başlangıç şüphesinin varlığı için gerekli koşulların bulunduğunun savcı tarafından değerlendirilmesi durumunda, ceza soruşturmasının başlatılmasında bir rol oynayabilecektir. MİT'in faaliyetleri kapsamında elde edilen bilgi, belge ve verilerin ceza muhakemesinde adli merciler tarafından talep edilebilmesin ilişkin bir istisna, sadece MİT Kanunu Ek Madde 1'de "devlet sırlarına karşı suçlar ve casusluk" suçları bakımından kabul edilmiştir. Bu suçlara ilişkin olarak adli merciler tarafından talep edilen bilgi, belge veri ve kayıtların ceza muhakemesinde delil mahiyetinde delil olarak kabul edilip edilemeyeceği savcılık ve mahkemeler tarafından değerlendirilecektir. Söz konusu suçların önlenmesi ve aydınlatılması, adli mercilerin operasyonel kabiliyetlerini aşabilecek ve bu bağlamda müdahale eşiğinin aşılaması söz konusu olabilecektir. [97]

Belirttiğimiz bu gerekçelerle, istihbarat amacıyla yapılan iletişim tespiti ve denetlenmesi sonucunda ulaşılan veri ve bulguların, bunların kullanımını meşru hale getirecek normatif ölçütlere dayalı olarak bir değerlendirmeye tabi tutulmaksızın başlangıç şüphesinin varlığı bakımından ceza soruşturmasına dayanak kabul edilmesini,[98] başlangıç şüphesinin kişi özgürlüğünü koruyucu fonksiyonunu ortadan kaldırdığı ve masumiyet karinesinin ihlali riskini beraberinde getirdiği gerekçesiyle isabetsiz bulmaktayız. Böyle bir durumda istihbarat ve emniyet birimleri

---

96 Yargıtay CGK, 26.9. 2017, E.2017/16-959, K. 2017/370.

97 Aynı yönde bkz., **BİRTEK**, Fatih, Ceza Muhakemesi Bakımından MİT Tarafından Elde Edilen İstihbarı Bilgilerin Delil Niteliği, in: Hukuk Devletinde İstihbarat, BİRTEK Fatih (edt.), Ankara 2025, s. 705-707.

98 CGK, 17.05.2011, 9/93-95, bkz. **ÜNVER/HAKERİ**, s. 465.

durumu derhal savcılığa bildirmekle yükümlüdür. Kanaatimizce savcılık, istihbarat amaçlı dinleme kapsamında elde edilen ve bir suçun işlenmiş olabileceği ihtimallini ortaya koyan bulguları tek başına yeterli kabul etmeyip, bu bulguları destekleyen başkaca olguların da bulunması halinde başlangıç şüphesinin varlığını kabul ederek soruşturmayı başlatmalıdır.

Bu noktada, istihbarat veya tehlike ve suçun önlenmesi amacıyla elde edilen delil ve bulguların ceza muhakemesinde kullanılabilmesi bakımından mukayeseli hukukta amaç değişikli hususuna odaklanılmaktadır. Tamamen farklı amaçla yürütülen bir faaliyet kapsamında elde edilen delillerin, elde edilmesi tamamen yasal yollarla gerçekleşmiş olsa bile, suçun şüphesinin aydınlatılmasını ve maddi gerçeğin hukuka uygun yöntemlerle ortaya çıkarılmasını amaç edinen ceza muhakemesinde kullanılması, gündeme gelecek köklü amaç değişimi göz önünde bulundurulduğunda, ancak bu amaç değişikliğini meşru hale getirecek bir normun varlığıyla meşru olabileceğini kabul etmektedir. Ceza muhakemesi kapsamında gerekli şüphe derecesi söz konusu olmadığı takdirde başvurulması mümkün olmayan yöntemlerle elde edilmiş bu bilgi, bulgu ve delillerin adli makamlara iletilmesini ve ceza muhakemesinde kullanılmasını meşru hale getirecek normatif düzenlemenin ancak ağır suçların (terör suçları) söz konusu olduğu durumlarda mümkün olabilmesi gerektiği savunulmaktadır.[99] Aktüel ve büyük tehditlere karşı güvenlik sağlanması maksadıyla birlikte hareket edilmesini zorunlu kılan durumların varlığı sebebiyle oluşan istihbarat ve emniyet birimlerinin ortak veri havuzunun kural olarak oluşturulma amacıyla uyumlu amaçlar doğrultusunda kullanılması gerekir. Aksi takdirde, istihbarat ve/veya önleyici kolluk faaliyetleri kapsamından istihbarat, tehlike ve suçun önlenmesi amaçlarına matuf olarak yürütülen faaliyetler kapsamında elde edilen bilgi ve bulguların başkaca herhangi bir koşula tabi tutulmadan doğrudan ceza muhakemesinde kullanımı, soruşturmanın başlatılabilmesi için gerekli başlangıç şüphesi ile onun kişi özgürlüğünü koruyan fonksiyonunun içinin boşaltılmasına ve başlangıç

[99] **WOHLERS**, s. 1323, 1324.

şüphesinin tamamen şekli bir hal almasına neden olacaktır.[100] Dolayısıyla, bunların ceza muhakemesinde kullanılmasının yasak olması genel kural olarak kabul edilmelidir.[101]

Alman ceza hukukunda da konuya ilişkin doğrudan hukuki düzenlemeler yer almamaktadır fakat mahkeme kararları ile geliştirilen ölçütlere dayalı uygulama istikrar kazanmıştır. Alman Anayasa Mahkemesinin terörle mücadele kapsamında; emniyet birimleri ile istihbarat birimleri arasında veri paylaşımı, verilerin işlenmesi ve ceza soruşturmasında kullanımına ilişkin düzenlemeleri değerlendirdiği kararında; veri paylaşımının ayrım prensibine aykırı olmaması için emniyet birimlerinin operasyonel faaliyetlerinin müdahale eşiğinin aşılmış olması gerektiği belirtilmiştir. Söz konusu müdahale eşiği, tehlike ve korunması gündeme gelen hukuki değer dikkate alınarak belirlenecektir. Mahkemeye göre, genişletilmiş veri kullanımının, kişinin hayatı, vücut bütünlüğü ve özgürlüğü ile Federal Devletin veya bir eyaletin varlığı veya güvenliği gibi önemli hukuki değerlerin korunmasına hizmet etmesi gerekir. Yine yeterince somutlaştırılmış bir tehlikenin varlığı da aranmalıdır. Fakat bu verilerin gnişletilmiş kullanımına izin veren düzenlemenin norm açıklığını sağlayacak şekilde yeterince belirli olarak ortaya koyması gerekir. Bu bağlamda istihbarat verilerinin güvenlik güçleri tarafından kullanılmasında müdahale eşiğinin (**Eingriffsschwelle**) aşılmış olması, erişim sağlanan verilerin

---

100 **WOHLERS**, s. 1324.

101 İsviçre Ceza Muhakemesi Kanunu m. 141 (İCMK) delillerin değerlendirilmesine ilişkin düzenlemede sadece adli makamlar tarafında elde edilen delillere ilişkin hususlar düzenlenmektedir. Bu yüzden güvenlik birimleri vasıtasıyla elde edilen delillerin ceza muhakemesinde kullanılmasına ilişkin farklı görüşler söz konusu olmaktadır, **WOHLERS**, s. 1324. Milli İstihbarat Teşkilatının (MİT) faaliyetleri kapsamında elde edilen bilgilerin, teşkilata özgü "gizli çalışma usul, prensip ve tekniklere" dayalı olarak herhangi bir şüphe derecesine bağlı olmaksızın, personelin bilgi ve tecrübesi çerçevesinde elde edilmiş olması sebebiyle, bunların hukuka uygun şekilde elde edilip edilmediğinin ve "sağlamlık ve güvenilirliğinin" sorgulanması ve tartışılması mümkün değildir Yine MİT mensuplarının, MİT'in görev ve faaliyetleriyle ilgili olarak tanık olarak dinlenmesi kural olarak mümkün değildir (MİT Kanunu m. 29); bu bilgilerin iddianamenin düzenlenmesinde esas alınması, CMK'da kişi hak ve hürriyetlerini korumayı amaçlayan güvenceleri işlevsiz hale getirecektir, bkz. **BİRTEK**, s. 703, 704.

sonraki kullanımlarının hukuka uygun olması için yeterli kabul edilemeyecektir. Özellikle elde edilen verilerin ceza soruşturması ve kovuşturmasında kullanımı için, gerekli müdahale eşiği bakımından yeterli şüphe derecesini karşılayacak şekilde, belirli bir suçun işlendiğine delalet eden somut dayanak noktalarının varlığını aranması bir zorunluluk olarak karar kapsamında dile getirilmiştir.[102]

b. Profilleme Teknolojileri, Tahmine Dayalı (Prediktif) Önleyici Kolluk Faaliyetleri (Predictive Policing)

Çalışmanın konusu bağlamında profilleme teknolojilerinin kullanımına ilişkin güncel tartışmalar özellikle suçun işlenmesinden önce tahmine dayalı kolluk faaliyetlerine[103] odaklanmaktadır. Tahmine dayalı önleyici kolluk süreçlerinin altında yatan temel kabul, suçların istatistiki bir düzen gösterdiği ve bu sebeple geçmiş suçlara ilişkin verileri dikkate alarak gelecekte işlenmesi muhtemel suçlara ilişkin tahminlerde bulunmanın mümkün olduğu düşüncesidir.[104] Tahmine dayalı kolluk faaliyeti, yapay zeka sisteminin geçmiş suçlara ilişkin verileri istatistiki olarak analiz ederek gelecekte gerçekleşmesi muhtemel suçlara ilişkin yine istatistiki olarak oluşturduğu sistem çıktılarının önleyici kolluk faaliyetlerinin icrasında dikkate alınması olarak tanımlanabilir.[105] Geçmiş

---

102 BVerfG: Datenaustausch zwischen Polizei und Nachrichtendienst („Datamining“) nach Antiterrordatengesetz, BVerfG (1. Senat), Beschluss vom 10.11.2020 – 1 BvR 3214/15, (116-120).

103 Kavram için bkz. **ERDOĞAN**, s. 44. Aynı olgu “proaktif polislik” kavramı ile de ifade edilmektedir, **ATLI,** Turan, Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi”, NEÜHFD 2 (1) 2019, s. 12. Öngörücü polislik uygulamaları, **ATEŞ,** Hüseyin, Ceza Muhakemesi Hukuku ve Yapay Zekâ, Ankara 2025, s. 52; **İÇER,** Zafer, Yapay Zeka Temelli Önleyici Hukuk Mekanizmaları-Öngörücü Polislik, in: Yapay Zeka Temelli Teknolojiler ve Ceza Hukuku (Yapay Zeka Çalışma Grubu Yıllık Rapor 2021 İstanbul Barosu), s. 33.

104 **SIMMLER**, Monika/**BRUNNERS**, Simone/**CHEDLER**, Schedler, Smart Criminal Justice - Eine Emprische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiararbeit und Strafrechtspflege (Studienbericht), Universität St. Gallen, s. 5: https://www.alexandria.unisg.ch/server/api/core/bitstreams/2bbe3121-5d11-4662-94bc-f91657c29f54/content, son erişim 27.04.2026.

105 **PULLEN**, Jennifer/**SCHEFER**, Patricia, Predictive Policing-grundlagen, Funktionweise und Wirkung, in: Smart Criminal Justice, SIMMLER Monica (edt.), Basel 2021, s. 105.

olaylarla ilgili veri yığınlarının analizi sonucunda elde edilen istatistiki korelasyonlara dayalı oluşturulan örüntüler dikkate alınarak gelecekteki olaylara ilişkin sistem çıktılarının, tam manasıyla somut verilere dayalı bir tahminden ziyade, olasılıksal bir değerlendirmeye dayandığına dikkat çekilmesi, çalışmanın konusu bakımından önem arz etmektedir.[106]

Tahmine dayalı kolluk faaliyetleri, risk analiz sistemleri kullanılarak verilerin işlenmesi ve analiz edilmesine dayalı olarak hangi suçların hangi kişi veya kişi grupları tarafından ne zaman ve nerede işlenebileceğine ilişkin istatistiksel tahminler dikkate alınarak, uygulanacak önleyici tedbirlerle suçla daha etkili mücadele edilmesi düşüncesine dayanır.[107] Yapay zeka destekli önleyici kolluk sistemleri, kamu güvenliğinin sağlanması ve tehlikenin önlenmesi faaliyetlerinde klasik önleyici kolluk usullerine nazaran önemli ölçüde kaynak tasarrufu ve işlevsellik vaatleri sebebiyle, önleyici kolluk faaliyetlerinin yürütülmesinde son derece cazip olarak değerlendirilmektedir.[108] Fakat söz konusu sistemlerin kullanımı, yaygın bir biçimde gözetimi ve potansiyel ayrımcılık tehlikesi gibi riskler barındırması sebebiyle, aynı zamanda kişisel verilerin korunması ve bilişimsel kaderini tayin hakkı bakımından önemli bir müdahale teşkil etmektedir. Önleyici kolluk sistemlerinin tehlike ve suça ilişkin risk öngörüsünü güvenilir bir şekilde oluşturabilmesi için davranış algoritmalarının geliştirilmesi ve eğitilmesi aşamasından itibaren, öngörünün oluşturulacağı konuya ilişkin yeterli büyüklükte bir veri havuzuna ihtiyaç duyulmaktadırlar. Kullanılacak verilerin insani ön yargılardan mümkün olduğunca arındırılmış olması ve bu şekilde kullanılması sistemin üreteceği istatistiksel tahminlerin güvenilir olması ve ayrımcılığa yol açmaması açısından son derece kritik öneme haizdir.[109]

Belirli kişi veya kişi grupları ile belirli lokasyon ve zaman dilimlerinde işlenmesi muhtemel suçlara ilişkin olarak tahmin çıktıları üreten sistemler, kullanılan veri çeşidine bağlı olarak, kişisel verilerin

---

106 **PULLEN/SCHEFFER**, s. 106.

107 **GLESS/ERIKSSON**, s. 49.

108 **GLESS/ERIKSSON**, s. 49; **ATEŞ**, s. 114.

109 **GLESS/ERIKSSON**, s. 50; **ATEŞ**, s. 116.

önleyici amaçlarla kaydedilmesini, depolanmasını ve işlenmesini gerekli kılmaktadır. Bu tahmine dayalı önleyici kolluk sistemlerinin kullanımı, özellikle kişisel verilerin korunması bakımından, verilerin önceden depolanması (Vorratsdatenspeicherung), kişisel verilerin otomatik olarak işlenmesi (automatisierte Datenverarbeitung)[110], otomatikleştirilmiş veri analizi (automatisierte Datenanalyse)[111] ve konumuz bakımından, risk öngörüsünde bulunan yapay zeka destekli sistemlerin bazılarında gündeme gelen riskli bir veri işleme yöntemi olarak otomatikleştirilmiş karar alma sistemleri (automatisierte Entscheidungsfindung/automated individual decision-making)[112] gibi oldukça tartışmalı ve güncel olguları gündeme getirmektedir.

Yapay zekâ destekli bir teknoloji olarak otomatikleştirilmiş karar alma (automatisierte Entscheidungsfindung/automated individual decision-making**)** sistemleri, insan tarafından alınan bir kararı destekleme işlevinin ötesinde, doğrudan bir kişi hakkında, kişisel verilerini kullanarak yapılan profilleme üzerinden kişi için hukuki açıdan dezavantajlı veya temel haklarına önemli müdahale teşkil eden kararlar alan sistemlerdir.[113] Önleyici kolluk faaliyetlerinde kullanımı gündeme gelen şekli ise, henüz suç işlememiş gerçek bir kişiye odaklanarak kişilik ve karakter özelliklerine ilişkin verilerin işlenmesiyle oluşturulan profil üzerinden suç işleme riskin değerlendirilmesidir. Yapay zekâ destekli teknolojilerin bu şekilde kullanımı, Avrupa Yapay Zekâ Düzenlemesi (KI-VO/EU AI Act/AB YZD) m. 5/1-d'de belirtilen yapay zekâ teknolojisinin yasaklı kullanım şekillerinden biridir.[114] Düzenlemenin gerekçesinde de

---

110 **TINNEFELD/ BUCHNER/PETRI/HOF**, s. 354.

111 **RABE** Lea, Das Urteil zur automatisierten Datenanalyse (BVerfGE 165, 363) – Besprechung des Urteils und seiner sicherheitsverfassungsrechtlichen Implikationen, in: Big Data und KI bei der Polizei, Das Palantir-Urteil in der interdisziplinären Diskussion, BÄUERLE Michael/DENKER Kai/GEMINN Christian/ SCHÖNDORF-HAUBOLD Bettina (edt.), Bad Langensalz Frankfurt am Main/New York 2025, s. 15.

112 **TINNEFELD/BUCHNER/PETRI/HOF**, s. 355, 356.

113 **TINNEFELD/BUCHNER/PETRI/HOF**, s. 356.

114 Yasak, bu tür yapay zeka sistemlerinin piyasaya sürülmesini, bu amaç için hizmete sokulmasını ve kullanılmasını kapsamaktadır, **AKBULUT**, Berrin/**AKBULUT** Mete Tuluhan, Yapay Zekâ Yasasında Risk Kategorileri, NEUHFD C. 8 S.1 2025, s. 480;

belirtildiği gibi, kişisel verilerin söz konusu amaçla ve bu şekilde işlenmesi, aynı zamanda Anayasa m. 38/4'te de düzenlenen masumiyet karinesine aykırılık teşkil etmektedir.[115] Bu bakımdan, Avrupa Yapay Zekâ Düzenlemesi m. 5/1-d'de yer alan bu yasağın, düzenlemenin 2. maddesinde kapsamın, Avrupa Birliği dışında yer alan bir ülkede bulunsa bile Avrupa Birliği vatandaşlarını etkileyecek faaliyetlerde bulunan üretici, hizmet sunucu ve ticari amaçla kullanan kişileri de içine alacak şekilde oldukça geniş belirlenmiş olması göz önünde tutulduğunda,[116] Türkiye'nin üye devlet olmaması sebebiyle ülkemiz bakımından geçerli olmadığı savunulamayacaktır. Hele çalışmanın konusu bakımından, başlangıç şüphesinin tespitinde yapay zekânın bu şekildeki kullanımının her şeyden önce Anayasa m. 38/4 bakımından yasak olduğu tartışmadan uzaktır.

Yapay zekâ yazılımlarının geliştirilmesinde kullanılan veriler çoğunlukla kolluk kuvvetlerinin ve devlet kurumlarının elinde bulunan (ikamet yeri, finansal durum, çocuk sayısı, sahip olunan aracın modeli, meslek, sağlık durumu vb.) ve farklı amaçlar doğrultusunda toplanmış verilerdir. Oysaki yapay zekâ yazılımına sahip sistemlerin isabetli çıktılara ulaşması için hem geliştirilme hem de kullanım aşamasında, yazılımın geliştirilme amacına uygun ve bu amaç bakımından ilgili hususları yansıtan verilerin kullanılması kritik bir öneme sahiptir. Örneğin, tahmine dayalı önleyici kolluk faaliyetlerinde tercih edilen büyük veri analizine dayalı öğrenme temelli bir yapay zekâ modelinin, bir tehdit ifadesinin varlığını tespit etmesi istendiğinde, konuşan kişinin tonlamasını dikkate alan bir kategorizasyon yöntemi belirlemiş ise,

örneğin Amerika'da kullanılan "risk değerlendirme skorlarına" dayalı kişisel kontaklar, etnik, sosyal ve coğrafi kökene ilişkin verilerinde değerlendirmeye dahil olduğu bir analiz sonucunda belirli bir gerçek kişi hakkında kasten öldürme suçunun faili olması veya yeniden suç işlemesi bakımından bir risk skoru belirleyen sistemler (Correctional Offender Management Profiling for Alternative Sanctions – COMPAS) bu kapsamda yasaklı uygulamalara örnek olarak gösterilebilecektir, **BRUN, Marcel,** Predictive Policing-Revolution in der Verbrechensbekämpfung und Polizeiarbeit?, ZStrR 140/2022, s. 164.

115 Düzenlemenin gerekçesi de masumiyet karinesine odaklanmaktadır, bkz. **ATEŞ,** s. 148.

116 **AKBULUT/AKBULUT**, s. 472, 473.

modelin eğitiminde bu hususiyet dikkate alınmadan yapılacak bir veri yüklemesinde sırf tonlama yüzünden tehdit içermeyen bir ifade tehdit olarak değerlendirilebilecekken, tehdit içeren bir diğer ifade ise risksiz olarak kategorize edilebilecektir.[117]

Yine bu bağlamda, kriminal amaçlarla kolluk tarafından toplanan veriler, yapay zekâ yazılımının geliştirilmesi aşamasının kendine özgü hususiyetleri dikkate alınmadan orantısız bir şekilde kullanılabilecektir. Bu bağlamda, bir yapay zeka modeli eğitim aşamasında kendisine yüklenen veriler arasında erkeklere ilişkin verilerin kadınlara kıyasla oldukça fazla olması halinde, risk değerlendirmesi yaparken değerlendirmede bulunduğu kişinin sadece erkek veya kadın olmasından kaynaklı olarak isabetsiz çıktılar ortaya koyabilecektir.[118] Yapay zekâ yazılımına sahip risk hesaplama sistemlerinin barındırdığı bu ve benzeri riskler sebebiyle, değerlendirilen kişiye ilişkin henüz makul suç şüphesinin bulunmadığı bir aşamada, belirli bir bireye odaklı olarak gelecekte gerçekleştirmesi muhtemel davranışlarına ilişkin risk tahmininde bulunulmasının kategorik olarak yasaklanması, kullanıldığı takdirde gündeme gelmesi kaçınılmaz görünen masumiyet karinesi, ayrımcılık yasağı[119] ve adil yargılanma hakkının ihlaline yol açmamak bakımından isabetli gözükmektedir.

Yasak kapsamının açıklığa kavuşturulması bakımından vurgulanması gereken, kişinin profili çıkarılarak veya kişilik özellikleri (yaş, etnik köken, sosyal çevre, adres, kişisel ilgi alanları vb.) dikkate alınarak gelecekte göstermesi olası davranışları belirlemeye yönelik programların yasak kapsamında olduğudur.[120] Buna karşın, kişinin gerçekleştirdiği davranışın suçla ilişkili olma riskini değerlendiren sistem çıktıları bir insan tarafından alınacak kararı desteklemek için kullanılırsa (belirli finansal hareketlerin dolandırıcılık veya terörizmin finansmanı ile

---

117 **GLESS/ERIKSSON**, s. 20.

118 Krş. **GLESS/ERIKSSON**, s. 20, 21.

119 **ERDOĞAN,** s. 47.

120 **AKBULUT/AKBULUT**, s. 480; **ATEŞ**, s. 149.

ilişkili olması vb.) bu sistemler yasak kapsamında değerlendirilmeyecektir.[121]

Bu bağlamda dijital ortamdaki yasak müstehcenlik, çocuk pornografisi, şiddet ve hayvanların cinsel istismarı (zoofili) teşkil eden içerikleri belirleyip, söz konusu veriye bir hash değeri (bir verinin sadece kendine ait bir karakter dizisine dönüştürülmesi -dijital parmak izi-) vererek adli kolluk personeli tarafından denetlenmeksizin kara listeye alarak kaydeden, İsviçre Polisi tarafından kullanılan Nationale Datei- und Hashwertesammlung (NDHS) örnek olarak gösterilebilecektir.[122] Kara listeye dahil edilecek içeriklerin sadece cezalandırılabilir içerikler olmasının sağlanması, zaman zaman insan tarafından yapılması gereken hukuki ve etik değerlendirmeleri (görüntülerde yer alan kişilerin yaşının tespiti, çocukların model olarak kullanıldıkları görüntüler vb.) gerekli kılmaktadır. Bu durumda NDHS'nin etik ve hukuki açıdan gri alanda bulunduğunu belirlediği içerikler, ancak birbirinden bağımsız üç kişi tarafından kesin olarak çocuk pornografisi olarak kategorize edilmeleri halinde kara listeye dahil edilmektedir.[123]

Veri analizi ve öğrenme temelli algoritmalar kullanılarak elde edilen çıktı, istatistiksel olarak bir ihtimale, bir "şüphe" zeminine işaret etmektedir. Fakat söz konusu istatistiksel analiz sonucu, sadece sistem içerisinde var olan verilere dayanan algoritmik analiz yoluyla, kullanılan verilerle sınırlı bir kapsamda bir ihtimal değeri ortaya koyabilmektedir. Bu bağlamda, sistem, analiz ettiği verinin tespiti amaçlanan sınır değerde bulunduğuna ilişkin tahmini bir ilişkiye işaret etmektedir. Değerlendirdiği verinin bazen insan tarafından kavranması oldukça zor bağıntılı ilişkiler nedeniyle (özellikle öğrenme temelli yapay zekâ yazılımlarında; örneğin işlenen verinin boyutu, formatı vb.) sınır değerde olduğu sonucuna varabileceği gibi, bazen de sistemde yer alan veri

---

121 **AKBULUT/AKBULUT**, s. 481; **ATEŞ**, s. 149

122 **BORGHI**, Nikolozi, Unermüdliche und unerschrokene digitale Helfer - KI-Systeme zur Auswertung pädokrimineller Daten, s. 193

123 **BORGHI**, s. 194.

eksikliğine dayalı olarak karşılaştığı veriyi hedeflenen sınır değer bakımından değerlendirmesi mümkün olmamaktadır.[124]

Ceza muhakemesi hukuku bakımından şüphenin belirlenmesinde, şüphenin varlığına hükmedecek kişiyi dikkate alan sübjektif şüphe anlayışı karşısında, istatistiksel analize dayalı bu çıktının tek başına başlangıç şüphesi olarak kabul edilmesi mümkün gözükmemektedir. Çalışmanın konusunu teşkil eden başlangıç şüphesi kavramı elbette bilinen olgulara dayalı olarak yetkili savcılık tarafından yapılan sübjektif, fakat rasyonel düşünme yetisine sahip bir birey açısından anlaşılabilir bir mantıksal kurguya sahip[125], diğer bir ifade ile özneler arası (ıntersubjektif) bir tahmin faaliyetine dayanmaktadır. Buna karşın başlangıç şüphesinin tespitini tek başına bir tahmin faaliyetinden ibaret görmek de mümkün değildir. Başlangıç şüphesi aynı zamanda, bilinen olgular dikkate alınarak soruşturulması mümkün ve yaptırım uygulanabilir belirli bir suçun işlendiğine, kriminalistik perspektiften mantıksal tutarlılık içinde işaret eden bir durumun bulunup bulunmadığı noktasında hem hukuki ve hem de kriminalistik bir değerlendirme faaliyetini gerekli kılmaktadır.[126] Bu açıdan, yapay zekâ destekli sistemin veriyi riskli kategorideki listeye dahil etmesine yönelik çıktısı, başlangıç şüphesinin varlığı için tek başına yeterli kabul edilemeyecektir. Ancak savcılık tarafından yapılacak, gerekli kıstasları taşıyan bir değerlendirme sonucunda, sistemin istatistiksel tahmini tek başına belirleyici olmaksızın dikkate alınarak, başlangıç şüphesinin varlığı için gerekli bütün koşulların mevcut olması durumunda soruşturma başlatılmalıdır.

Suçların önlenmesi ve aydınlatılması amacıyla şüpheli çevrim içi işlemleri otomatik olarak değerlendiren yapay zekâ sistemlerinin kolluk

---

124 **PETERS**, Amadeus, Smarte Verdachtsgewinnung, Baden- Baden 2023, s. 116

125 **PETERS**, s. 113.

126 **WOHLERS**, s. 1316; **PETERS**, s. 91, 95; Başlangıç şüphesinin varlığına ilişkin karar geçmişe dönük bir karar değil aynı zamanda ileri dönük olarak olan yapılan iki yönlü bir değerlendirme içermektedir. Aydınlatılması mümkün gözükmeyen bir olayın araştırılması anlamsızdır. Örneğin oldukça kalabalık, insanların dip dibe yürüdüğü bir festival esnasında gerçekleşen ve sonradan fark edilen cepten para çalınması olayının aydınlatılması mümkün olmayacağı en başından öngörülebilecektir, Müko-**PETERS**, § 152 Kn. 50, 52, 53.

kuvvetleri tarafından veya onların adılına kullanılması hali, AB Yapay Zekâ Düzenlenmesi (AB YZD) m. 6/2 bağlamında yüksek riskli yapay zekâ sistemlerini belirten Ek III/6(d)'de düzenlenmiştir. Söz konusu sistemler, profilleme yapmaksızın gerçek kişilerin ve grupların özelliklerini, niteliklerini ve geçmiş suç davranışlarını değerlendirilmek amacıyla tasarlanmış olmaları veya profil çıkarmaları durumunda, Ek III/6(e)' de suçların tespiti amacıyla kolluk kuvvetleri tarafından kullanılması halinde yüksek riskli yapay zekâ sistemi olarak tanımlanmıştır. AB Yapay Zekâ Düzenlenmesinde bir sistemin yüksek riskli olarak kategorize edilmesinin sonucu, kullanımına ancak barındırdığı riskin minimize edilmesi için gerekli önlemlerin alınması durumunda izin verilmesidir.[127] Söz konusu yapay zekâ sistemlerinin davranış algoritması geliştirilirken kullanılan veri kümelerinin, oluşturulan örnekler bakımından yeterli temsil kabiliyetine haiz, mümkün olduğunca hatasız ve eksiksiz olması (AB YZD m. 10/2-5) gerekmektedir. Yapay zekâ sistemlerinin önyargısız ve ayrımcılığa sebebiyet vermeyecek çıktılar üretmesi veri kalitesine ilişkin kriterlerin temel amaçlarından birini teşkil etmektedir.[128]

Söz konusu sistemler kişisel verileri işleyerek otomatik kararlar almakta ve bazı durumlarda profillemeler de yapmaktadır. Gündeme gelen kişisel verilerin kaydedilmesi, işlenmesi ve otomatikleştirilmiş karar alma süreçlerinde kullanılması sistemlerin kişisel verilerin korunması perspektifinden değerlendirilmesini gerekli kılmaktadır.

Bireylere ilişkin kişisel verilerin analizi suretiyle profilleme yapan sistemlerin suçun önlenmesi ve aydınlatılması amacıyla kullanılması durumunda da kişisel verileri kullanılan kişilerin temel hak ve özgürlüklerinin korunmasına yönelik gerekli koruma mekanizmalarının öngörülmesi önem arz etmektedir. Örneğin, AB 2016/680 sayılı Yargı ve Çevresinde Kişisel Verilerin Korunmasına Yönelik Direktif, suçun işlenmesinin önlenmesi ve aydınlatılması veya kamu güvenliğine yönelik tehditlere karşı korunma ve bunların önlenmesi gibi amaçlarla verilerin

---

127 **VOLZ Stephanie**, Die KI-Verordnung und die Schweiz, SİC! 2025, s. 663

128 **VOLZ**, s. 663; **ATEŞ**, s. 150.

işlenmesi durumunda da verilerin elde edilme amacına uygun kullanılmasını, kişisel verileri işlenen kişinin suçun soruşturulmasını ve aydınlatılmasını temin edecek şekilde bilgilendirilmesi (m. 13),[129] kişisel verileri işlenen kişilerin temel hak ve özgürlüklerini dikkate alan ve özellikle bu bağlamda bunlara müdahale teşkil eden kişisel verilerin işlenmesinde ölçülülük prensibinin dikkate alınmasını (m. 15), kişisel verileri işlenen kişilerin verilerinin silinmesini, verilere erişimin kısıtlanmasını ve eksik veya yanlış olan kişisel verilerin düzeltilmesini/tamamlanmasını talep etme hakkına ilişkin (m. 16)[130] garantileri öngörmektedir.

Buna karşın, KVKK m. 28/1-ç'de kişisel verilerin milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenliği sağlama amacıyla kanunla yetkilendirilmiş kamu kurum ve kuruluşlarınca yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesini ve yine m. 28/1-d'de kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemleri kapsamında yargı makamları ve infaz mercileri tarafından işlenmesini, KVKK kapsamında kişisel verileri işlenen kişilere tanınan koruma rejiminin dışında değerlendirmiştir. Fakat bu durumda söz konusu veri işleme faaliyetlerine özgü güvenceler KVKK'da düzenlenmemiştir. Yine hukukumuzda istihbarat ve önleyici kolluk faaliyetleri arasındaki ayrımın oldukça muğlak olduğu hukuki düzenlemeler (PVSK Ek m. 7, Siber Güvenlik Kanunu m. 6/1-ç) göz önünde bulundurulduğunda[131] söz konusu faaliyetler kapsamında istihbarat amaçlı işlenen bilginin kolluk faaliyetleri kapsamında kullanılması ve bunun da adli merciler tarafından yürütülen ceza yargılamasında kullanılması gündeme geldiğinde T.C. Anayasası'nda düzenlenen kişisel verilerin korunmasını

---

129 **TINNEFELD/ BUCHNER/PETRI/HOF**, s. 357.

130 Verileri işlenen kişiler, suçun aydınlatılması delil olarak kullanılacak olması nedeniyle adli merciler tarafından tutulması gereken veriler silinmediği durumda, verilerin işlenmesinin kısıtlanmasını talep etme hakkına da sahiptir, **TINNEFELD/ BUCHNER/PETRI/HOF**, s. 358, 359.

131 **ERDOĞAN**, s. 140, 141; **KIZILIRMAK**, s. 254, 257.

isteme hakkının (Anayasa m. 20/3)[132] sanal dünyadaki kaçınılmaz görünümü olan "bilişimsel kaderin tayin hakkı" kapsamında gündeme gelecek verilerin elde edildiği amaçla bağlantılı kullanılması prensibinin, yine Anayasa m. 38/6 ve CMK m. 217/1-2 bağlamında suçun ancak hukuka uygun yöntemlerle elde edilmiş delillere dayalı olarak ispatlanabileceği, hakimin ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayalı hüküm verebileceğine ilişkin düzenlemelerin ihlalinin gündeme gelmesi olası olacaktır. Bu bağlamda hem ilgili kanunlarda hem de KVKK bağlamında suçun önlenmesi ve aydınlatılması amacıyla kişisel verilerin işlenmesi durumunda gerekli güvenceleri öngören ve amaca bağlılık kuralının gereğine uygun olarak istisnai rejimin öngörüldüğü durumlarda istihbarat, önleyici kolluk ve suç soruşturması ayrımının dikkate alındığı bir düzenlemeye ihtiyaç olduğu açıkça ortadadır.[133]

Bu noktada yine, önleyici kolluk faaliyetlerinde kullanılan, kişilere ait verilerin anonimleştirilerek belirli bir suçun ne zaman ve nerede işlenebileceğine ilişkin öngörüler oluşturan sistemlerin AB Yapay Zekâ Düzenlemesi kapsamında yasak olmadığı belirtilmelidir. Söz konusu sistemlere örnek olarak, Avrupa'da birden fazla ülkede (Almanya, İsviçre vd.) kullanılan, operasyonel veri tabanlarını kullanarak yaptığı analizlere dayalı olarak belirlediği korelatif bağıntıları dikkate alarak gelecekte ne zaman ve nerede nitelikli hırsızlık (Einbruchsdiebstahl**,** Alman Ceza Kanunu § 243, 244) suçunun işleneceğine ilişkin çıktılar üreten "Precobs" uygulaması gösterilebilecektir. Sistem, anonimleştirilmiş verileri kullanmakta ve belirli kişiler üzerinde tahminde bulunmamaktadır. Bu sebeple, veri koruma bakımından otomatikleştirilmiş bir karar alma söz konusu olmadığı gibi, Yapay Zekâ Düzenlemesi kapsamında yasaklanmış veri işleme yöntemlerine ilişkin yasaklar kapsamında da

---

132 "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

133 Aynı yönde bkz. **ERDOĞAN**, s. 141; **KIZILIRMAK**, s. 258.

değerlendirilmemektedir.[134] Sistemin istatistiki analiz sonucu oluşturduğu çıktı, gelecekte belirli bir bölge ve zamanda suçun işlenmesine ilişkin bir olasılık derecesi mahiyeti taşımaktadır. Her ne kadar suç nitelikli hırsızlık olarak belirli olsa da, henüz işlenmemiş bir suça ilişkindir. Burada başlangıç şüphesinden bahsetmek mümkün değildir. Sistem, önleyici kolluk faaliyetlerinin yürütülmesinde optimizasyon amaçlıdır.

Sistemin çıktısı dahilinde belirli bir bölgede yürütülen suçun işlenmesini önlemek amacıyla gerçekleştirilen devriye faaliyeti esnasında polis, bir suçun işlendiği veya işlenmekte olduğu bilgisini edinirse, PVSK Ek m. 6 kapsamında olay yerinin korunması, suç delillerinin tespiti ve korunması için gerekli tedbirleri aldıktan sonra derhal Cumhuriyet savcısına durumu bildirecektir. Bu aşamadan itibaren sonra söz konusu olay bakımından adli kolluk faaliyeti söz konusu olacaktır. Cumhuriyet savcısı, suçun aydınlatılması amacıyla gerekli soruşturma işlemlerini yürütecek veya emrindeki adli kolluk aracılığı ile bu işlemleri yaptıracaktır.

c. Yüz Tanıma Sistemleri

Yüz tanıma sistemleri, ağız, göz, çene ve burun gibi kişinin tanımlanması bakımından kilit noktaları referans alarak oluşturdukları verilere dayalı olarak resim veya video materyalleri üzerinden elde ettikleri verileri kendi veri tabanında bulunan verilerle karşılaştırarak kişilerin kimliklerinin otomatik olarak tespitini mümkün kılmak için geliştirilen yapay zekâ destekli (makine öğrenmesi) sistemlerdir.[135] Yüz tanıma sistemlerine suçun önlenmesi amacıyla başvurulması durumunda, başlangıç şüphesinin varlığının ne zaman gündeme

---

134 **TINNEFELD/ BUCHNER/PETRI/HOF**, s. 356.

135 **SIMMLER,** Monika/**CANOVA,** Giulia, Gesichterkennungstechnologie: Die "smarte" Polizeiarbeit auf dem rechtlichen Prüfstand, Sicherheit & Recht 3/2021, s. 107; **SCHINDLER**, Stephan, EU-Kommission: Verordnungsentwurf zur Regulierung von KI das Ende polizeilicher Gesichtserkennung im öffentlichen Raum?, ZD-Aktuell 10/2021, son erişim 21.05.2025 : https://beck-online.beck.de/Bcid/Y-300-Z-ZDAKTUELL-B-2021-N-05221; **ZAFER,** İçer/**DÖNMEZ,** Elif, Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları, CHD Ağustos 2020, Cilt: 15 Sayı: 43, s. 423.

geleceğinin tespiti, sürecin artık suç soruşturması aşaması olarak değerlendirilmesini gerektirdiğinden, konumuz bakımından önem arz etmektedir.

Biyometrik tanımlama sistemleri içerisinde yer alan yüz tanıma sistemleri, önleyici ve adli kolluk faaliyetleri kapsamında sıklıkla kullanılmaktadır.[136] Yüz tanımanın temelde, bir yüzün belirli bir kişiye ait olup olmadığının doğrulanması (face verification) ve bir yüzün diğer yüzlerden ayırt edilmesini sağlayacak şekilde tanımlaması (face identification) olarak iki farklı şekilde gerçekleştiği ifade edilebilir.[137] Yüz tanıma sistemlerinin her iki türü de kişilerin kimliklerinin, onları diğer insanlardan ayıran kendilerine özgü ölçülebilir bedensel özellikleri olan biyometrik veriler vasıtasıyla doğrulanması ve tespitine yönelmektedir. Bu bakımdan her iki yüz tanıma yöntemi klasik anlamda bir biyometrik tanımlama süreci teşkil eder.[138]

Yüz tanıma sistemlerinin çalışma süreçleri, diğer biyometrik tanımlama sistemleri ile benzer şekilde, yapay zekâ destekli sistemin sensörleri vasıtasıyla elde edilen ham verilerin, sistemin algoritması tarafından belirli bir modele indirgenerek bir veri kümesine dönüştürülmesinden sonra analiz edilerek veri şablonlarına dönüştürülmüş başkalarına ait verilerle karşılaştırılmasına dayanmaktadır.[139] Kişilerin elmacık kemikleri arasındaki mesafe, gözleri, ağızları ve burun arasındaki mesafeler veya bunların birbirleri ile oransal ilişkileri gibi kişilerin yüzlerinin ayırt edici özelliklerine ilişkin veriler, sensörler vasıtasıyla belirlenmekte, sistemlerin algoritması tarafından veri kümesi teşkil eden şablonlara çevrilmekte ve benzer şekilde dönüştürülen veri şablonları ile karşılaştırılmaktadır.[140] Bu karşılaştırma sonucunda, kullanılan görsel içerikte yer alan kişilerin yüz verilerine

---

136 **ATEŞ**, s. 178; **SIMMLER/ CANOVA**, s. 107.

137 **SIMMLER/ CANOVA**, s. 107.

138 **SIMMLER/ CANOVA**, s. 107.

139 **SIMMLER/CANOVA,** s. 107; **ATEŞ**, s. 185; **AKBULUT,** Berrin/ **AÇIL,** Murat, Avrupa Birliği Yapay Zekâ Tüzüğü'ne Göre Yasaklanmış Yapay Zekâ Uygulamaları, HBV-HFD Nisan 2026 C. 30 Sayı 2, s. 1021.

140 **SIMMLER/CANOVA**, s. 108; **İÇER/DÖNMEZ**, s. 425.

dayalı olarak kimlikleri otomatik olarak doğrulanabilmekte veya tespit edilebilmektedir.

Yüz tanıma sistemleri kamuya açık işlek caddeler, kalabalık meydanlar, yoğun şekilde kullanılan istasyonlar ve geçiş güzergahları gibi yerlerde genel genel önleme ve işlenen suçların tespiti amacıyla bir izleme aracı olarak kullanılabildiği gibi, somut ve özel bir izleme yöntemi olarak belirli bir suçun aydınlatılmasına yönelik olarak da kullanılmaktadır.[141] Konumuz bakımından, önleyici kolluk faaliyetlerinde genel izleme aracı olarak yüz tanıma sistemlerinin kullanımı gündeme gelmektedir. Genel izleme, özellikle büyük şehirlerde ve insanların toplu biçimde bulunduğu alanlarda güvenliği sağlama ve suçun işlenmesini önleme amacıyla, Mobil Elektronik Sistem Entegrasyonu (MOBESE) kameraları vasıtasıyla kayda alınan görüntülerin bir yetkili tarafından denetlenmesine dayanmaktadır. Ülkemizde MOBESE sistemine plaka tanıma sistemi (PTS) entegre edilmiştir.

Yüz tanıma sistemleri ise MOBESE'den farklılaşmakta, çok büyük video verileri içerisinde çok kısa sürede algoritmasının eğitildiği amaç doğrultusunda çok büyük boyutta verileri işleyerek çıktılara ulaşmakta, otomatikleştirilmiş bir şekilde sadece bireylerin değil herhangi bir şekilde kategorize edilecek insan topluluklarını izleme ve denetleme imkânı sağlamaktadır. Bu hususiyetleri sebebiyle, sadece bir veya daha fazla yetkili tarafından yapılan video kaydı incelenmesinin çok ötesinde hızlı veri analizi imkânı sağlamakta[142], bununla birlikte temel hak ve özgürlüklere müdahale açısından önemli bir potansiyel taşımaktadır.[143]

MOBESE kullanımına ilişkin düzenlemelerin veya PTS kullanımını mümkün kıldığı iddia edilen düzenlemelerin, yapay zekâ destekli yüz tanıma sistemlerinin kullanımı için yasal dayanak teşkil etmediği[144]

---

141 **SIMMLER/CANOVA,** s. 108.

142 **İÇER/DÖNMEZ**, s. 425.

143 **SIMMLER/CANOVA**, s. 112.

144 İl İdaresi Kanunu m. 11/H dayanak gösterilmekte, düzenleme, yeterli açıklıkta teknik destekli denetimi içermemesi ve kaydedilen kişisel verilere ilişkin gerekli güvenceleri sağlamaması nedeniyle haklı olarak eleştirilmektedir, **ATEŞ**, s. 225, 226,

dikkate alınmalıdır. Söz konusu sistemlerin teknik hususiyetlerini (sistemin eğitilmesi için gereken verilerin toplanması, elde edilen yeni verilerin karşılaştırılması ve işlenerek yeni çıktılar elde edilmesi) ve taşıdıkları temel hak ve özgürlüklere yoğun müdahale potansiyelini dikkate alan güvenceleri (kullanılan verilerin elde edilme amacıyla sınırlı kullanımı, saklanma süresinin tahdidi, ilgilinin bilgilendirilmesi, kullanılacak yapay zeka yazılımlarının veri kalitesi, şeffaflık ve denetlenebilirlik bakımından sertifikalandırılması) içeren bir yasal düzenlemeye kavuşturulması elzemdir. Aksi takdirde sistemin kullanımının yasal dayanaktan yoksun olması sebebiyle, temel hak ve özgürlüklere hukuka aykırı bir müdahale söz konusu olacak ve bu suretle elde edilen deliller de hukuka aykırı olacaktır.

Bu noktada, ülkemizde Havelsan tarafından geliştirilen ve Emniyet Genel Müdürlüğü tarafından kullanılan yapay zekâ destekli EYEMINER sistemi, aynı zamanda kişilerin eşkâl bilgilerinin tespitinde kullanılmaktadır. Kişisel verileri işleyen söz konusu sistemin suçun önlenmesi ve aydınlatılması amacıyla kullanımı, KVKK m. 28/1-ç ve d'de kişisel veriler için öngörülen koruma rejiminin dışında tutulmuştur. Fakat bu istisna hükümleri, herhangi bir hukuki düzenlemeye gerek olmaksızın kişisel verilere herhangi bir güvenceye ve sınırlamaya tabi olmaksızın müdahale edilebileceği anlamına gelmemektedir. Her halükârda, kullanılan sistemin hangi kapsamda, hangi suçlarla ilgili olarak[145] ve ne ölçüde kullanılabileceği, elde edilen ve işlenen kişisel verilerin nasıl saklanacağı ve bu verilere hangi suçlarla ilgili olarak yeniden başvurulabileceği gibi hususları[146] ayrıntılı olarak ele alan bir

233. İsviçre Federal Mahkemesi, yüz tanıma sistemlerinin kullanımı bakımından video denetim sistemlerine ilişkin mevcut yasal düzenlemelerin yasallık ilkesi bakımından yetersiz olduğuna ve yeni bir yasal düzenlemeye ihtiyaç olduğuna hükmetmiştir. BGE 146 I 11, E.4.2 (19) aktaran bkz., **SIMMLER/CANOVA**, s. 112, 115.

145 Gerçek zamanlı uzaktan biyometrik tanımlamanın ihtiva ettiği, temel hak ve özgürlüklere yoğun müdahale sebebiyle, Alman Anayasa Mahkemesi, ancak belirli ağır suçlarla sınırlı olarak başvurulabilmesi durumunda orantılı olacağına hükmetmiştir, BVerfGE 129, 208, karar için bkz. **HAHN,** Johanna, Automatisierte Gesichtserkennung in der Strafverfolgung, Baden- Baden 2025, s. 131.

146 **TINNEFELD/ BUCHNER/PETRI/HOF**, s. 35.

yasal düzenlemeye kavuşturulması zorunludur. Aksi takdirde, sistemin kullanımı, yasal dayanaktan yoksun bir özel hayata müdahale niteliğinde olacak ve Anayasa m. 20'ye aykırılık teşkil edecektir.[147]

Kişinin yüzüne ait görsel materyallerden (video kaydı, fotoğraf vb.) elde edilen biyometrik verilerin kişisel veri olduğu (GDPR m. 4)[148] hususunda bir tartışma olmadığı gibi, söz konusu veriler, kişinin kişiliği ile sıkı ilişkisi sebebiyle gerek GDPR bağlamında gerekse KVKK m. 6/1 bakımından hassas kişisel veri olarak değerlendirilmektedir.[149] Yüz tanıma sistemlerinin genel izleme amacıyla kullanılması kapsamında, elde edilen görüntülerden kişilerin yüzlerine ait biyometrik hususiyetlerin anlık olarak veri kümesine dönüştürülmesi, sistemde mevcut verilerle kıyaslanarak edilen çıktı üzerinden tanımlama işleminin gerçekleştirilmesi anlamına gelen "gerçek zamanlı anlık uzaktan biyometrik tanımlama"[150] sistemleri gündeme gelmektedir. Söz konusu sistemler, genel izleme amacıyla hedef gözetmeksizin kullanıldığında,

---

147 Halihazırda söz konusu sistemin kullanımı kapsamında gerçekleştirilen gerçek zamanlı biyometrik tanımlama işlemleri, kamuya açık alanlarda gerçekleşse bile, AİHM kararları kapsamında AİHS m. 8 bağlamında özel hayata müdahale teşkil etmektedir, Glukhin v. Rusya, paragraf 66. Anayasa Mahkemesi, CMK m. 134/1'de yer alan "Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim … tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir." bölümü ve (2) numaralı fıkrasının birinci cümlesinin "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması … halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir." bölümünün Anayasa'ya aykırı olduğuna ve iptaline, kişisel verilerin kaydedilmesi suretiyle özel hayata saygı ve kişisel verilerin korunmasını isteme hakları özelinde, bilişimsel kaderini tayin hakkı bağlamında gerekli güvenceleri içermeyen bir yasal düzenlemenin içerdiği sınırlamanın "orantısız" bir müdahale olduğu gerekçesiyle karar vermiştir, AYM, E. 2023/128, K. 2026/36, 12.2.2026, RG 25.5.2026/33264.

148 **LI**, s. 62, 63.

149 **BULUT,** Metin, Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler, Ankara Barosu Dergisi 2020/3, s. 108, 110, 114; **HAHN**, s. 35.

150 **ATEŞ,** s., 194.

özel yaşama "sistematik ve daimî"[151] bir müdahale teşkil edecektir. İnsanın kendisini gerçekleştirebilmesi için gerekli olan özgürlük duygusunu "sürekli gözetim altında tutulma" kaygısıyla ortadan kaldırma riski taşıyan bu uygulama, Avrupa İnsan Hakları Mahkemesi'nin kararlarına yansıyan taraf ifadelerinde de isabetli olarak belirtildiği gibi, "dijital çağda temel haklara yönelik en büyük tehditlerden biri"[152] olarak nitelendirilmektedir. Özel yaşama orantısız müdahale teşkil eden yapay zekâ destekli gerçek zamanlı uzaktan biyometrik tanımlama sistemlerinin, genel gözetleme amacıyla, hedef gözetmeksizin internet veya kapalı devre güvenlik kameraları (CCTV) vasıtasıyla elde edilen verileri "kazıması" (untargeted scraping)[153] suretiyle veri tabanı oluşturacak veya mevcut veri tabanını genişletecek şekilde piyasaya arzı, bu özel amaçla hizmete sunulması veya kullanımı" AB YZD m. 5/1-e'de yasaklanmıştır.[154]

AB YZD m. 5/1-h'de ise, kolluk kuvvetlerinin (adli ve önleyici kolluk) amaçları doğrultusunda kamuya açık alanlarda gerçek zamanlı uzaktan biyometrik tanımlama sistemlerinin kullanımı kural olarak yasaklamış, ancak maddede belirtilen amaçlarla sınırlı olarak bu sistemlerin kullanımına izin verilmiştir. Fakat Düzenleme, izin verilmiş kullanımın "ancak ve yalnızca m. 5/1-h' de sayılan amaçlardan biri için" ve "kesin bir şekilde gerekli olması halinde" mümkün olabileceğini belirtmiştir. Söz konusu düzenlemede, önleyici kolluk faaliyeti kapsamında izin verilen kullanım, m. 5/1-h (ii)'de belirtilen "gerçek kişilerin yaşamına veya fiziksel güvenliğine yönelik belirli, esaslı ve yakın bir tehdidin veya bir terör saldırısına yönelik gerçek ve mevcut ya da

---

151 **İÇER/DÖNMEZ,** s. 446.

152 "*They argued that biometric mass surveillance, in particular with the use of facial recognition technology, represented one of the greatest threats to fundamental rights in the digital age*", Glukhin v. Rusya, paragraf 63, son erişim 12.06.2026: https://hudoc.echr.coe.int/?i=001-225655.

153 Söz konusu yöntemin somut hali olarak adlandırılabilecek bir start-up girişimi olan Clearview şirketinin, internetteki görsel materyallerden elde edilmiş 30 milyardan fazla görsele sahip bir veri tabanına sahip olduğu belirtilmektedir, **HAHN**, s. 49.

154 **AKBULUT/AÇIL**, s. 1022; **ATEŞ**, s. 195.

gerçek ve öngörülebilir bir tehdidin önlenmesi" amacının söz konusu olması durumunda gündeme gelebilecektir.

Temel hak ve özgürlüklere oldukça ağır ve sistematik bir müdahale teşkil eden, gerçek zamanlı biyometrik verilere dayanan takibin hukuka uygun olabilmesi için, toplumsal düzenin tamamını hedef alan "terör saldırısına yönelik gerçek ve mevcut veya gerçek ve öngörülebilir" bir tehdit veyahut gerçek kişilerin hayatını veya bedensel bütünlüğünü hedefleyen "belirli, esaslı ve yakın bir tehdit" aranmıştır. AB YZD, bu şekildeki takibe istisna olarak izin vermekle birlikte, bu sistemlerin kullanımı durumunda Düzenlemede belirtilen yüksek riskli yapay zekâ sistemlerine ilişkin kurallara da tabi oldukları belirtilmelidir.[155]

Terör suçları bakımından aranan nitelikte bir terör saldırısı tehdidi söz konusu olması durumunda, hazırlık hareketi niteliğinde bazı fiillerin dahi suç olarak düzenlenmiş olması sebebiyle, belirli bir suçun işlendiğine yönelik başlangıç şüphesinin varlığının gündeme gelmesi ciddi bir ihtimaldir. Bu sebeple, durumun, gerekli hukuki değerlendirmenin ve henüz başlangıç şüphesinin bulunup bulunmadığına ilişkin değerlendirmenin yapılabilmesi için dahi savcıya bildirilmesi gerekecektir. Yapılacak yasal düzenlemede, gerçek zamanlı biyometrik veriye dayalı takibin bu sebeple hâkim kararına dayalı olarak yapılması esas olmalıdır. Fakat gecikmesinde sakınca bulunan hallerde, savcı ve konunun terör saldırısına ilişkin olması halinde ise gerekli acil müdahale dikkate alınarak kolluk amiri tarafından verilecek bir emirle de, sonradan hâkimin onayına sunulmak ve hâkimin onay vermemesi durumunda ilgili kayıtların silinmesi kaydıyla, bu takibin gerçekleştirilebilmesi mümkün olmalıdır.

Buna karşın, öldürme ve yaralama suçları bakımından retro perspektif açıdan oluşturulacak, bir suçun işlenmiş olabileceğine ilişkin başlangıç şüphesinin varlığından her somut olayda bahsetmek mümkün

---

155 AB YZD m. 5/2 bağlamında, kolluk faaliyetlerinde bu sistemlerin kullanılması durumunda, kullanımın ulusal hukukta zaman, coğrafi kapsam ve kişiler bakımından getirilecek sınırlamalar açısından gereklilik ve orantılılık şartlarını yerine getirecek önlem ve güvenceleri içerecek şekilde düzenlenmesi gerektiği belirtilmiştir; ayrıca bkz., **AKBULUT/ AKBULUT**, s. 485, 486.

olmayacaktır. Failin, mağdurun öldürülmesine veya yaralanmasına yönelik olarak gerçekleştirdiği düşünülen davranışları (silahla evden ayrılması, mağdurun bulunduğu yerin otogarına otobüsle gelmesi, mağdurun henüz gelmediği, ancak belirli bir süre sonra gelmesinin beklendiği mekâna gitmesi) henüz cezaya değer haksızlığın gerçekleştiği ilk aşama olan suça teşebbüs (doğrudan doğruya icraya başlama) aşamasına ulaşmamış olabilecektir. Bu durumda, önleyici kolluk faaliyeti kapsamında, bir suçun işlenebileceğine ilişkin bir tehlikenin varlığından bahsetmek mümkündür.

Gerçek zamanlı biyometrik takibin somut olarak belirli bir kişiye yönelik gerçekleşmesi durumunda dahi, takip edilen kişi bakımından temel hak ve özgürlüklere ağır bir müdahale söz konusu olmaktadır. Bu sebeple, bu yönteme başvurulması oldukça ağır suçlarla sınırlı tutulmuştur. Takip, henüz başlangıç şüphesinin söz konusu olmadığı bir aşamada gerçekleştirilse dahi, takip sırasında gündeme gelecek takip konusu dışındaki suçlara ilişkin delil elde edilebileceği de dikkate alınarak, hâkim kararına tabi tutulmalı; ancak gecikmesinde sakınca bulunan hallerde sonradan hâkimin onayına sunulmak ve onaylanmaması durumunda kayıtların silinmesi koşuluyla, savcı ve savcıya ulaşılamadığı hallerde ise kolluk amiri tarafından verilecek emirle gerçekleştirilmelidir.[156]

AB YZD m. 5/1-h (i)' de belirtilen, gerçek zamanlı uzaktan biyometrik takip sisteminin kullanımına istisnai olarak izin verildiği durumlardan biri de belirli kaçırma, insan ticareti veya cinsel sömürü mağdurlarının hedefli olarak aranması ya da kayıp kişilerin bulunmasına

---

[156] AB YZD m. 5/3'te, kolluk kuvvetleri tarafından kamuya açık alanlarda gerçekleştirilecek gerçek zamanlı biyometrik tanımlama işlemleri için "bir adli makamdan veya kararı, kullanımın gerçekleşeceği üye devlet açısından bağlayıcı olan bağımsız bir idari makamdan, gerekçeli bir talep üzerine ve m.5/5'te belirtilen ulusal mevzuat uyarınca önceden alınmış bir izne tabi olması" gerektiği belirtilmiştir. Fakat "gerekçelendirilmiş acil durumlarda, bu tür bir sistemin kullanımına izinsiz başlanabileceği", 24 saat içinde onaya sunulması ve onay verilmediği takdirde, kullanımın derhal durdurulması, bu kullanıma ilişkin tüm veriler ile elde edilen sonuç ve çıktıların gecikmeksizin imha edilerek silinmesi gerektiği belirtilmiştir.

yönelik aranmadır. Sadece kayıp kişilerin aranması durumunda, eğer başlangıç şüphesi düzeyinde bir suç işlendiği izlenimini veren somut olgular söz konusu değilse, söz konusu faaliyetin önleyici kolluk faaliyeti kapsamında kaldığının kabulü gerekecektir. Buna karşın, kaçırma, insan ticareti ve cinsel sömürü mağdurlarının aranmasına yönelik kullanım durumunda, ilgili suçun işlendiğine yönelik en az başlangıç şüphesi düzeyinde bir şüphenin bulunması söz konusu olacağından, adli süreç gündeme gelecektir. Bu durumda, yapılacak yasal düzenlemede ilgili kararın, kullanılacak yöntemin temel hak ve özgürlüklere ağır müdahale teşkil etmesi sebebiyle, kural olarak hâkim tarafından verilmesi gerekmektedir.

SONUÇ

Başlangıç şüphesinin varlığının üç unsura bağlı olduğu kabul edilmektedir. İlk olarak bir suçun işlendiği ihtimaline delalet eden somut emarelerin bulunması gerekmektedir. Sonrasında somut emareler kriminalistik biliminin tecrübeleri doğrultusunda yorumlandığında bir suçun tipinin unsurlarını gerçekleştiğinin olası görünmesi gerekmektedir. Son olarak ise değerlendirmeye konu hal bir bütün olarak ele alındığında cezalandırılabilir ve kovuşturulabilir bir suçun işlendiği ihtimali neticesine ulaşılması gerekmektedir.

Veri analizi ve öğrenme temelli algoritmalar kullanılarak elde edilen çıktı istatistiksel olarak bir ihtimale, bir "şüphe" zeminine işaret etmektedir. Fakat söz konusu istatistiksel analiz sonucu sadece sistem içerisinde var olan verilere dayalı algoritmik analiz yine kullandığı veriyle sınırlı bir kapsamda ihtimal değeri ortaya koyabilmektedir. Bu bağlamda analiz ettiği verinin tespiti amaçlanan sınır değerde bulunduğuna ilişkin tahmini bir ilişkiye işaret etmektedir. Değerlendirdiği veriyi bazen insan tarafından kavranması oldukça zor bir korelatif ilişkiyle (özellikle öğrenme temelli yapay zekâ yazılımlarında; Sadece işlenen verinin boyutu, formatı vb..) sınır değerde olduğu sonucuna gidebileceği gibi, bazen de sisteminde yer alan veri eksikliğine dayalı karşılaştığı veriyi hedeflenen sınır değer bakımından değerlendirmesi mümkün olmamaktadır. Ceza hukuku bakımından şüphenin belirlenmesinde şüphenin varlığına hükmedecek kişiyi dikkate

alan subjektif, objektif olarak makul bir şekilde izah edilebilir bir mantık silsilesine dayanmak kaydıyla, öznel değerlendirmeye dayanan şüphe kavramı dikkate alındığında istatistiksel analize dayalı bu çıktıyı başlangıç şüphesi olarak kabul etmek mümkün gözükmemektedir. Çalışmanın konusunu teşkil eden başlangıç şüphesi kavramı elbette bilinen olgulara dayalı olarak yetkili savcılık tarafından yapılan subjektif, fakat rasyonel düşünme yetisine sahip bir birey açısından anlaşılabilir bir mantıksal kurguya sahip (intersubjektif) bir tahmin faaliyetine dayanmaktadır. Buna karşın başlangıç şüphesinin tespitinin tek başına bir tahmin faaliyetinden ibaret görmek mümkün değildir. Aynı zamanda bilinen olgular dikkate alınarak soruşturulması/kovuşturulması mümkün ve yaptırım uygulanabilir belirli bir suçun işlendiğine, kriminalistik perspektiften mantıksal tutarlık içinde işaret eden bir durumun varlığını bulunduğu noktasında hem hukuki hem de etik bir değerlendirme faaliyetini gerekli kılmaktadır.

Sadece yapay zekâ destekli sistem tarafından bir davranışın belirli bir suç tipi bakımından riskli olduğuna ilişkin sistem çıktısı tek başına başlangıç şüphesinin varlığına hükmetmek için dayanak teşkil etmeyecektir. Profilleme teknolojileri/Risk analiz yazılımları kriminalistik istatistiksel veriler dikkate alınarak eğitilmekte ve yine bu bağlamda verileri işlemekte ve çıktılar üretmektedir. Kriminalistik verilerinin ortaya koyduğu belirleyici istatistiki korelatif ilişkiler somut olguların değerlendirilmesinde elbette dikkate alınacaktır, fakat sadece istatistiksel verilerin somut olgulardan başlangıç şüphesinin varlığını kabul etmek bakımından yegâne dayanak noktası kabul edilmesi durumunda yapılan soruşturma "balık yakalamak için rastgele bir olta atmak"[157] eyleminden farklı görünmeyecektir. Söz konusu sistem çıktısı belirli bir kişiye yönelmiş belirli bir suçla ilgili olarak suçun işlenmiş olduğu yönünde bir risk anlamına geliyorsa, çıktı yetkili adli mercilere iletilmeli ve adli merciler (Cumhuriyet Savcılığı) tarafından kişiye yönelik olarak bir ceza soruşturması başlatmadan önce kişinin ortaya çıkan bu çıktı dikkate alınarak bir suç işlemiş olabileceği ihtimalini destekleyebilecek başkaca

157 **WOHLERS**, s. 1318.

somut dayanak noktalarının bulunup bulunmadığı ilişkin (CMK m. 158/6) genel bir araştırma yapılması gereklidir.

Yine önleyici kolluk faaliyetlerinde kullanılan kişilere ait verilerin anonimleştirilerek belirli bir suçun ne zaman ve nerede işlenebileceğine ilişkin öngörüler oluşturan sistemlerin yasak kapsamında olmadığı belirtilmelidir. Her ne kadar suç nitelikli hırsızlık olarak belirli olsa da henüz işlenmemiş bir suça ilişkindir. Burada başlangıç şüphesinden bahsetmek mümkün değildir. Bu sistem önleyici kolluk faaliyetlerinin yürütülmesinde optimizasyon amaçlıdır. Sistemin çıktısı dahilinde belirli bir bölgede yapılan suçun işlenmesini önlemek amaçlı devriye faaliyeti esnasında polis suçun işlendiğini gösteren bir hal veya bir suçüstü hali ile karşılaşırsa PVSK ek madde 6 kapsamında suçun delilerinin tespiti ve korunması için gerekli tedbirleri aldıktan sonra derhal Cumhuriyet savcısına durumu bildirecektir. Bu durumdan sonra artık önleyici kolluk faaliyeti söz konusu değildir. Cumhuriyet savcısı suçun aydınlatılması noktasında gerekli soruşturma işlemlerini yürütecektir.

Yapay zekâ destekli sistemlerin suçla mücadelede bir diğer yaygın kullanımı bir biyometrik tanımlama sistemi olan yüz tanıma teknolojileridir. Bu noktada hem mukayeseli hukukta hem de ülkemizde yasal düzenleme eksikliği dikkat çekmektedir. MOBESE kullanıma ilişkin düzenlemelerin veya PTS kullanımını mümkün kıldığı iddia edilen düzenlemelerin yapay zekâ destekli yüz tanıma sistemlerin kullanımı için yasal dayanak teşkil etmediği dikkate alınmalıdır. Söz konusu sistemlerin teknik hususiyetlerini (sistemin eğitilmesi için gereken verilerin toplanması, elde edilen yeni verilerin karşılaştırılması ve işlenerek yeni çıktılara elde edilmesi) ve taşıdıkları temel hak ve özgürlüklere yoğun müdahale potansiyelini dikkate alan korumaları (kullanılan verilerin elde edilme amacıyla sınırlı kullanımı, saklanma süresinin tahdidi, ilgilinin bilgilendirilmesi, kullanılacak yapay zeka yazılımlarının veri kalitesi, şeffaflık ve denetlenebilirlik bakımından sertifikalandırılması) içeren bir yasal düzenlemeye kavuşturulması elzemdir. Aksi takdirde kullanımı yasal dayanaktan yoksun olması sebebiyle temel hak ve özgürlüklere yasal olmayan bir müdahale teşkil edecek ve bu suretle elde edilen deliller hukuka aykırı delil teşkil edecektir. Bu noktada ülkemizde Havelsan

tarafından geliştirilen ve Emniyet genel Müdürlüğü tarafından kullanılan yapay zeka destekli Eyminer sistemi aynı zamanda kişilerin eşkâl bilgilerini tespitinde kullanılmaktadır. Kişisel verileri işleyen söz konusu sistemin suçun önlenmesi ve aydınlatılması amacıyla kullanımı KVVK m. 28/1-ç ve d'de kişisel veriler için öngörülen koruma rejiminin dışında tutulmuştur. Fakat bu istisna herhangi bir hukuki düzenlemeye gerek olmaksızın kişisel verilere her türlü güvenceye ve sınırlamaya tabi olmadan müdahale edilebileceği anlamına gelmemektedir. Her halükârda kullanılan sistemin hangi kapsamda, hangi suçlarla ilgili olarak ve ne ölçüde kullanılabileceği ve elde edilen ve işlenen kişisel verilerin nasıl saklanacağı ve hangi suçlarla ilgili olarak bu verilere yeniden başvurulabileceği gibi hususları ayrıntılı olarak ele alan bir yasal düzenlemeye kavuşturulması zorunludur. Aksi takdirde sistemin kullanımı yasal dayanaktan yoksun bir özel hayata müdahale olarak Anayasa m. 20'ye aykırı olmaktadır.

Yapılması muhtemel bir düzenlemede özelikle temel hak ve özgürlüklere yönelik teşkil ettiği ağır müdahale içeriği değerlendirildiği gerçek zamanlı yüz tanıma teknolojilerinin kullanımı önem arz edecektir. Bu noktada kullanımının gündeme getirdiği temel hak ve özgürlüklere müdahale içeriğinin orantılı olması bakımından AB YZD m. 5/1-h'de istisnalar yol gösterici olacaktır. Konumuz bakımından bu istisnalar başlangıç şüphesi bağlamında değerlendirildiğinde;

Terör suçları bakımında aranan nitelikte bir terör saldırısı tehdidi söz konusu olması durumunda bir suçun niteliği gereği hazırlık hareketi niteliğinde fiillerin dahi bazı durumlarda suç olarak düzenlenmiş olması sebebiyle belirli bir suçun işlendiğine yönelik başlangıç şüphesinin varlığının gündeme gelmesi ciddi bir ihtimaldir. Bu sebeple sürecin savcıya gerekli hukuki değerlendirmenin, henüz bir başlangıç şüphesinin bulunup bulunmadığının ele alınması gereği için olsa dahi, yapılması için bildirilmesi gerekli olacaktır. Yapılacak yasal düzenlemede gerçek zamanlı biyometrik veriye dayalı takibin bu sebeple hâkim kararına dayalı olarak yapılması esas kural olmalıdır. Fakat gecikmesinde sakınca bulunan hallerde savcı veya konunun terör saldırısına ilişkin olması sebebiyle gerekli acil müdahale dikkate alınarak kolluk amiri tarafından

verilecek bir emirle de sonradan hâkimin onayına sunulmak ve hâkimin onay vermemesi durumunda ilgili kayıtların silinmesi kaydıyla, gerçekleştirilebilmesi mümkün olmalıdır. Buna karşın öldürme ve yaralama suçları bakımından her somut olayda retro perspektif açıdan oluşturulacak bir suçun işlenmiş olabileceğine ilişkin başlangıç şüphesinin varlığından bahsetmek mümkün olmayacaktır. Failin mağdurun öldürülmesine veya yaralamasına yönelik olarak gerçekleştirdiği düşünülen davranışları (silaha evden ayrılması, mağdurun bulunduğu yerin otogarına otobüsle gelmesi, mağdurun henüz gelmediği ama belirli bir süre sonra gelmesinin beklediği mekâna gitmesi) henüz cezaya değer haksızlığın gerçekleştiği ilk aşama olan suça teşebbüs aşamasına (doğrudan doğruya icra başlangıcı) ulaşmamış olabilecektir. Bu durumda önleyici kolluk faaliyeti kapsamında söz konusu olan bir suçun işlenebileceğine ilişkin tehlikeden bahsetmek mümkündür. Gerçek zamanlı biyometrik takibin somut olarak belirli bir kişiye yönelik olarak gerçekleşmesi durumunda dahi takip edilen kişi bakımından temel hak ve özgürlüklere ağır bir müdahale teşkil etmektedir. Bu sebeple başvurulabilmesi oldukça ağır suçlarla sınırlı tutulmuştur. Bu sebeple henüz başlangıç şüphesinin söz konusu olmadığı bir aşamada bulunsa dahi, takip sırasında gündeme gelecek takip konusu dışındaki suçlara ilişkin delil elde edilebileceği de dikkate alınarak, hâkim kararına tabi tutulması, ancak gecikmesinde sakınca bulunan hallerde sonradan hâkim tarafında onaylanmak ve aksi durumunda kayıtların silinmesi koşuluyla savcı ve savcıya ulaşılamadığı hallerde kolluk amiri tarafından verilecek emirle gerçekleştirilmesi mümkün olabilmelidir.

AB YZD m. 5/1-h (i)' de belirtilen gerçek zamanlı uzaktan biyometrik takip sisteminin kullanımına izin verildiği diğer durumlardan biri de somut olarak belirlenmiş olan kaçırma, insan ticareti veya cinsel sömürü mağdurlarının ya da kayıp kişilerin aranmasıdır. Sadece kayıp kişilerin aranması durumunda eğer başlangıç şüphesi düzeyinde bir suç işlendiği izlemini veren somut olgular söz konusu değilse söz konusu faaliyetin önleyici kolluk faaliyeti kapsamında kaldığının kabulü gerekecektir. Buna karşın kaçırma, insan ticareti ve cinsel sömürü mağdurlarının aranmasına yönelik kullanılması durumunda ortada en

azından gündeme gelen suçun işlendiğine yönelik en az başlangıç şüphesi düzeyinde bir şüphenin gündeme gelmesi söz konusu olması sebebiyle adli bir süreç söz konusu olacaktır. Bu durumda ilgili kararın adli merciler tarafından, kullanılacak yöntemin temel hak ve özgürlüklere ağır müdahale olması sebebiyle kural olarak hâkim tarafından alınmış bir karara dayanması gerekmektedir.

KAYNAKÇA

AKBULUT, Berrin/**AKBULUT**, Mete Tuluhan: "Yapay Zekâ Yasasında Risk Kategorileri", NEÜHFD, C. 8, S. 1, 2025, s. 466-496

AKBULUT, Berrin/AÇIL**, Murat:** "Avrupa Birliği Yapay Zekâ Tüzüğü'ne Göre Yasaklanmış Yapay Zekâ Uygulamaları", HBV-HFD, C. 30, S. 2, Nisan 2026, s. 995-1058.

ATLI, Turan: "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi", NEÜHFD, C. 2, S. 1, 2019, s. 4-22.

BANERT, Christian: KI-gestütze Ermittlungen und der Kernbereich privater Lebensgestaltung, Baden-Baden 2025.

BİRTEK, Fatih: "Ceza Muhakemesi Bakımından MİT Tarafından Elde Edilen İstihbari Bilgilerin Delil Niteliği" içinde: BİRTEK, Fatih (Editör), Hukuk Devletinde İstihbarat, Ankara 2025, s. 19- 30.

BORGHİ, Nikolozoi: Unermüdliche und unerschrokene digitale Helfer-KI-Systeme zur Auswertung pädokrimineller Daten, Sabine Gless/Dorotea Avedisian (Editörler), Künstliche Intelligenz in der Strafrechtspflege, Basel 2026, s. 191-200.

BRUN, Marcel: "Predictve Policing - Revolution in der Verbrechenskämpfung und Polizarbeit?", ZStrR, C. 140, Sayı: 2, 2022, s. 157-181.

BULUT, Metin: "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", Ankara Barosu Dergisi, S. 2020/3, 2020, s. 99- 150.

CİĞER, Selim: "Yeni Tip Gemilerin İşleyiş Esasları Bakımından Otonomi Kavramı ve IMO'nun Otonom Gemi Kategorileri Üzerine Düşünceler", İstanbul Hukuk Mecmuası, C. 82, S. 4, 2024, s. 1135-1183.

CONRAD, Catharina Pia: Ein Update für den Kernbereichsschutz, Berlin 2024.

ÇELİK, Dursun: "Tam Otomatikleştirilmiş İdari İşlemler", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, C. 28, S. 4, Ekim 2024, s. 413 - 452.

ERCAN, Cannur: "Robotların Fiillerinden Doğan Hukuki Sorumluluk: Sözleşme Dışı Sorumluluk Hallerinde Çözüm Önerileri", Türkiye Adalet Akademisi Dergisi, S. 40, 2019, s. 19-51.

ERDOĞAN, Irmak: Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlnilmesine Etkileri, Ankara 2022.

GERCKE, Björn: § 152, Gercke, Björn/Julius, Karl-Peter/Temming, Dieter/Zöller, Mark A. (Editörler), Heidelberger Kommentar zur Strafprozessordnung, 5. Baskı, Heidelberg 2012.

GLESS, Sabine**/ERIKSSON,** Salome**:** KI in der Strafrechtspflege: Einführung, Gless, Sabine/Avedisian, Dorotea (Editörler), Künstliche Intelligenz in der Strafrechtspflege, Basel 2026, s. 1-62.

GÖZLER, Kemal: İdare Hukuku, C. II, 3. Baskı, Bursa 2019.

GRAULICH, Kurt: Zum Trennungsgebot im Sicherheitsrecht, ENGELHART, Marc/KUDLICH, Hans/VOGEL, Benjamin (Editörler), Digitalisierung, Globalisierung und Risikoprävention, Festschrift für Ulrich Sieber, 2. Baskı, Berlin 2022, s. 929-946.

GUSY, Christoph: "Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität", Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV), Vol. 77, No. 3, 1994, s. 242- 251.

HAHN, Johanna: Automatisierte Gesichtserkennung in der Strafverfolgung, Baden-Baden 2025.

HOVEN, Elisa: "Die Grenzen des Anfangsverdachts- Gedanken zum Fall Edathy", NStZ, 2014, s. 361- 368.

İÇER, Zafer: "Yapay Zeka Temelli Önleyici Hukuk Mekanizmaları-Öngörücü Polislik, Yapay Zeka Temelli Teknolojiler ve Ceza Hukuku" Yapay Zekâ Çağında Hukuk: Yapay Zekâ Temelli

Teknolojiler ve Ceza Hukuku, Yapay Zekâ Çalışma Grubu Yıllık Rapor 2021, İstanbul Barosu, 2021, s. 30- 48.

İÇER, Zafer/DÖNMEZ, Elif: "Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları", CHD, Cilt: 15, Sayı: 43, Ağustos 2020, s. 421-461.

KIZILIRMAK, Baran: "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", KHASHFD, C. 7, S. 2, Aralık 2019, s. 225-261.

LI, Rueisiang: Die Auswirkungen von Künstlicher Intelligenz auf die Strafverfolgung, Baden-Baden 2025.

ÖZBEK, Veli Özer/**DOĞAN**, Koray/**BACAKSIZ**, Pınar: Ceza Muhakemesi Hukuku, 18. Baskı, Ankara 2025.

ÖZTÜRK, Bahri/**TEZCAN**, Durmuş/**ERDEM,** Mustafa Ruhan/**ALAN**, Esra/**GEZER, Özge Sırma/SAYGILAR,** Yasemin/**ÖZAYDIN,** Özdem/**ERDEN TÜTÜNCÜ,** Efser/**TOK,** Mehmet Can: Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 17. Baskı, Ankara 2023.

PETERS, Amadeus: Smarte Verdachtsgewinnung: Eine strafprozessuale und verfassungsrechtliche Untersuchung der Verdachtsgewinnung mittels Künstlicher Intelligenz, Baden-Baden 2023.

PETERS, Sebastian: StPO § 152, Schneider, Hartmut (Editör), Münchener Kommentar zur Strafprozessordnung, C. 2, 2. Baskı, Münih 2024.

PULLEN, Jennifer**/SCHEFER,** Patricia**:** Predictive Policing- Grundlagen, Funktionweise und Wirkung, SIMMLER, Monica (Editör), Smart Criminal Justice, Basel 2021, s. 103-122.

RABE, Lea: Das Urteil zur automatisierten Datenanalyse (BVerfGE 165, 363) – Besprechung des Urteils und seiner sicherheitsverfassungsrechtlichen Implikationen, BÄURLE, Michael/DENKER, Kai/GEMINN, Christian/SCHÖNDORF-HAUBOLD, Bettina (Editörler), Big Data und KI bei der Polizei, Bad Langensalza 2025, s. 15-43.

RICKER, Daniel: Anfangsverdacht und Vorurteil: Eine strafprozessrechtliche Untersuchung, Berlin 2021.

SCHINDLER, Stephan: "EU-Kommission: Verordnungsentwurf zur Regulierung von KI das Ende polizeilicher Gesichtserkennung im öffentlichen Raum?", ZD-Aktuell, 10/2021, https://beck-online.beck.de/Bcid/Y-300-Z-ZDAKTUELL-B-2021-N-05221 (Erişim Tarihi: 21.05.2025).

SCHULENBURG, Johanna: "Legalität- und Opportunitätsprinzip im Strafverfahren", JuS 2004, SAYI? s. 765-770.

SEROZAN, Rona: Hukukta Yöntem- Mantık, 3. Bası, İstanbul 2024.

SIMMLER, Monika**/BRUNNER,** Simone**/SCHEDLER,** Kuno**: Smart Criminal Justice - Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege (Studienbericht), Universität St. Gallen 2020.**

SIMMLER, Monika**/CANOVA,** Giulia**:** "Gesichterkennungstechnologie: Die "smarte" Polizeiarbeit auf dem rechtlichen Prüfstand", Sicherheit & Recht, 3/2021, s. 105-117.

STUCKENBERG, Carl-Friedrich: "The Constitutional Deficiencies of the German Rechtsgutslehre", Oñati Socio-Legal Series, v. 3, n. 1, 2013, s. 31-41.

ŞAHİN, Cumhur**/GÖKTÜRK,** Neslihan: Ceza Muhakemesi Hukuku, 15. Baskı, Ankara 2024.

SÖZÜER, Adem/**TURHAN**, Esma Nur: "Risk Toplumunda Ceza Hukukunun Rolü ve Fonksiyonu", Özgenç, İzzet (Editör), Risk Toplumunun Ceza Hukuku Alanında Ortaya Çıkardığı Sorunlar, Türkiye Bilimler Akademisi Yayınları, Ankara 2025, s. 11-43.

TINNEFELD, Marie-Theres**/BUCHNER,** Benedikt**/PETRI,** Thomas**/HOF,** Hans-Joachim: Einführung in das Datenschutzrecht, 7. Baskı, Berlin/Boston 2020.

TURHAN, Faruk/**KIRLIOĞLU**, Gamze/**BELCİ**, Ozancan: Türk Ceza Kanunu'na Göre Bilişim Sistemlerinin Araç Olarak Kullanılması

Suretiyle Dolandırıcılık- Phishing Yöntemiyle Online Bankacılık Erişim Bilgilerinin Ele Geçirilmesi ve Bunların Kullanılmasının Ceza Hukuku Açısından Değerlendirilmesi, Semih Yumak (Editör), Türk-Alman-Gürcü Ceza Hukuku Kolokyumu, Legal Yayınları Temmuz 2025, s. 105-142.

TURHAN, Faruk: "Tanıklara Yemin verilmesine İlişkin Ceza Muhakemesi Kanunu Hükümlerinin Eleştirel Bir Değerlendirilmesi", HBV-HFD, C. 24, S. 4, Ekim 2020, s. 359-410.

TURHAN, Faruk: Ceza Muhakemesi Hukuku, Ankara 2006

TURHAN, Faruk/**AKSU**, Muharrem: "11 Eylül Sonrası ABD'de Özgürlük ve Güvenlik Dengesi Açısından Terörü Önleme Amaçlı Tedbirler/Özellikle Patriot Kanunu ile Getirilen Kısıtlamalar", S.D.Ü. Hukuk Fakültesi Dergisi C. I, S. 1, 2011, s. 47-90.

ÜNVER, Yener/**HAKERİ,** Hakan: Ceza Muhakemesi Hukuku, 17. Baskı, Ankara 2020.

VOLZ, Stephanie: "Die KI-Verordnung und die Schweiz", sic!, 2025, s. 656-671.

WOHLERS, Wolfgang: "Das an einen tatbezogenen Anfangsverdacht gekoppelte Strafverfahren. Ein Konzept von gestern?", AJP/ PJA, 2020, s. 1311-1326.

YURTLU, Fatih: "Güncel Yargıtaya Kararlar Işığında Önleme Araması Neticesinde Elde Edilen Delillerin Hukuka Uygunluğu Üzerine Bir Değerlendirme", AndHD, 11 (1), Ocak 2025, s. 289-312.

ZAFER, Hamide/**YAVUZ,** Yağız: "Ceza Muhakemesinde Suç Şüphesi ve Dereceleri", MÜHF-HAD (Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi), Cilt: 30, Sayı: 2, Aralık 2024, s. 462-485.